CISSP MIND MAP

Simplifying "O" risk

Siorik Consultancy Pvt. Ltd

Find us @: http://siorik.com/

DOMAIN 1: Security and Risk Management

1. Security Governance through Principles and Policies

1.1. Confidentiality

Prevent or minimize unauthorized access to data while in storage, in process, and in transit.

Sensitivity: quality of information; cause harm or damage if disclosed.
Discretion: operator can influence or control disclosure to minimize harm or damage.
Criticality: mission critical information
Concealment: Security through obscurity
Secrecy: a secret information
Privacy: might cause harm, embarrassment, or disgrace to someone if revealed
Seclusion: storing in an out-of-the-way location
Isolation: separated from others to **prevent commingling of information**

1.2. Integrity

Integrity is the concept of protecting the reliability and correctness of data.

Accuracy: Being correct and precise
Truthfulness: Being a true reflection of reality
Authenticity: Being authentic or genuine
Validity: Being factually or logically sound
Nonrepudiation
Accountability: Being responsible or obligated for actions and results
Responsibility: Being in charge or having control over something or someone
Completeness: Having all needed and necessary components or parts
Comprehensiveness: Being complete in scope; the full inclusion of all needed elements

1.3. Availability

Authorized subjects granted timely and uninterrupted access to objects

Usability: easy to use or learn or being able to be understood and controlled by a subject
Accessibility: widest range of subjects can interact with a resource
Timeliness: being prompt, on time, within a reasonable time frame

1.4. CIA Priority

Military, government and IT system: CIA
Operational Technology (OT) systems: AIC

1.5. Other Security Concepts

Non-repudiation: Ensures that subject cannot deny the event occurred
Identification: Claiming to be an identity
Authentication: Proving that you are that identity
Authorization: Defining the permissions
Auditing: Recording a log
Accounting (aka accountability): Reviewing logs files to check for compliance and violations

1.6. Legally Defensible Security

To obtain legal restitution when bad thing happens, demonstrate that a crime was committed; that the suspect committed that crime, and that you took reasonable efforts to prevent the crime.

1.7. Protection Mechanisms

Layering: Defense in depth (controls in series)
Abstraction: Group similar elements and apply controls
Hide data: prevent data from being discovered. Security through obscurity
Encryption

1.8. Security Governance

Collections of practices to support, define, and direct the security efforts of an organization

Security management planning ensures proper creation, implementation, and enforcement of a security policy. Responsibility of upper management. Use a top-down approach. Elements

Define security roles
Prescribe how security will be managed, who will be responsible for security, and how security will be tested for effectiveness;
Develop security policies;
Perform risk analysis; and
Require security education for employees

Approval by senior management is must. Developing and implementing a security policy is evidence of due care and due diligence on the part of senior management.

A security management planning

Strategic Plan Five years plan that defines security goals. Includes a risk assessment

Tactical Plan a year plan to accomplish organizational goals. Like project plans, acquisition, hiring, budget, maintenance, support, and system development plans.

Operational Plan short-term (monthly or quarterly), highly detailed plan on how the implementation processes are in compliance with the organization's security policy. Training, system deployment, and product design plans; Resource allotments, budgetary requirements, staffing assignments, scheduling.

Acquisitions and mergers risk includes inappropriate information disclosure, data loss, downtime, or failure to achieve sufficient return on investment (ROI).

A divestiture or any form of asset or employee reduction is another area of risk.

1.8.1. Change Control Management

The goal of change management: Ensure that any change does not lead to compromised security

Goals of change management

Implement changes in controlled manner
A formalize testing process to verify change
All change be reversed (rollback plans/procedures)
Inform user before change to prevent loss of productivity
Minimize impact of change on security or business processes
Changes are reviewed and approved by a Change Advisory Board (CAB)

1.9. Data Classification

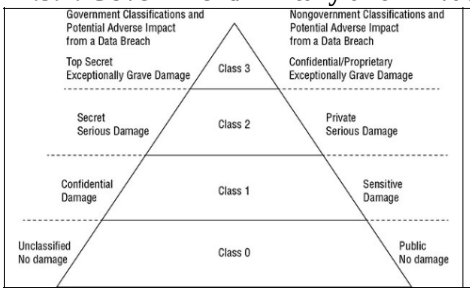
Data classification: Goal is to formalize and stratify the process of securing data based on assigned labels of importance and sensitivity. Provides means to store, process, transfer and declassify data.

Demonstrates commitment to protect valuable assets
Identifies most critical assets
Lends credence to the selection of protection mechanisms
Required for regulatory compliance or legal restrictions
Defines access levels, types of authorized uses, and parameters for declassification
It helps with data lifecycle management (storage length (retention), usage, and destruction) Data classification is based on

Usefulness/Timeliness/Value/Cost/Maturity/Age/Lifetime/Storage/Association with personnel/ Data disclosure/modification damage assessment/ National security implications/ Authorized access/ Restriction/ Maintenance and monitoring of the data Steps to data classification

Identify the custodian, and define their responsibilities.
Evaluate classification/labeling criteria
Classify and label each resource. (Owner conducts but a supervisor should review)
Document any exceptions
Select the security controls to each classification level
Specify declassification and custody transfer procedures
Create an awareness program to all personnel

1.9.1. Government/Military and Private/Business classification



Top secret cause grave damage. Data is compartmentalized on a need-to-know basis
Secret cause critical damage
Confidential cause serious damage
Sensitive But Unclassified (SBU) damage. Individual's private information is protected
Unclassified neither sensitive nor classified.

1.10. Organizational Roles and Responsibilities

Senior Manager ultimately responsible for the security. Must sign off on all policy issues
Security Professional Network, systems, and security engineer. Functional responsibility for security and are implementers. Write the security policy and implement it.
Data owner a high-level manager responsible for classifying information.
Data custodian provides protection for the CIA. Testing backups, validating data integrity, deploying security solutions, and managing data storage based on classification.
User (end user or operator) Comply with the security policy
Auditor responsible for reviewing and verifying implementation

1.11. Security Control Frameworks

Control Objectives for Information and Related Technology (COBIT) set of best IT security practices. It prescribes goals and requirements for security controls and encourages the mapping of IT security ideals to business objectives. Five key principles: *Meeting Stakeholder Needs, Covering the Enterprise End-to-End, Applying a Single, Integrated Framework, Enabling a Holistic Approach, Separating Governance From Management*
Open Source Security Testing Methodology Manual (OSSTMM) A peer-reviewed guide for the testing and analysis of a security infrastructure
ISO/IEC 27002 basis of implementing organizational security and management practices
Information Technology Infrastructure Library (ITIL) set of recommended best practices for core IT security and operational processes

1.12. Due Care and Due Diligence

Due care: Reasonable care to protect the interests of an organization (security policy, standards, baselines, guidelines, and procedures)
Due diligence: Practicing the activities that maintain the due care effort.
Operational security is the ongoing maintenance of continued due care and due diligence

The due care principle states that an individual should react in a situation using the same level of care that would be expected from any reasonable person. It is a very broad standard. The due diligence principle is a more specific component of due care that states an individual assigned a responsibility should exercise due care to complete it accurately and in a timely manner.

1.13. Security Policy

A strategic plan for implementing security and defines the scope of security.
It is used to assign responsibilities, define roles, specify audit requirements, outline enforcement processes, indicate compliance requirements, and define acceptable risk levels.
Security policies are compulsory.

An **organizational security policy** focuses on issues relevant to every aspect of an organization.
An **issue-specific security policy** focuses on a specific network service and department
A **system-specific security policy** focuses on individual systems and prescribes approved hardware and software, outlines methods for locking down a system, and even mandates firewall or other specific security controls.

In addition to these focused types of security policies, there are three overall categories
Regulatory policy: industry or legal standards are applicable
Advisory policy: discusses acceptable behaviors and defines consequences of violations.
Informative policy: provides information - company goals, mission statements, or how the organization interacts with partners and customers. It provides support or background information to the overall policy.

1.13.1. Acceptable Use Policy

The acceptable use policy is specifically designed to assign security roles within the organization as well as ensure the responsibilities tied to those roles. This policy defines a level of acceptable performance and expectation of behavior and activity. Failure to comply with the policy may result in job action warnings, penalties, or termination.

1.14. Standards, Baselines, Guidelines, and Procedures

Standards define compulsory requirements for the homogenous use of hardware, software, technology, and security controls. Tactical document defines steps to accomplish the goals

Baseline defines a minimum level of security that every system in organization must meet

Guideline how standards and baselines are implemented and serves as an operational guide. Suggests security mechanisms to deploy instead of a specific product & are not compulsory.

Procedure or standard operating procedure (SOP) is a detailed, step-by-step how-to document that describes the exact actions necessary. Ensures the integrity of business processes. Procedures help ensure standardization of security across all systems.

1.15. Threat Modeling

Threat modeling is a process where potential threats are identified, categorized, and analyzed.

Microsoft Security Development Lifecycle (SDL) motto "Secure by Design, Secure by Default, Secure in Deployment and Communication" (SD3+C) has two goals

- To reduce the number of security-related design and coding defects
- To reduce the severity of any remaining defects

A proactive approach (defensive approach). Defenses during the coding

A reactive approach (adversarial approach) is the core concept behind ethical hacking, penetration testing, source code review, and fuzz testing.

1.15.1. Identifying Threats

Focused on Assets Attempts to identify threats to the valuable assets

Focused on Attackers Identifies potential attackers and the threats they represent

Focused on Software Considers potential threats against the software

An ultimate goal of threat modeling is to prioritize the potential threats against assets.

Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of Privilege **PASTA: Process for Attack Simulation and Threat Analysis**

7-stage threat modeling methodology, a risk-centric approach that aims at selecting or developing countermeasures in relation to the value of the assets to be protected.

Definition of the Objectives (DO) for the Analysis of Risks
Definition of the Technical Scope (DTS)
Application Decomposition and Analysis (ADA)
Threat Analysis (TA)
Weakness and Vulnerability Analysis (WVA)
Attack Modeling & Simulation (AMS)
Risk Analysis & Management (RAM)

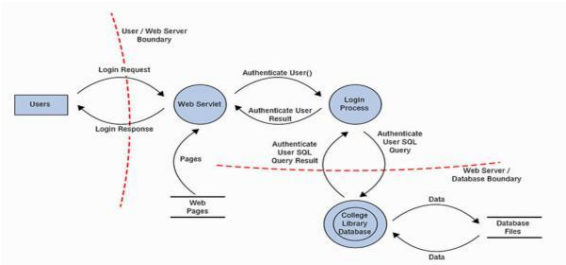
TRIKE and VAST

Trike focuses on a risk-based approach; provides a method of performing a security audit in a reliable and repeatable procedure; provides a consistent framework for communication and collaboration among security workers; is used to craft an assessment of an acceptable level of risk

Visual, Agile, and Simple Threat (VAST) is a threat modeling concept based on Agile project management and programming principles. The goal of VAST is to integrate threat and risk management into an Agile programming environment on a scalable basis.

1.15.2. Threat Identification: Determining and Diagramming Potential Attacks

Crafting an architecture diagram: a diagram of the elements involved in a transaction along with indication of data flows and privilege boundaries. It helps to detail the functions and purpose of each element of a business task, development process.



1.15.3. Performing Reduction Analysis

Reduction analysis: decompose the application, system, or environment to understand the logic of the product as well as its interactions with external elements. Identifies five key concepts:

Trust Boundaries Any location where the level of trust or security changes

Data Flow Paths The movement of data between locations
Input Points Locations where external input is received
Privileged Operations activity that requires greater privileges
Details about Security Stance and Approach The declaration of the security policy, security foundations, and security assumptions

1.15.4. Prioritization and Response

Priority basis: Probability × Damage Potential ranking, high/medium/low, or the DREAD system. The DREAD is a rating system

Damage potential: How severe is the damage likely to be if the threat is realized?
Reproducibility: How complicated is it for attackers to reproduce the exploit?
Exploitability: How hard is it to perform the attack?
Affected users: How many users are likely to be affected by the attack (as a percentage)?
Discoverability: How hard is it for an attacker to discover the weakness?

Response should include making adjustments to software architecture, altering operations and processes, and implementing defensive and detective components.

1.16. Risk-Based Management Concepts to Supply Chain

Supply chain: computers, devices, networks, and systems not built by single entity
A secure supply chain vendors in the chain are reliable, trustworthy, reputable organizations that disclose their practices and security requirements to their business partners
Goal of a secure supply chain: ensure that finished product is of sufficient quality

Outsourcing, contracting with suppliers, and engaging consultants are also elements of acquisition.
Process to evaluate a third party

On-Site Assessment
Document Exchange and Review
Process/Policy Review
Third-Party Audit third-party auditor can provide an unbiased review: SOC reports

Statement on Standards for Attestation Engagements (**SSAE**) is a regulation that defines how service organizations report on their compliance using the various SOC reports.

The SOC1 audit focuses on a description of security mechanisms to assess their suitability.
The SOC2 audit focuses on implemented security controls in relation to availability, security, integrity, privacy, and confidentiality.

The difference between SOC 2 and 3 is that the resulting SOC 2 report provides very detailed test data pertaining to the controls that provide the listed trust services, which is not for the general public. SOC 3 results in a report that has less detail and can be used for general purposes. SOC 3 is commonly used as a "seal of approval" and placed on service providers' websites and marketing collateral.

1.17. Enterprise Architecture Development

Zachman Framework: development of enterprise architectures
TOGAF Model and methodology: The Open Group development of enterprise architectures
DoDAF (Department of Defense architecture framework) that ensures interoperability of systems to meet military mission goals
MODAF Architecture framework in military support by British Ministry of Defence
SABSA for the development of information security enterprise architectures
Committee of Sponsoring Organizations (COSO) help reduce the risk of financial fraud
Six Sigma Business management strategy that can be used to carry out process improvement
OCTAVE is a team-oriented risk management methodology that employs workshops and is commonly used in the commercial sector.
A fault tree analysis is a useful approach to detect failures that can take place within complex environments and systems.
SWOT stands for Strengths/Weaknesses/Opportunities/Threats

Personnel Security and Risk Management Concepts

Humans are the weakest link.

2.1. Personal Security Policies and Procedures

2.1.1. Hiring

Creating a job description (what type of individual should be hired?)
Setting a classification for the job (individual should handle sensitive information?)
Screening employment candidates

Hiring and training for the job Important elements in constructing JD

Separation of duties: Protects against collusion. Deterrence effect.

Job responsibilities: Task performed on regular basis. Principle of Least Privilege.

Job rotation: First, provides knowledge redundancy; second, reduces the risks of fraud, data modification, theft, sabotage, and misuse of information. Problem: privilege aggregation

Cross training: Alternative to job rotation. Enables existing personnel to fill the work gap

2.1.2. Candidate Screening and Hiring

Screening is based on sensitivity and classification defined by the JD.

Work and educational history; checking references; verifying education; interviewing colleagues, neighbors, and friends; checking policy and government records; verifying identity through fingerprints, driver's license, and birth certificate; polygraph test, drug testing, personality testing

2.1.3. Employment Agreements and Policies

Outlines the rules and restrictions of the organization, the security policy, the acceptable use policies, details JD, violations and consequences, and the length of time the position is to be filled

Nondisclosure agreement protects confidential information. Violations met with penalties.

Noncompete agreement prevents employee working in competing organization.

2.1.4. On-boarding and Termination

Onboarding: adding new employees to the identity and access management (IAM)

Off-boarding: removal from IAM. Disabling/deleting user accounts, revoking certificates, canceling access codes, and terminating other specifically granted privileges.

Best time to terminate an employee is at the end of their shift midweek.

2.2. Vendor, Consultant, and Contractor Agreement

Agreement includes: Performance, expectation, compensation, and consequences for entities, persons, or organizations external to primary organization. Defined in SLA which addresses

System uptime, Maximum consecutive downtime, Peak load, Average load, Failover time

2.3. Risk Management

Primary goal: reduce risk to an acceptable level. Upper management decides risks appetite

IT security: logical/technical attacks. Physical protection: physical attacks

Risk analysis is a process by which goals of risk management are achieved

Threat: Any potential occurrence that may cause an unwanted outcome. Any action or inaction that could cause damage, destruction, or disclosure of assets

Threat Agents exploit vulnerabilities. Fire, earthquake, system failure, human error

Vulnerability: Weakness, flaw, oversight, error, limitation, frailty, or susceptibility

Exposure: being susceptible to asset loss; a threat agent can exploit vulnerability

Risk: The likelihood that a threat will exploit a vulnerability to cause harm to an asset. It is an assessment of probability, possibility, or chance. Every instance of exposure is a risk.

Attack: It is the exploitation of vulnerability by a threat agent.

Breach: security mechanism being bypassed or thwarted by a threat agent. When a breach is combined with an attack, a penetration, or intrusion, can result.

Quantitative risk analysis: assigns real dollar figures to the loss of an asset

Qualitative risk analysis: assigns subjective and intangible values to the loss of an asset.

2.3.1. Quantitative Risk Analysis

Exposure Factor (Loss Potential): the percentage of loss if assets were violated by a realized risk

Single Loss Expectancy (SLE): Single realized risk against an asset. AV * EF

Annualized Rate of Occurrence (ARO): Expected frequency a risk will occur in a year

It is a probability determination & derived from historical records, statistical analysis Annualized Loss Expectancy (ALE): Yearly cost of realized threat. ALE = SLE * ARO ALE with Safeguard: EF remains the same but ARO changes

Annual costs of safeguard should not exceed the expected annual cost of asset loss

Value of safeguard to the company = ALE before safeguard – ALE after safeguard – Annual cost of safeguard = (ALE_1-ALE_2) - ACS

Quantitative risk assessment process end values are used for prioritization and selection.

Obtaining the best security for the cost is an essential part of security management.

Value of Countermeasure: Various factors determines the value

Cost of purchase, development, and licensing
Cost of implementation and customization
Cost of annual operation, maintenance, administration
Cost of annual repairs and upgrades
Productivity improvement or loss
Changes to environment
Cost of testing and evaluation

2.3.2. Qualitative Risk Analysis

Qualitative risk analysis is scenario based and it involves judgment, intuition, and experience.
Brainstorming, Delphi technique, Storyboarding, Focus Groups, Surveys/Questionnaris, Checklists, One-on-one meetings, Interviews etc.

Delphi Technique is an anonymous feedback- and – response process used to enable a group to reach an anonymous consensus.

2.3.3. Risk Analysis Outcome

Complete and detailed valuation of all assets
An exhaustive list of all threats and risks, rate of occurrence, and extend of loss if realized
A list of threat-specific safeguards and countermeasures and ALE
A cost/benefit analysis of each safeguard

2.3.4. Risk Response

Reduce or mitigate, Assign or transfer, Accept
Deter: Implementing deterrents to would-be violators
Avoid: Selecting an alternative. Fly instead of drive.
Reject or ignore: Denying that a risk exists. Not prudent due-care response.

Residual Risk: Risk that remains once countermeasures are implemented

*Total risk = threats * vulnerabilities * asset value*	*Residual risk = Total risk – control gap*

2.3.5. Countermeasure Selection and Implementation

Selecting countermeasure or control in risk management relies on cost/benefit analysis results.

Technical Control: authentication methods (passwords, smartcards, and biometrics), encryption, constrained interfaces, ACL, protocols, firewalls, routers, IDS, clipping levels.
Administrative controls: policies, procedures, hiring practices, data classifications and labeling, security awareness and training, work supervision, personnel controls, and testing.
Physical controls: guards, fences, motion detectors, locked doors, sealed windows, lights, cable protection, badges, swipe cards, guard dogs, video cameras, mantraps, and alarms.

2.3.6. Applicable Types of Controls

Preventive Control: thwart or stop unwanted or unauthorized activity from occurring. E.g. fences
Detective Control: discover or detect unwanted or unauthorized activity. E.g. motion detectors
Compensating Control: provides options to controls. E.g. policy that all PII must be encrypted
Corrective Control: modifies environment to return systems to normal during an event. E.g. Reboot
Recovery Control: extension to corrective controls but after an event. E.g. backups and restores
Directive Control: directs, confies or controls the actions of subjects. E.g. security policy

2.3.7. Security Control Assessment

Formal evaluation of a security mechanism against a baseline
Goal is to evaluate, ensure and produce a report of the relative strength and weakness of the deployed security mechanism. SCA is based on NIST 800-53A

2.3.8. Asset Valuation

To select or evaluate safeguards and countermeasure ○
To provide values for insurance purposes
- To establish overall net worth for organization
- To make senior management understand exactly what is at risk

2.3.9. Reporting

Risk reporting is key task to perform at the conclusion of a risk analysis
Note: the risk assessment/analysis is a “point-in-time” metric. Threats and vunnerability changes.

2.3.10. Risk Framework

Security must be cost effective and measurable. Risk management framework: NIST 800-37
Security categorization, (categorize)
Security control selection, (select)
Security control implementations, (implement)

Security control assessment, (assess)
Information system authorization, (authorize) and
Security control monitoring (monitor)

2.4. Establish and Maintain a Security Awareness, Education, and Training Program

The successful implementation of a security solution requires changes in user behavior.
A prerequisite to security training is awareness. Awareness establishes a minimum standard or foundation of security understanding.
Training teaching employees to perform their work tasks to comply with the security policy.
Education is a more detailed endeavor. Learns much more than to perform their work tasks.

Business Continuity Planning

BCP involves assessing the risks to organizational processes and creating policies, plans and procedures to minimize the impact those risks might have on organization if occurred.
Goal of BCP is to provide quick, calm and efficient response in the event of an emergency and to enhance company's ability to recover from disruptive event promptly.
Top priority of BCP and DRP is people.

BCP has four main steps

1. Project scope and planning 2. BIA 3. Continuity Planning 4. Approval and implementation

The first two phases: determines working of BCP process and prioritize the business assets. Continuity planning: develop and implement a continuity strategy to minimize the impact

3.1. Project Scope and Planning

Structured business organization analysis (BOA)
Creation of BCP team with approval of senior management. First task then is BOA.
Assessment of resources available to participate in business continuity activities
Major resource consumed by BCP is human resource
Analysis of legal and regulatory landscape to a catastrophic event

3.2. Business Impact Assessment

Identify priorities
Factors affecting priorities: asset value, MTD, RTO
Goal of BCP is to ensure RTO < MTD
Risk identification: Identify natural and man-made risks. This is purely qualitative.
Likelihood assessment: Usually expressed in terms of ARO
Impact assessment
Assess the impact of each identified risks on business if it were to occur
Quantitatively: EF, SLE and ALE
Qualitatively: Loss of goodwill/employees. Social responsibility. Negative publicity
Resource prioritization
ALE can be used in quantitative point of view.
Qualitative concerns can be used to justify the prioritization done with quantitative
Recovery point objective RPO: maximum data, measured in time, that may be lost during recovery

3.3. Continuity Planning

Strategy development
It bridges the gap between BIA and continuity plan
Determine which risks are acceptable and which must be mitigated
risk of a blizzard striking in Egypt is negligible hence acceptable
risk ○ risk of monsoon in New Delhi is serious enough hence mitigate
Provisions and processes
Meat of entire business continuity plan
Design specific procedures and mechanisms to mitigate unacceptable risk
Categories of Assets to protect: People, Building/Facilities/Infrastructure
Hardening provision for facility/system
Alternative site/system
Plan approval: Once design is complete, top-level management endorsement is required
Plan implementation: Once approved, dive in and start implementing plan

Training and education: All personnel involved in plan should receive some sort of training on the overall plan and their individual responsibilities.

3.4. BCP Documentation

Helps in "sanity check"

Continuity Planning Goals: Operation of the business in the an emergency situation.
Statement of Importance: criticality of the BCP to organization's viability
Statement of Priorities: Functions critical to the continued business operations
Statement of Organizational Responsibility: BCP is everyone's responsibility!
Statement of Urgency and Timing: criticality of BCP and implementation timetable
Risk Assessment: decision-making process in BIA. Quantitative and qualitative analyses performed. Must be updated on a regular basis
Risk Acceptance/Mitigation: outcome of strategy development.
Vital Records Program: critical business records storage and the procedures for making and storing backup copies of those records. Challenge: identify the vital records
Emergency-Response Guidelines: outline the organizational and individual responsibilities
Immediate response procedures (security & safety procedures, fire suppression etc.) ○ A list of the individuals to notify
○ Secondary response procedures while waiting for the BCP team
Maintenance: The BCP documentation and the plan itself must be living documents.
Testing and Exercises: exercise program and personnel training

Laws, Regulations and Compliance

4.1. Categories of Laws

Criminal Law: outlines the rules and sanctions for major violations of the public trust
Civil Law: Framework to conduct business. Designed to provide for an orderly society
Administrative Law: policies, procedures, and regulations that govern the daily operations of the agency

criminal laws: Electronic Communications Privacy Act and the Digital Millennium Copyright Act. Trademark and patent law, are civil laws. HIPAA, PCI DSS administrative law

4.2. Comprehensive Crime Control Act (CCCA)

CCCA was related to federal system. Fine $1000 for any malicious damage caused.

4.3. Computer Fraud and Abuse Act (CFAA)

Written to exclusively cover computer crimes that crossed state boundaries. Threshold of damage was increased from $1,000 to $5,000. The act covered all "federal interest" computers.

4.4. Computer Abuse Amendments Act (CAAA)

Outlawed any type of malicious code
Computer used in interstate commerce
Imprisonment of any offenders (no matter if damage was done)
Victims can pursue civil action

4.5. National Information Infrastructure Protection Act of 1996

Computer used in international commerce
Infrastructure other than computing systems, such as railroads, gas pipelines etc.
Any act of damage to critical portions of the national infrastructure is a felony

4.6. Federal Sentencing Guidelines

The guidelines formalized the prudent man rule. Three burdens of proof for negligence
Person must have a legally recognized obligation
Person failed to comply with standards
Causal relationship between the act of negligence and subsequent damages

4.7. Federal Information Security Management Act (FISMA)

FISMA repealed and replaced: the Computer Security Act and GISRA. Burden on Federal agencies and government contractors

- Must develop and maintain substantial documentation of their compliance activities

4.8. Federal Cybersecurity Law 2014

Federal Information Systems Modernization Act (FISMA): Centralization of federal cybersecurity responsibility to Department of Homeland Security. Exceptions

– Defense-related cybersecurity issues: Secretary of Defense.
Intelligence-related issues: The Director of National Intelligence

Cybersecurity Enhancement Act: charged the NIST with responsibility for coordinating nationwide work on voluntary cybersecurity standards.

National Cybersecurity Protection Act: charged the Department of Homeland Security with establishing a national cybersecurity and communications integration center.

– Role of this center is to serve as the interface between federal agencies and civilian organizations for sharing cybersecurity risks, incidents, analysis, and warnings.

NIST Standard

NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations.

NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. Federal contractors must often comply

The NIST Cybersecurity Framework (CSF) is a set of standards designed to serve as a voluntary risk-based framework for securing information and systems.

4.9. Intellectual Property

4.9.1. Copyright

Expression in computer software is protected i.e. actual source code and not the idea behind

Ownership defaults to creator. Except works for hire

Works by one or more authors: 70 years after the death of the last surviving author

Works for hire and anonymous works: 95 years from the date of first publication or 120 years from the date of creation, whichever is shorter.

❖ ***Digital Millennium Copyright Act (DMCA)***

Designed to protect digital media CDs, DVDs

Penalties of up to $1,000,000 and 10 years in prison for repeat offenders

Exception: Nonprofit institutions such as libraries and schools are exempted

ISPs as *common carrier* & not held liable for the *transitory activities* of users. To qualify

Provider not initiate transmission

The technical process be automated

Provider must not determine the recipients

Any intermediate copies must not be retained for longer than necessary

No modification of content

Exception: system caching, search engines, and the storage of information on a network by users. However, remove copyrighted materials upon notification

Backup copies of computer software allowed if is licensed for use on a particular computer

Audio/video content in Internet to be treated as “eligible non-subscription transmissions.”

4.9.2. Trademarks

Words, slogans and logos. Objective: avoid confusion in the marketplace

™ to protect words or slogans

Official registration in United States Patent and Trademark office (USPTO)

Registered trademark symbol ®

Trademarks acceptance requirements

Must not be confusingly similar to another

trademark ○ Should not be descriptive

Valid for 10 years and can be renewed for unlimited successive 10-years periods

4.9.3. Patents

Protects intellectual property rights of inventors. Protection period is 20 years.

A patent is the strongest form of intellectual property protection.

Three requirements:

Invention must be new ○

Invention must be useful.

○ Invention must not be obvious.

“Patent trolls” Companies

The business that exist solely as patent holding companies that derive revenue by engaging in legal action against companies that fringe the patents held in their portfolio.

4.9.4. Trade-Secrets

Property critical to business
Copyright and Patents can be used to protect trade secret but will reveal the secret.
Official process
Keep them to yourself
Implement adequate
controls ○ Bound by NDA
Best ways to protect computer software

4.9.5. Economic Espionage Act 1996

Stealing trade secrets to benefit foreign agent be fined upto $500,000 and jail for 15 years
Other circumstances be fined upto $250,000 and jail for 10 years

4.10. Licensing

Contractual license agreements written contract for highly specialized software packages
Shrink-wrap license agreements written on packaging, acknowledge by breaking the seal
Click-through license agreements written on software box or included in documentation
Cloud services license agreements not in written form, simple flash of legal terms on screen or link to terms and a check box

4.11. Import and Export

The International Traffic in Arms Regulations (ITAR) controls the export of military and defense items. Listed on United States Munitions List (USML), maintained in 22 CFR 121
The Export Administration Regulations (EAR) items for commercial use but may have military applications. Listed on Commerce Control List (CCL), Department of Commerce
Computer Export Controls: export of high-performance computing systems prohibited to Cuba, Iran, North Korea, Sudan, and Syria.
Wassenar Agreement - Import/Export of encrypted goods.

Submit for review to the Commerce Department. Review will take no longer than 30 days.
After successful completion of this review, companies may freely export these products.

4.12. Privacy

4.12.1. US Privacy Law

Fourth Amendment is the basis for privacy rights.
Private property requires a warrant and probable cause
Protections against wiretapping and other invasions of privacy

4.12.2. Privacy Act 1974

Maintain only the records that are necessary and destroy when no longer needed
Applies only to government agencies

4.12.3. Electronic Communication Privacy Act 1986

Crime to invade the electronic privacy
Prohibits interception or disclosure of electronic communication
Protects against the monitoring of email and voicemail communications
Illegal to monitor mobile telephone conversations. Fine of up to $500 and a 5 years jail

4.12.4. Communications Assistance for Law Enforcement Act (CALEA) of 1994

Communications carriers to make wiretaps possible for law enforcement with court order

4.12.5. Health Insurance Portability and Accountability Act of 1996

Requires strict security measures for organizations that process private medical information

4.12.6. Health Information Technology for Economic and Clinical Health Act of 2009

Business associates be compliant (organizations that handle PHI on behalf of HIPAA entity)
Covered entity and a business associate be governed by a written contract known as a business associate agreement (BAA)
HITECH Breach Notification Rule: notify data breach to individuals and to Secretary of Health and Human Services and the media when the breach of more than 500 individuals

4.12.7. Children's Online Privacy Protection Act of 1998

Websites have a privacy notice stating types of information collected and it's use
Privacy notice to include contact information of operators of the site
Parents to review children's information and can permanently delete
Parents to give verifiable consent for younger than 13 prior to any such collection

Exceptions minimal information collection to obtain parental consent is OK!

4.12.8. Gramm-Leach-Bliley Act of 1999

Is considered a vertical regulation as it deals mainly with financial institutions
Institutions to give option to prohibit from sharing personal information with third parties
Board of directors is responsible for many of the security issues
Risk management must be implemented
All employees need to be trained on information security issues
Implemented security measures be fully tested
Institutions to have a written security policy in place
Requires financial institutions to explain how they share and protect their customers' private information. Communicate how they share the customers' sensitive data, inform customers of their right to opt-out, and apply specific protections to customers' private data in accordance with a written information security plan created by the institution.

Major components in place to govern PII include

Financial Privacy Rule: Provides with a privacy notice
Safeguards Rule: a written information security plan to protect PII
Pretexting Protection: Implement safeguards against pretexting (social engineering)

4.12.9. USA PATRIOT Act

Allows blanket authorization to monitor communications under single warrant
ISPs voluntarily provide government with a large range of information.
Detailed information on user activity through the use of a subpoena
Severe penalties for criminal acts of CFAA. Jail terms of up to 20 years

4.12.10. Family Educational Rights and Privacy Act

FERPA affects educational institution that accepts funding from the federal government.
It grants certain privacy rights to students older than 18 and the parents of minor students.
Specific FERPA protections include the following:

- Rights of parents/students to inspect any educational records
- Rights of parents/students to request correction of records
- Schools to not release personal information from student without consent

4.12.11. Identity Theft and Assumption Deterrence Act

This act makes identity theft a crime against the person whose identity was stolen and provides severe criminal penalties (up to a 15-year prison term and/or a $250,000 fine) for anyone guilty

4.12.12. European Union Privacy Law

The directive requires that all processing of personal data meet one of the following criteria:

- Consent
- Contract
- Legal obligation
- Vital interest of the data subject
- Balance between the interests of the data holder and the interests of the data subject

The directive also outlines key rights of data subjects

- Right to access the data
- Right to know the data's source
- Right to correct inaccurate data
- Right to withhold consent to process data in some situations
- Right of legal action should these rights be violated

American companies doing business in Europe can obtain protection under the Privacy Shield agreement. Businesses that comply are offered "safe harbor"

To qualify for Privacy Shield protection, U.S. companies must meet seven requirements

Informing Individuals About Data Processing
Providing Free and Accessible Dispute Resolution: response to complaints within 45 days
Cooperating with the Department of Commerce: respond to requests from the U.S. DoC
Maintaining Data Integrity and Purpose Limitation
Ensuring Accountability for Data Transferred to Third Parties
Transparency Related to Enforcement Actions
Ensuring Commitments Are Kept As Long As Data Is Held

4.12.13.GDPR

Applies to all organizations that collect/process data from EU residents

GDPR – Key provisions

Serious data breach notification within 24 hours
The creation of centralized data protection authorities in each EU member state
Provisions that individuals will have access to their own data
Data portability provisions - facilitate the transfer of information between service providers
The "right to be forgotten"

4.13. Contracting and Procurement

The increased use of cloud services and other external vendors leads organizations to focus on implementing security reviews and controls in contracting and procurement processes.
Reviews of the security controls put in place by vendors

4.14. Miscellaneous points

Enterprise security architecture describes current/future security process t ensure strategic alignment
Blueprints functional definitions for integration of technology into business processes
Enterprise architecture frameworks architectures to map organizational needs and business drivers
COSO governance model prevent fraud in corporate environment
ITIL set of best practices for IT service management
Six Sigma identify defects in processes so that it can be improved
Security enterprise architecture ties strategic alignment, business enablement, process enhancement, and security effectiveness
OCTAVE team-oriented risk management methodology that employs workshops
A fault tree analysis approach to detect failures in complex environments

DOMAIN 2: Asset Security

5. Protecting Security of Assets

Asset classifications should match the data classifications.

5.1. Identify and Classify Assets

First steps in asset security is identifying and classifying information and assets. Classification definitions are within a security policy.
PII defined by NIST SP 800-122
Any information about an individual maintained by an agency, including
Proprietary data is any data that helps an organization maintain a competitive edge.
software code, technical plans, internal processes, intellectual property, or trade secrets.

5.2. Determining Data Security Controls

After classifications, define security requirements and identify security controls to implement. E.g.
Confidential/Proprietary (highest level of protection) Encrypt email and attachments with AES 256

5.3. Handling Information and Assets

A key goal of managing sensitive data is to prevent data breaches
Steps to limit data breaches
Marking Sensitive Data and Assets
Handling Sensitive Data and Assets: Handling refers to the secure transportation ○ Storing Sensitive Data
- ○ Destroying Sensitive Data: ensures that it cannot fall into the wrong hands
- ○ Eliminating Data Remanence
- ○ Ensuring Appropriate Asset Retention

5.3.1. Eliminating Data Remanence

Degausser generates a heavy magnetic field and are only effective on magnetic media
Degaussing does not affect optical CDs, DVDs, or SSDs.
Degaussing SSDs won't remove data. Destroy using disintegrator to a size of 2 millimeters
Or, ensure all stored data in SSD is encrypted. If sanitization fails data would be unreadable
Erasing media performs delete operation against a file. Anyone can retrieve using tools
Clearing or overwriting, prepares media for reuse ensuring traditional tool can't recover data
Spare sectors on hard drives, sectors labeled as "bad," and areas on many modern SSDs are not necessarily cleared and may still retain data
Purging an intense form of clearing prepares media for reuse in less secure environments.
Assures that original data is not recoverable using any known methods
Top secret data will always remain top secret until it is destroyed

Destruction the final stage in lifecycle of media and is most secure sanitization method incineration, crushing, shredding, disintegration, and dissolving using caustic or acidic chemicals.

Declassification purges media in preparation for reuse in an unclassified environment

Often efforts required to securely declassify media are significantly greater than new media

5.4. Data Protection Methods

Protecting Data with Symmetric Encryption

AES is most popular symmetric encryption algorithms. Used in Microsoft and others

Triple DES in MasterCard, Visa (EMV), and Europay standard for smart payment cards

Linux systems use bcrypt (based on Blowfish) to encrypt passwords. Adds 128 bits as a salt

Protecting Data with Transport Encryption

TLS to protect data in transit. Protects against sniffing attack

IPsec is combined with L2TP for VPNs. L2TP transmits in cleartext, L2TP/IPsec encrypts.

IPsec AH provides authentication and integrity, and ESP provides confidentiality

IPsec and Secure Shell (SSH) protect data in transit on internal networks.

Telnet within VPN tunnel is not acceptable as the traffic is only encrypted from the client to the VPN server and is sent as cleartext from the VPN server to the Telnet server

5.5. Determining Ownership

Data Owners

Has ultimate organizational responsibility for data. CEO, president, or a department head

Identifies classification of data, ensure label, ensure security controls

Liable for negligence if they fail to perform due diligence

The asset/system owner is person who owns the asset/system that processes sensitive data

Responsible for ensuring that data processed on the system remains secure

Ensures that data is protected while at rest on system, in transit between systems, and in use

Business/Mission Owners

Program manager or an information system owner

Sales department is business owner but the IT/software department could be the system owners for systems used in sales processes

Business owners are responsible for ensuring that systems provide value to the organization

Organizations often implement IT governance methods such as COBIT

Any system used to process data

GDPR “a natural or legal person, public authority, agency, or other body, which processes personal data solely on behalf of the data controller.”

Grants access to personnel based on the principles of least privilege and the need to know

Custodians

A custodian helps protect the integrity and security of data

Personnel within IT department or system security administrators would be the custodians

Users

Accesses data via a computing system to accomplish work tasks. Complies with policies

5.6. EU Privacy Directives

Privacy Shield Principles

Notice: must inform purpose to data collection

Choice: must offer the opportunity to opt out

Accountability for Onward Transfer: only transfer data to organizations that comply with the Notice and Choice principles

Security: must take reasonable precautions to protect personal data

Data Integrity and Purpose Limitation: only collect needed data. Ensure data is accurate, complete, and current

Access: personal information be accessible. Must have the ability to correct, or delete

Recourse, Enforcement, and Liability: must ensure compliance with principles and provide mechanisms to handle individual complaints

Two technical security controls are encryption and pseudonymization

A pseudonym is an alias. E.g. J. K. Rowling pseudonym of Robert Galbraith.
It can be done to prevent the data from directly identifying an entity
The GDPR refers to pseudonymization as replacing data with artificial identifiers.
Tokenization is similar to pseudonymization but uses tokens.
Neither the pseudonym nor the token has any meaning or value outside the process that creates them and links them to the other data. Additionally, both methods can be reversed to make the data meaningful.

Process of removing relevant data so that it is impossible to identify original subject.
GDPR is not relevant for the anonymized data
Data masking is an effective method. Masking cannot be reversed

5.7. Using Security Baselines

Baselines provide a starting point and ensures a minimum security standard
One common baseline that organizations use is imaging
MS Group Policy periodically checks systems and reapply settings to match the baseline

5.8. Scoping and Tailoring

Scoping: review lists of baseline security controls and select only those that apply your system. E.g. if two people cannot login into your system then concurrent session control is not required
Tailoring: modify lists of security controls within a baseline to align with organization's mission. E.g. a set of baseline controls applies perfectly to computers in main location, but some controls aren't feasible in a remote office. Then, select compensating security controls to tailor the baseline to the remote location

DOMAIN 3: Security Architecture and Engineering

6. Cryptography and Symmetric Key Algorithm

Cryptography provides confidentiality, integrity, authentication, and nonrepudiation for sensitive information

6.1. Cipher

Ceaser Cipher

Mono-alphabetic substitution, Shift three places right, Vulnerable to frequency analysis

Ultra vs. Enigma

Enigma: 3-6 rotors to implement an complicated substitution cipher. Ultra: top-secret effort to break Engima

6.2. Cryptographic Basics

Goals of Cryptography

Confidentiality (Symmetric and Asymmetric Cryptosystems)
Integrity (Digital Signatures)
Authentication, (challenge-response authentication technique that uses encryption)
Non-repudiation

Key nothing more than a number. A binary.
Key space: range of valid values for use as a key
Cryptography: art of creating and implementing secret codes/ciphers
Cryptanalysis: methods to defeat ciphers
Cryptology: Cryptography + Cryptanalysis
Cryptosystems: implementation of cipher in hardware and software
Nonce: A random number. IV.
Zero-knowledge proof
Split knowledge: separation of duties and two-person control. Eg. Key escrow
M of N control
Work function: time and effort to perform a complete brute-force attack against an encryption

Codes and Ciphers: codes work on words/phrases, ciphers on individual characters and bits
Transposition Ciphers: rearrange the letters
Substitution Ciphers: replace each character or bit
Polyalphabetic substitution: protects against direct frequency analysis but is vulnerable period analysis **Period analysis** an examination of frequency based on the repeated use of the key
One-Time Pads extremely powerful type of substitution cipher. Also known as Vernam ciphers
Difficulty of generating, distributing, and safeguarding the lengthy keys required

Can be used only for short messages, because of key lengths

The Caesar cipher: key of length one, Vigenère cipher: longer key (word or sentence)

Running Key Ciphers: encryption key is as long as the message, chosen from a common book

Block Ciphers: operate on chunks. E.g. transposition ciphers

Stream Ciphers: one character/bit at a time. E.g. Caesar cipher

Confusion plaintext & key so complicated that altering plaintext & analyzing ciphertext can't determine key

Diffusion a change in plaintext results in multiple changes spread throughout ciphertext

6.3. Modern Cryptography

Modern cryptosystems rely on the secrecy of one or more cryptographic keys.

6.3.1. Symmetric Key Algorithms

Key distribution is a major problem
Does not implement nonrepudiation
Algorithm is not scalable. Difficult for large groups to communicate.
Keys must be regenerated often.
Major strength is the great speed. 1000 to 10,000 times faster than asymmetric.
Keys: [n*(n-1)/2]

6.3.2. Asymmetric Key Algorithms

Key requirement: 2n

Strengths:

The addition of new users requires one public-private key pair
Users can be removed far more easily from asymmetric systems
Key regeneration is required only when a user's private key is compromised
Can provide integrity, authentication, and nonrepudiation
Key distribution is a simple process
No preexisting communication link needs to exist

Weakness: Slow speed of operation

6.4. Symmetric Cryptography

6.4.1. Data Encryption Standard (DES)

64-bit block. The key is 56 bits long
Uses a long series of XOR. 16 rounds of operations

Modes of Operation

ECB

the simplest mode of operation
Security Issues: Pattern at block level are preserved. Leak in security
Error Propagation: Error in one block does not have any effect other blocks

Cipher Block Chaining

Each plaintext block XOR with the previous ciphertext block before being encrypted
An IV is XOR with first block of message. Produces unique o/p everytime
Error Propagation: propagated. if one block is corrupted, impossible to decrypt that & the next block

Cipher Feedback Mode

Streaming cipher version of CBC operates against data produced in real time.
Instead of breaking a message into blocks, it uses memory buffers of the same block size.
As the buffer becomes full, it is encrypted and then sent to the recipients.
It uses an IV, and it uses chaining. Propagates error

Stream cipher. Instead of XOR previous block of ciphertext, XORs the plaintext with a seed value.
For the first encrypted block, an IV is used to create the seed value.
Future seed values are derived from previous seed value.
Advantage: there is no chaining function and errors do not propagate

Stream cipher, similar to that used in CFB and OFB modes
However, seed value is created using a simple counter that increment for each operation
As with OFB mode, errors do not propagate in CTR mode
Allows breaking encryption/decryption operation into multiple independent steps.
Well suited for use in parallel computing

6.4.2. Triple DES

Four version of 3DES

DES-EEE3: 3*56=168 bits
DES-EDE3: 3*56=168 bits
DES-EEE2: 2*56=112 bits
DES-EDE2: 2*56=112 bits

6.4.3. International Data Encryption Algorithm (IDEA)

Plaintext/ciphertext is 64 bits
Key is of 128 bits. And it is divided in 52 16-bit subkeys
8 rounds are identical and in each round 6 keys are used. 8*6=48 keys
Last round uses 4 keys (6 * 8 = 48 + 4 =52 total)
IDEA was used in Pretty Good Privacy (PGP) v2.0

6.4.4. Blowfish

64-bit blocks of text, 32-448 bits key. Often used in SSH.
Faster than IDEA and DES

6.4.5. Skipjack

64-bit blocks of text, 80-bits key
Supports the escrow of encryption keys. NIST and Department of the Treasury holds key
Supported the Clipper and Capstone encryption chips

6.4.6.RC5

Block cipher of variable sizes (32, 64, or 128 bits), 0- 2040 bits key

6.4.7.AES

AES is Replacement of DES. 128 bit data
128-bit keys require 10 round, 192-bit keys require 12 round, 256-bit keys require 14 round

6.4.8. TwoFish

One of the AES finalists
A 128-bit blocks of data, keys up to 256 bits Twofish
uses two techniques not found in other algorithms:
Prewhitening XORing plaintext with a separate subkey before the first round of encryption
Postwhitening uses a similar operation after the 16th round of encryption.

Name	Block Size	Key Size
AES	128	128, 192, 256
Rijndael	Variable	128, 192, 256
Blowfish (often used in ssh)	64	32-448
DES	64	56
IDEA (used in PGP)	64	128
RC2	64	128
RC5	32, 64, 128	0-2040
Skipjack	64	80
Triple DES	64	112 or 168

6.5. Symmetric Key Management

Methods to exchange secret keys securely
offline distribution (out of band)
public key encryption, and
Diffie–Hellman key exchange algorithm. *Secure RPC employs Diffie–Hellman for key exchange.*

Storage and Destruction of Keys:
Keys and encrypted data should be stored in different system
Use split knowledge for sensitive key

6.5.1. Key Escrow and Recovery

Key escrow systems allow the government to obtain the cryptographic key
Fair Cryptosystems secret keys divided into two or more pieces & given to independent third party
Escrowed Encryption Standard provides government with technological means to decrypt ciphertext. This standard is the basis behind the Skipjack algorithm.

PKI and Cryptographic Application

7.1. RSA

Based on difficulty in factoring large prime numbers (typically 512 bits). N=P*Q

7.2. Merkle-Hellman Knapsack

Relies on a component of set theory known as super-increasing sets rather than large prime numbers
Merkle-Hellman was proven ineffective when it was broken in 1984

7.3. ElGamal

Extension to Diffie–Hellman key exchange algorithm
It was not patented and hence free to use unlike RSA
Disadvantage: doubles the length of any message it encrypts

7.3.1. Elliptic Curve

Extremely efficient due to very small key sizes
Provides digital signing, secret key distribution, and data encryption
Based on discrete logarithm problem

RSA and DSA – 1024 bits key
Elliptic Curve – 160 bits key

7.4. Hash Function

Requirements for a cryptographic hash function
The input can be of any length
The output has a fixed length
The hash function is relatively easy to compute for any input
The hash function is one-way
The hash function is collision free

7.4.1. Hash of Variable Length (HAVAL)

Modification of MD5
1,024-bit blocks and hash values of 128, 160, 192, 224, and 256 bits

7.4.2.SHA

These are government standard hash functions promoted by the NIST.
SHA-1: 512-bit block, 160-bit digest. There are weaknesses don't use.
SHA-256: 512-bit block, 256-bit digest
SHA-224: 512-bit block, 224-bit digest
SHA-512: 1024-bit block, 512-bit digest
SHA-384: 1024-bit block, 384-bit digest
Keccak algorithm: SHA-3 standard

7.4.3.MD2

Secure hash function for 8-bit processors
MD2: multiple of 16 bytes block, 128-bit digest
Collisions may occur. It is not a one-way function

7.4.4.MD4

Secure hash function for 32-bit processors
Pads message to ensure the message length is 64 bits smaller than a multiple of 512 bits.
Then processes 512-bit blocks of the message in three rounds of computation. 128-bit digest

7.4.5.MD5

512-bit blocks, four distinct rounds of computation, 128 bits digest.
Padding requirement is same as MD4

7.5. Digital Signatures

Goals: Enforce nonrepudiation, Message Integrity
Based on public key cryptography and hashing function.
Sender encrypts using the private key and receiver decrypts using the public key
Software vendors use digital signature to authenticate code distributions
Does not provide privacy but ensures that goals of integrity, authentication, and non-repudiation

Rule of Thumb

Encrypt a message: recipient's public key
Decrypt a message: your private key
Digitally sign a message: use your private key
Verify the signature: use the sender's public key

7.6. HMAC

Implements a partial digital signature - guarantees the integrity but not nonrepudiation
Uses a shared secret key

7.7. Digital Signature Standard

NIST specifies digital signature algorithms acceptable for federal government
Acceptable: SHA-3 hash; DSA, RSA, Elliptic Curve DSA encryption

NOTE: Two other DSA: Schnorr's signature algorithm and Nyberg-Rueppel's signature algorithm **7.8. Public Key Infrastructure**

Combines asymmetric with symmetric cryptography along with hashing/digital certificates
Provides hybrid cryptography

7.8.1. Certificates

Digital certificates provide assurance that communicating parties truly are who they claim to be
If certificate is signed by trusted CA, public key is legitimate

Version of X.509 to which the certificate conforms
Serial number (from the certificate creator)
Signature algorithm identifier (specifies the technique used to sign)
Issuer name (identification of CA)
Validity period
Subject's name (DN of entity that owns the public key)
Subject's public key (the meat of the certificate)

7.8.2. Certificate Authorities

These neutral organizations offer notarization services for digital certificates.

Symantec, IdenTrust, AWS, GlobalSign, Comodo, Certum, GoDaddy, DigiCert, Secom, Entrust, Actalis, Trustwave

Registration authorities (RAs) assist CAs with burden of verifying users' identities. They do not directly issue certificates

7.8.3. Certificate Path Validation

CPV: each certificate in certificate path from root of trust down to server/client is valid/legitimate
CPV verifies that every link between "trusted" endpoints remains current, valid, and trustworthy

7.8.4. Certificate Generation and Destruction

Enrollment: prove your identity to the CA

Once enrolled, you provide your public key. CA creates X.509 digital certificate with your identification & public key. Then digitally signs using CA's private key and provide you with a copy of your signed digital certificate. Distribute this certificate to with whom you want to communicate

Verify other's certificate by checking CA's digital signature using CA's public key
Check if the certificate was revoked using a CRL or Online Certificate Status Protocol (OCSP)

Revocation

Revocation of certification might occur because

The certificate was compromised
The certificate was erroneously issued
The details of the certificate changed
The security association changed (subject no longer employed by organization)

The revocation request grace period is maximum response time a CA will perform any requested revocation
Certificate Practice Statement (CPS) states practices a CA employs when issuing or managing certificates
Techniques to verify the authenticity of certificates and identify revoked certificates

Certificate Revocation Lists (CRL): List of invalid certificates. Causes latency
OCSP: Eliminates latency of CRL and provides real-time certificate verification. Query online

7.9. Asymmetric Key Management

Hardware security modules (HSMs) provide an effective way to manage encryption keys
These hardware devices store and manage encryption keys in a secure manner

7.10. Applied Cryptography

7.10.1. Portable Devices

Apply and manage encryption on portable devices. E.g.
BitLocker/FileVault/VeraCrypt **Trusted Platform Module**

A chip that resides on the motherboard of the device
Serves as storage and management of keys for full disk encryption (FDE)
TPM prevents from removing drive from one device and accessing data in another device

7.10.2. Email

PGP (Pretty Good Privacy)

It combines the CA hierarchy with the "web of trust"
Commercial: RSA for key exchange, IDEA for encryption, and MD5 for digest
Freeware: (OpenPGP) Diffie-Hellman key exchange, the Carlisle Adams/Stafford Tavares (CAST) 128-bit for encryption, and SHA-1 for digest

S/MIME uses the RSA encryption algorithm
X.509 certificates for exchanging cryptographic keys
RSA is the only public key supported. The protocol supports AES and 3DES private key
The use of browser extensions is required

7.10.3. Web Applications

SSL and TLS

When a user accesses a website, extracts the server's public key from server's certificate
Browser creates random symmetric key, encrypts with server's public key, and sends to server
Server decrypts symmetric key, and exchanges all future messages using the symmetric key

POODLE attack demonstrated a significant flaw in the SSL 3.0 fallback mechanism of TLS

7.10.4. Steganography and Watermarking

Art of using cryptographic techniques to embed secret messages within another message
Alters least significant bits. Creates covert channel.
Often used for illegal activities, such as espionage and child pornography
Legitimate purposes: digital watermarks

7.10.5. Digital Rights Management

Uses encryption to enforce copyright restrictions on digital media
Fatal flaw: the device used to access the content must have access to the decryption key. Device can be manipulated to gain access to the key.

High-Bandwidth Digital Content Protection (HDCP) DRM protection for content sent over digital connections including HDMI, DisplayPort, and DVI interfaces. Hackers released master key
Advanced Access Content System (AACS) Protects the content stored on Blu-Ray and HD DVD. Hackers released key for this too

Adobe offers Adobe Digital Experience Protection Technology (ADEPT) DRM for e-books
AES to encrypt and RSA protect the AES key

Verify the game license with a cloud-based service

Document DRM

Common permissions restricted
Reading/Modifying/Removing watermarks/Downloading/saving/Printing/Taking screenshots

7.10.6. Networking – Circuit Encryption

Link encryption

protects entire communications circuits by creating a secure tunnel
all data is encrypted which slows the routing
encryption done at lower layers of OSI model

protects communications between two parties. Use TLS: between user & web server
does not encrypt the header/trailer/address, and routing data, so moves faster
Susceptible to sniffers and eavesdroppers
Encryption at higher OSI layers
Secure Shell (SSH) is a good example

7.10.7. Networking – IPSec

IPsec uses public key cryptography to provide encryption, access control, nonrepudiation, and message authentication, all using IP-based protocols. IPsec is commonly paired with L2TP
AH provide integrity/nonrepudiation. Also authentication/access control/prevents replay attacks
ESP provide confidentiality/integrity. Also encryption/limited authentication/prevents replay attacks
Transport Mode only packet payload is encrypted. Designed for peer-to-peer communication
Tunnel Mode entire packet is encrypted. Designed for gateway-to-gateway communication

Security association is used to set up an IPsec session. represents a simplex connection. o
For a two-way channel, two SAs is needed, one for each direction
- To support bidirectional channel using both AH and ESP, four SAs is needed

7.10.8. Networking – IKE

Internet key exchange phases
Negotiate
H: hashing
A: Authentication
- G: Group
- L: Lifetime
- E: Encryption

Share the secret (DH)
Authenticate

7.10.9. Networking – ISAKMP

Provides services for IPsec by negotiating/establishing/modifying/deleting security associations. Four basic requirements for ISAKMP
Authenticate communicating peers
Create and manage security associations
Provide key generation mechanisms
Protect against threats (replay and denial-of-service attacks)

*Note: **Oakley**: Used for key management (uses Diffie Hellman)*

7.10.10. Wireless Networking

WPA does not provide an end-to-end security solution. It encrypts traffic only between a mobile computer and the nearest wireless access point. Once traffic hits wired network, it's in clear again
IEEE 802.1x: flexible framework for authentication and key management in wired/wireless networks
To use 802.1x, the client runs a supplicant that communicates with authentication server.
WPA was designed to interact with 802.1x authentication servers.

7.11. Cryptographic Attacks

Analytic Attack algebraic manipulation to reduce complexity of algorithm. Focus on logic of algo.
Implementation Attack exploits weakness of cryptography system. Not just errors but methodology
Statistical Attack exploits statistical weaknesses (random numbers), vulnerability in hardware/OS
Brute Force attacks directly proportional to the length of the key. Will always be successful given enough time. Every additional bit of key length doubles the time to attack
Hashing with salt (PBKDF2, bcrypt, and scrypt) use key stretching
Frequency Analysis and the Ciphertext Only Attack: frequency analysis is helpful
Known Plaintext: attacker has copy of ciphertext and plaintext
Chosen Ciphertext: attacker has ability to decrypt chosen portions of the ciphertext
Chosen Plaintext attacker has ability to encrypt chosen plaintext
Meet in the Middle vulnerability in 2DES
Man in the Middle:
Birthday Attack. Collision Attack or Reverse Hash Matching
Replay: intercept and then later replay to open a new session. Defeat using a time stamp expiry

8. Principles of Security Models, Design and Capabilities

8.1. Subjects and Objects

The subject is user/process that request access to resource. Access mean reading/writing a resource.
The object is the resource a user/process wants to access
Transitive trust: if A trusts B and B trusts C, then A trust C

8.2. Closed and Open Systems

The standards for closed systems are often proprietary and not normally disclosed
Open systems: designed using agreed-upon standards. Can integrate with different manufacturers
Closed systems can be more secure as known vulnerabilities may not exist
Openness makes them more vulnerable to attack

8.3. Techniques to Ensure CIA

8.3.1. Confinement

Process confinement restricts the actions of a program
Read from and write to only certain memory locations and resources. Sandboxing

8.3.2. Bounds

The authority level tells the operating system how to set the bounds for a process
The bounds sets limit on memory addresses and resources a process can access
OS is responsible to enforce these logical bounds
More secure systems require physically bounded processes.

8.3.3. Isolation

When a process is confined through bounds, that process runs in isolation
Process isolation ensures that any behavior will affect only the associated memory and resources
Isolation is used to protect operating environment, kernel OS, and other applications

8.3.4. Controls

A control uses access rules to limit the access of a subject to an object

8.3.5. Trust and Assurance

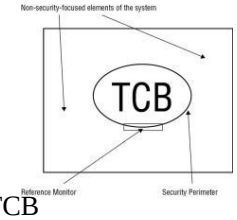
Trusted system: all protection mechanisms work together to process sensitive data for many users maintaining a stable and secure computing environment
Assurance: degree of confidence in satisfaction of security needs. maintain/update/re-verify
Change is often the antithesis of security; it often diminishes security
Specific security features builds trusts and assurance assess reliability/usability of those features

8.4. Fundamental Concepts of Security Models

A security model provides a way for designers to map abstract statements into a security
Security token: separate object associated with resource and describes its security attributes. Token communicates security info about object prior to requesting access to actual object
Capabilities: rows of security attributes for each controlled object. Offers quicker lookups
Security label: permanent part of object. Once set, not altered. Safeguard against tampering

8.4.1. Trusted Computing Base

Combination of hardware/software/controls to form trusted base to enforce security policy
A subset of complete information systems. Be as small as possible
It can be trusted to adhere to and enforce the security policy
TCB components are responsible for controlling access to the system



It is an imaginary boundary that separates the TCB from the rest of the system
It ensures that no insecure communications occur between the TCB and other elements
Trusted path: channel established with strict standards to allow interaction without exposing TCB
A trusted path protects system users (subjects) from compromise
Required for high-trust-level systems such as B2 or higher of TCSEC

Reference monitor: part of TCB that validates access to every resource prior to granting access
Security kernel: collection of components in TCB that work together to implement reference monitor
The reference monitor is implementation of a security kernel in software and hardware.
Working is based on Tokens, Capabilities, and Labels

8.4.2. State Machine Model

It is based on object and attributes. Machine is secure no matter what state it is in.
It's based on finite state machine (FSM)
A state is a snapshot of a system at a specific moment in time
A transition occurs when accepting input or producing output

8.4.3. Information Flow Model

Data flow between objects at various security levels and are based on a state machine model
Designed to prevent unauthorized, insecure, restricted information flow between different levels
It dictates transformation of object from one state to another
It addresses covert channels by specifically excluding all nondefined flow pathways

8.4.4. Noninterference Model

Barriers between levels to prevent data leakage
How actions of subject at higher security level affect system state/actions of subject at lower level?
The actions of subject A (high) should not affect the actions of subject B (low) or even be noticed
This model can provide a form of protection against damage caused by malware like Trojan horse

Composition Theories

Cascading: Input for one system comes from the output of another system.
Feedback: One system provides input to another system, which reciprocates by reversing those roles
Hookup: One system sends input to another system but also sends input to external entities

8.4.5. Take Grant Model

Dictate how rights can be passed from one subject to another or from a subject to object.
Take rule: Allows subject to take rights over object
Grant rule: Allows subject to grant rights to object
Create rule: Allows subject to create new rights
Remove rule: Allows subject to remove rights it has

8.4.6. Access Control Matrix

It is a table of subjects and objects that indicates the actions that each subject can perform on object
Each column of the matrix is an ACL and each row is capabilities list
ACL is tied to object while capability list is tied to subject

8.4.7. Lattice-Based Access Control

Defined upper and lower bound
Subjects are assigned positions in a lattice that define security labels/classifications
Subjects can access only those objects that fall into the range
A subject that falls between private and sensitive can access public & sensitive but not private, proprietary, or confidential data

8.4.8. Bell-LaPadula Model

Maintaining the confidentiality of objects
Based on state machine concept and the information flow model.
It employs mandatory access controls and the lattice concept.
There are three basic properties of this state machine:

Simple Security Property: no read up
* (star) Security Property: no write down. Confinement Property
Discretionary Security Property: uses access matrix to enforce discretionary access control

Exception: a *trusted subject* is not constrained by * Security Property in de/re-classification
Trusted subject: subject guaranteed not to consummate a security-breaching even if it is possible

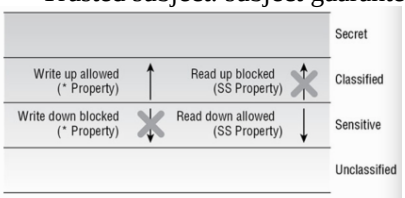


FIGURE 8.3 The Bell-LaPadula model

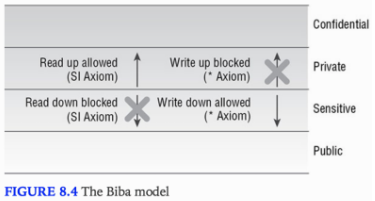


FIGURE 8.4 The Biba model

8.4.9. Biba Model

Biba model addresses integrity
Built on a state machine concept, based on information flow, and is a multilevel model.
The basic properties or axioms of the Biba model state machine:

- Simple Integrity Property no read-down
- * (star) Integrity Property no write-up

Bell-LaPadula and Biba requires that all subjects and objects have a classification label

8.4.10. Clark-Wilson Model

Approach to enforcing data integrity.
It defines each data item and allows modifications through a small set of programs
It uses a three-part relationship of subject/program/object known as access control triple
Subjects do not have direct access to objects. Objects can be accessed only through programs.
It uses of two principles: well-formed transactions and separation of duties

Constrained data item (CDI) data item whose integrity is protected
Unconstrained data item (UDI) data item that is not controlled
Integrity verification procedure (IVP) procedure that scans data items and confirms their integrity
Transformation procedures (TPs) procedures that are allowed to modify a CDI

8.4.11. Brewer and Nash Model (Chinese Wall)

Access controls change dynamically based on user's activity (kind of state machine model)
Applies to single integrated database; build on notion of conflict of interest

X works at C, has access to data for A, should not be allowed access to similar data for B

Uses the principle of data isolation

8.4.12. Goguen-Messeguer Model

Integrity model that is said to be the foundation of noninterference conceptual theories

Based on predetermining the set/domain; a list of objects that a subject can access.
This model is based on automation theory and domain separation.
Subjects are grouped in domain and are unable to interfere with each other's activities

8.4.13. Sutherland Model

It is an integrity model and focuses on preventing interference in support of integrity
Based on state machine and the information flow model.
Does not directly indicate specific mechanisms but on the idea of defining a set of system states, initial states, and state transitions. Through the use of only these predetermined secure states, integrity is maintained and interference is prohibited.
It is use to prevent a covert channel

8.4.14. Graham-Denning model

It is focused on secure creation and deletion of both subjects and objects.
Eight primary protection rules
- Securely create object/subject
- Securely delete object/subject
- Securely provide the read/grant/delete/transfer access right

Abilities/permissions of a subject over objects is defined in access control matrix

8.5. Security Controls based on Systems Requirements

Rainbow Series: series of information security standards that specify minimum acceptable security criteria

8.5.1. TCSEC Classes and Required Functionality *TCSEC*

was repealed and replaced by the Common Criteria TCSEC –
Trusted Computer System Evaluation Criteria

Category A Verified protection. The highest level of security.
Category B Mandatory protection.
Category C Discretionary protection.
Category D Minimal protection. Systems that have been evaluated but do not belong to any

Discretionary Protection (Categories C1, C2)

Provides basic access control
C1 & C2 provide basic controls, complete documentation for system installation/configuration *Discretionary Security Protection (C1):* access control by user IDs and/or groups. *weak protection Controlled Access Protection (C2)*: stronger than C1. Users identified individually. Enforce media cleansing

Mandatory Protection (Categories B1, B2, B3)

Labeled Security (B1): each subject and each object has a security label
Structured Protection (B2): ensure no covert channel. Operator/admin function separate, process isolation
Security Domains (B3) further increases separation/isolation of unrelated processes. Check unused code.

Verified Protection (Category A1)

Development cycle controlled using formal methods; each phase documented/evaluated/verified

8.5.2. Red Book

Orange Book applies only to stand-alone computers not attached to a network.
Red Book interpret TCSEC in a networking context. Functions of the Red Book:
- Rates confidentiality and integrity
- Addresses communications integrity
- Addresses denial of service protection
- Addresses compromise protection and prevention
- Is restricted to "centralized networks with a single accreditation authority"
- Uses only four rating levels: None, C1 (Minimum), C2 (Fair), and B2 (Good)

8.5.3. ITSEC Classes and Required Assurance

ITSEC: Information Technology Security Evaluation Criteria
Functionality rating: states how well system performs all necessary functions based on its design
Assurance rating: degree of confidence that the system will work in a consistent manner
ITSEC uses two scales to rate functionality and assurance
The functionality rated from F-D through F-B3 (no F-A1). The assurance rated from E0 through E6.

Difference between TCSEC and ITSEC

TCSEC – confidentiality; ITSEC – CIA
ITSEC does not rely on the notion of a TCB
TCSEC required any changed systems be reevaluated anew
ITSEC does not require a new formal evaluation

TABLE 8.4 Comparing security evaluation standards

TCSEC	ITSEC	CC description	
D	F-D+E0	EAL0, EAL1	Minimal/no protection
C1	F-C1+E1	EAL2	Discretionary security mechanisms
C2	F-C2+E2	EAL3	Controlled access protection
B1	F-B1+E3	EAL4	Labeled security protection
B2	F-B2+E4	EAL5	Structured security protection
B3	F-B3+E5	EAL6	Security domains
A1	F-B3+E6	EAL7	Verified security design

8.5.4. Common Criteria

The objectives of CC

Add confidence in security products
To eliminate duplicate evaluations
To keep evaluations/certification cost effective/efficient
To make sure evaluations of IT products is high standards
To promote evaluation and increase availability of evaluated products
To evaluate the functionality and assurance of the TOE

Security audits, communications, cryptographic support, user data protection, identification and authentication, security management, TOE security functions, resource utilization, and trusted paths.
Covers the complete range of security functions

Covers assurance requirements for TOEs in areas of configuration management, delivery and operation, development, guidance documents, and lifecycle support plus assurance tests and vulnerability assessments.
Covers the complete range of security assurance checks and protects profiles

Not sure how users act on data is secure
Do not address administrative issues outside the specific purview of security
Do not include evaluation of security in situ (controls related to personnel, organizational practices)
EMI are not addressed, nor are the criteria for rating strength of cryptographic algorithms

Level	Assurance level	Description
EAL1	Functionally tested	Confidence in correct operation but threats to security is not serious. Due care has been exercised
EAL2	Structurally tested	Delivery of design information and test results are in good commercial practices. Low to moderate level security. Relevant in legacy systems
EAL3	Methodically tested and verified	Security engineering begins at the design stage and is carried through without substantial subsequent alteration. Moderate level of assured security, thorough investigation of TOE and its development.
EAL4	Methodically designed, tested and verified	Rigorous, positive security engineering and good commercial development practices are used. It involves independent testing of all TOE security functions.
EAL5	Semi-formally designed and tested	Uses rigorous security engineering and commercial development practices, including specialist security engineering techniques. High level of assured security in a planned development approach, followed by rigorous development.
EAL6	Semi-formally designed, tested and verified	Uses direct, rigorous security engineering techniques at all phases of design, development, and testing to produce a premium TOE. Applies when TOEs for high-risk situations are needed, where the value of protected assets justifies additional cost. Extensive testing reduces risks of penetration, probability of covet channels, and vulnerability to attack.
EAL7	Formally designed, tested, and verified	Used only for highest-risk situations or where high-value assets are involved. This is limited to TOEs where tightly focused security functionality is subject to extensive formal analysis and testing.

8.5.5. International Security Guidelines

ISO defines standards for industrial and commercial equipment, software, protocols, and management, among others. It issues six main products: International Standards, Technical Reports, Technical Specifications, Publicly Available Specifications, Technical Corrigenda, and Guides.

8.6. Certification and Accreditation

8.6.1. Certification

The first phase in a total evaluation process is certification.
Certification is the comprehensive evaluation of the technical and nontechnical security features of an IT system and other safeguards to establish the extent to which a particular design and implementation meets a set of specified security requirements.

System certification is the technical evaluation of each part of a computer system to assess its concordance with security standards.

Choose evaluation criteria.

Analyze/assess each system component to determine whether it satisfies the desired security goals.

Includes testing hardware, software, and configuration.

Evaluate all controls; administrative, technical, and physical

Evaluate the results to determine the security level the system supports in its current environment.

When all factors are evaluated and the level of security is determined, certification phase is complete

8.6.2. Accreditation

In certification phase, test and document security capabilities in a specific configuration

Management compares the capabilities to the needs of organization.

Management reviews certification information and decides if it satisfies the security needs

If management decides the certification of the system satisfies their needs, the system is accredited.

Accreditation is the formal declaration by the designated approving authority (DAA)

Certification is an internal verification of security. Accreditation is performed by a third-party testing service, and everyone in the world who trusts the specific testing group involved trusts the results.

8.6.3. Certification and Accreditation Systems

Phase 1: **Definition** assign project personnel; document mission need; and registration, negotiation, and creation of System Security Authorization Agreement (SSAA) that guides entire process

Verification refine SSAA, systems development activities, and a certification analysis

Validation further refine SSAA, certification evaluation of the integrated system, development of a recommendation to the DAA, and the DAA's accreditation decision

Post Accreditation maintenance of SSAA, system operation, change management, compliance validation Three types of accreditation that may be granted

System accreditation a major application or general support system is evaluated

Site accreditation the applications and systems at a specific, self-contained location are evaluated

Type accreditation application/system that is distributed to number of different location is evaluated

8.7. Security Capabilities of Information System

Include memory protection, virtualization, TPM, interfaces, and fault tolerance

8.7.1. Memory Protection

Isolation, virtual memory, segmentation, memory management, and protection rings Meltdown exploitation allows reading of private kernel memory contents by a non-privileged process Spectre can enable the wholesale theft of memory contents from other running applications

8.7.2. Virtualization

Used to host one or more OS within the memory of a single host computer.

Able to launch individual instances of servers or services as needed, real-time scalability

8.7.3. Trusted Platform Module

A cryptoprocessor chip on a mainboard to store/process cryptographic keys for hard drive encryption

If hard drive is removed from system, it cannot be decrypted. A TPM is example of HSM.

A hardware security module (HSM) is a cryptoprocessor used to manage/store digital encryption keys, accelerate crypto operations, support faster digital signatures, and improve authentication.

An HSM is an add-on adapter/peripheral/TCP/IP network device

HSMs include tamper protection to prevent misuse

HSMs provide an accelerated solution for large (2,048+ bit) asymmetric encryption calculations and a secure vault for key storage

Used by: CA systems; ATM and POS bank terminals; hardware SSL accelerators; and DNSSEC

8.7.4. Interfaces

A constrained/restricted interface restricts what users can do/see based on their privileges.

Practical implementation of the Clark-Wilson model

8.7.5. Fault Tolerance

The ability of a system to suffer a fault but continue to operate. RAID, failover cluster

It avoids single points of failure and the implementation of redundancy

Security Vulnerabilities, Threats, and Countermeasures

9.1. Assess and Mitigate Security Vulnerabilities

Computer architecture is concerned with design/construction of computing systems at a logical level

The more complex a system, the less assurance it provides.

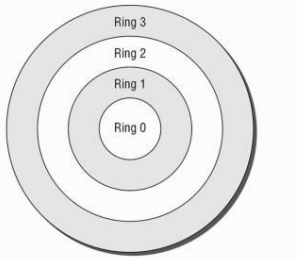
Multitasking: Multitasking is handling two or more application/tasks simultaneously. Managed by OS
A single-core multitasking system is able to juggle more than one process at any given time
Multicore: Multiple processors
Multiprocessing: use of more than one processor to increase computing power.
Database receives many queries; it might send each query to a separate processor for execution
Symmetric Multiprocessing (SMP) a single computer with multiple processors that are treated equally
Processors share not only a common OS but also a common data bus and memory resources
Systems may use a large number of processors
Processes simple operations at extremely high rates
Massively Parallel Processing (MPP): serves computationally intensive operations, scientific research
Systems house hundreds or even thousands of processors, each with own OS and memory/bus
Suited for processing very large, complex, computationally intensive tasks
Multiprogramming
The pseudo-simultaneous execution of two tasks on a single processor
When one process stops to wait, its state is saved and the next process in line begins to process.
Multiprogramming vs. Multitasking
Multiprogramming usually takes place on mainframes, whereas multitasking takes place on PC
Multitasking is normally coordinated by OS, multiprogramming requires specially written software
Multithreading
Multithreading permits multiple concurrent tasks to be performed within a single process
– A thread is a self-contained sequence of instructions that can execute in parallel with other threads that are part of the same parent process.
In multithreading, switching between threads incurs far less overhead
E.g. multiple documents are opened at the same time in word
Processing Types
Single State
Systems require use of policy mechanisms to manage information at different levels.
A processor/system handle only one security level at a time.
The burden of protecting the information is on admin who control access to the system
Multistate
Handles multiple security levels simultaneously
Technical mechanisms prevent information from crossing between the two users

9.2. Protection Mechanism

Protection rings, Operational states, and Security modes.

9.2.1. Protection Rings

The essence of the ring model lies in *priority, privilege, and memory segmentation.*
Higher-number process must ask driver in lower-numbered ring for services;
mediated-access model
Driver/handler request is **system call**

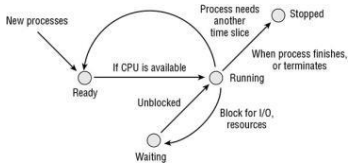


Ring 0: OS Kernel/Memory (Resident Components)
Ring 1: Other OS Components
Ring 2: Drivers, Protocols, etc.
Ring 3: User-Level Programs and Applications

Rings 0–2 run in supervisory or privileged mode.
Ring 3 runs in user mode.

9.2.2. Operational States

The problem state not because problems are guaranteed to occur but because the unprivileged nature of user access means that problems can occur and the system must take appropriate measures to protect security, integrity, and confidentiality.



9.2.3. Security Modes of Operation

The mode of operation describes the security conditions under which the system actually functions.
Determining the mode the operating system should be working in
– The types of users connecting to the system
– The type of data (classification levels, compartments, and categories) processed
– The clearance levels, need-to-know, and formal access approvals the users will have

9.3. Security Mode

Dedicated Mode: single classification level
System High Mode: single classification level
Compartmented Mode: various classification level
Multilevel Mode: various classification level

	Signed NDA for	Proper clearance for	Formal access approval for	A valid need-to-know for
Dedicated security mode	ALL information on the system	ALL information on the system	ALL information on the system	ALL information on the system
System high-security mode	ALL information on the system	ALL information on the system	ALL information on the system	SOME information on the system
Compartmented security mode	ALL information on the system	ALL information on the system	SOME information on the system	SOME information on the system
Multilevel security mode	ALL information on the system	SOME information on the system	SOME information on the system	SOME information on the system

9.4. Operating Modes

User Mode

CPU allows execution of only a portion of its full instruction set.
Processes are executed in controlled environment called a virtual machine

Privileged Mode

Access to full range of instructions
Privileged mode, Supervisory mode, System mode, Kernel mode
Concept: this mode grants a wide range of permissions to the process executing on the CPU

9.5. Memory

9.5.1.ROM

Memory the PC can read but can't change (no writing allowed).
The contents are burned in at factory. Often contain *bootstrap* information (power-on self-test)
Extremely desirable for orchestrating a computer's innermost workings

9.5.2. Programmable Read-Only Memory (PROM)

It allows an end user to burn in the chip's contents later
- Once data is written no further changes are possible

Used where custom functionality is necessary but seldom changes once programmed

9.5.3. Erasable Programmable Read-Only Memory (EPROM)

UVEPROM: can be erased with a light.
EEPROM: uses electric voltages delivered to the pins of the chip to force erasure **9.5.4. Flash Memory**

Flash memory is a derivative concept from EEPROM.
It is a nonvolatile form of storage media that can be electronically erased and rewritten.
EEPROM must be fully erased to rewrite, flash memory can be erased and written in blocks or pages
Common type is NAND flash
Memory cards, thumb drives, mobile devices, and SSD

NOTE: *WORM: Write once read multiple times. CD/DVD*

9.5.5.RAM

Cache RAM:

Taking data from slower devices and temporarily storing it in faster devices
The processor normally contains an onboard cache of extremely fast memory L1, L2, L3, L4

Static RAM vs Dynamic RAM

Dynamic RAM uses a series of capacitors. Frequent refresh is required
Static RAM uses a flip-flop: Imposes no CPU overhead
Dynamic is cheaper than static RAM, static RAM runs much faster than dynamic RAM

9.5.6. Registers

A memory in CPU that ALU uses when performing calculations or processing instructions
Any data ALU is to manipulate must be loaded to a register unless directly supplied as instruction
Operates in lockstep with the CPU at typical CPU speeds

9.6. Memory Addressing

Registers Addressing Mov DX, EBX
Immediate Addressing data is supplied. Add DX, 50
Direct Addressing: actual address of the memory location to access
Indirect Addressing: Memory address supplied contains another memory location
Base+Offset Addressing: MOV CL, BYTE_TABLE[2]

9.7. Secondary Memory

Virtual memory: special type of secondary memory OS manages to act just like real memory
Common virtual memory is pagefile
Memory functions in nanoseconds, disk systems in microseconds

9.8. Security Issues

9.8.1. Primary Memory Security Issues

Cold boot attack: attack that freezes memory chips to delay the decay
HDD Decryption: attack that focuses on image/crash dumps to extract encryption keys

9.8.2. Random vs Sequential Access

Random Access Storage:
- RAM, secondary storage devices, CD and DVD

Sequential Access Storage: Magnetic tape drive

9.8.3. Security Issues in Secondary Storage

Data remanence

SSD wear leveling: often blocks of data that are not marked as "live" but that hold a copy of the data

Prone to theft. Full disk encryption

9.8.4. I/O Devices Security Issue: Monitor

CRT monitors prone to radiate, LCD monitors leak much less

EMI can be read from a distance

Shoulder surfing is a concern for desktop displays, notebook displays, tablets, and mobile phones.

9.8.5. I/O Devices Security Issue: Keyboards/Mice

Vulnerable to TEMPEST monitoring

Keyboards are vulnerable to key-logger

Radio signals can be intercepted

9.8.6. I/O Devices Security Issue: Firmware

BIOS and UEFI

The process of updating the BIOS is known as "flashing the BIOS."

Phlashing attack: malicious BIOS/firmware is installed that introduces remote control or other malicious features into a device.

Unified Extensible Firmware Interface (UEFI) is a more advanced interface between hardware and the operating system, which maintains support for legacy BIOS services.

9.9. Client Based Systems: Applets

Benefits of Applets

The processing burden is shifted to the client

In a properly programmed applet, the web server does not receive any data provided to the applet as input, therefore maintaining the security and privacy of the user's financial data.

However, just as with agents, applets introduce a number of security concerns.

They allow a remote system to send code to the local system for execution

Ensure that code sent to client systems is safe and properly screened for malicious activity

Unless code is analyzed line by line, user can never be certain it doesn't contain a Trojan horse

Java Applets: developed by Sun Microsystems (owned by Oracle)

ActiveX Controls: Implemented using Visual Basic, C, C++, and Java

ActiveX proprietary Microsoft technology execute only on Microsoft browsers

Second, ActiveX controls are not subject to the sandbox restrictions placed on Java applets. They have full access to the Windows operating environment and can perform a number of privileged actions.

9.9.1. Local Caches

A local cache is anything that is temporarily stored on the client for future reuse.

Local caches: ARP, DNS, and internet files cache

ARP cache poisoning

DNS cache poisoning MitM attack. (hosts poisoning, authorized DNS server attacks, caching DNS server attacks, DNS lookup address changing, and DNS query spoofing.)

Solution

Apply patch, HIDS, NIDS, review logs of DNS/DHCP/network

Use a split-DNS system (split-horizon DNS, split-view DNS, and split-brain DNS).

9.10. Server-Based Systems

Data flow is the movement of data between processes/devices/across a network/over channels.

Management of data flow ensures efficient transmission with minimal delays, reliable throughput using hashing and confidentiality protection with encryption.

Data flow control also ensures that receiving systems are not overloaded with traffic

Load balancer technique: random choice, round robin, load/utilization monitoring, and preferencing

A denial-of-service attack can be a severe detriment to data flow control

9.11. Database Systems Security

Aggregation

Aggregation attacks: collect numerous low security items & combine them to create high value

Strict control access and assessment of potential information is required

Inference

Inference attacks: combining several pieces of non-sensitive information to gain access to information that should be classified at a higher level

– Inference makes use of the human mind's deductive capacity rather than the raw mathematical ability of modern database platforms

As with aggregation, the best defense is to maintain constant vigilance over user's permissions

Blurring of data may be used

Partition database to help subvert these attacks

Data Mining and Data Warehousing

Data warehouses: stores large amounts of information from a variety of databases for use with specialized analysis techniques

These data warehouses often contain detailed historical information not normally stored in production databases because of storage limitations or data security concerns.

A data dictionary is commonly used for storing critical information about data, including usage, type, sources, relationships, and formats.

DBMS software reads data dictionary to determine access rights for users

Data mining techniques allow analysts to comb through data warehouses and look for potential correlated information.

Data mining uses mathematical approaches to analyze data, searching for patterns that predict future activity.

Metadata is data about data. It is stored in a secure container known as **data mart**

Significance of Data warehouses

First, data warehouses contain large amounts of potentially sensitive information vulnerable to aggregation and inference attacks, and security practitioners must ensure that adequate access controls and other security measures are in place to safeguard this data. Second, data mining can be used as a security tool when it's used to develop baselines for statistical anomaly–based intrusion detection systems.

9.11.1. Data Analytics

It is the science of raw data examination with focus of extracting useful information out of bulk set

– The results could focus on important outliers, a summary of all data items, or some focused extraction and organization of interesting information

Big data is collections of data that traditional means of analysis or processing are ineffective, inefficient, and insufficient.

9.12. Large Scale Parallel Data Systems

Parallel data systems/computing is computation system designed to perform numerous calculations

Implementation is based on the idea that some problems can be solved efficiently if broken into smaller tasks that can be worked on concurrently

Also concerned with performance, power consumption, and reliability/stability issues

Asymmetric Multiprocessing (AMP), the processors are often operating independently of each other

Symmetric Multiprocessing (SMP), the processors each share a common OS and memory

9.13. Cloud-Based Systems and Cloud Computing

The hypervisor, also known as the virtual machine monitor (VMM), is the component of virtualization that creates, manages, and operates the virtual machines.

The computer running the hypervisor is known as the host OS, and the OSs running within a hypervisor-supported virtual machine are known as guest Oss.

A type I hypervisor is a native or bare-metal hypervisor. There is no host OS

A type II hypervisor is a hosted hypervisor. There is host OS.

Elasticity refers to flexibility of virtualization & cloud solutions to expand/contract based on need

A hosted solution is a deployment concept where the organization must license software and then operates and maintains the software. The hosting provider owns, operates, and maintains the hardware that supports the organization's software.

A cloud access security broker (CASB) is a security policy enforcement solution. The goal is to enforce and ensure that proper security measures are implemented between cloud solution and a customer organization.

Security as a service (SECaaS) is a cloud provider concept in which security is provided

The purpose is to reduce the cost and overhead of implementing and managing security

The cloud shared responsibility model is concept that when an organization uses a cloud solution, there is a division of security and stability responsibility between the provider and the customer.

9.13.1. Grid Computing

Grid computing is a form of parallel distributed processing that loosely groups a significant number of processing nodes to work toward a specific processing goal.
Uses: projects seeking out intelligent aliens, performing protein folding, predicting weather, modeling earthquakes, planning financial decisions, and solving for primes
The biggest security concern with grid computing is that the content of each work packet is potentially exposed to the world
It often uses a central primary core of servers to manage the project, track work packets, and integrate returned work segments

- If central servers are overloaded/go offline, complete failure/crashing of the grid can occur

9.13.2. Peer to Peer

Security concerns with P2P solutions include a perceived inducement to pirate copyrighted materials, the ability to eavesdrop on distributed content, a lack of central control/oversight/management/filtering, and the potential for services to consume all available bandwidth.

9.13.3. IoT

The security issues related to IoT are about access and encryption. One possible secure implementation is to deploy a distinct network for the IoT equipment, which is kept separate and isolated from the primary network. This configuration is often known as the three dumb routers.

9.14. Industrial Control Systems

An industrial control system (ICS) is a form of computer-management device that controls industrial processes and machines. ICSs are used across a wide range of industries, including manufacturing, fabrication, electricity generation and distribution, water distribution, sewage processing, and oil refining. There are several forms of ICS, including distributed control systems (DCSs), programmable logic controllers (PLCs), and supervisory control and data acquisition (SCADA).

9.15. Web Based Vulnerability

Structured Query Language (SQL) injection, Lightweight Directory Access Protocol (LDAP), XML injection, command injection, Hypertext Markup Language (HTML) injection, code injection, and file injection
Mitigation

Perform input validation: limiting the length of input, filtering on known malicious content patterns, and escaping metacharacters.
Limit account privileges

9.15.1. XSS

Maintain patched web server, use WAF/HIDS, audit suspicious activity, performing server-side input validation for length, malicious content, and metacharacter filtering

9.15.2. XFRF

Web Administrator: Require confirmations/reauthentication whenever a sensitive action is requested ○
Like reenter password, sending a code via sms/email, phone call–based verification, or solving CAPTCHA
Add a randomization string (called a nonce) to each URL request and session establishment and to check the client HTTP request header referrer for spoofing
End users: run anti-malware scanners; use HIDS; run a firewall; avoid nonmainstream websites; always logging off from sites instead of closing the browser, closing the tab, or moving on to another URL; keeping browsers patched; and clearing out temporary files and cached cookies regularly.

9.16. Mobile System – Assess and Mitigate and BYOD Concerns

Mobile System – Access and Mitigate	BYOD Concerns

• Full Device Encryption • Remote Wiping • Lockout • Screen Locks • GPS • Application Control: Limits application installed • Storage Segmentation • Asset Tracking • Inventory Control: Hardware asset tracking • Mobile Device Management (MDM) • Disable Unused Feature • Removable Storage: Mobile as removable storage	• Data Ownership • Support Ownership • Patch Management • Antivirus Management • Forensics • Privacy • On-boarding/Off-boarding • Adherence to Corporate Policies • User Acceptance • Architecture/Infrastructure Considerations • Legal Concerns • Acceptable Use Policy • On-board Camera/Video

COPE company-owned, personally enabled: organization's device, user customize & use for work/personal
CYOD choose your own device: provides user list of approved device. Implemented as BYOD/COPE
Corporate-owned mobile strategy: company's mobile device that cannot be used for personal use

9.17. Embedded Devices and Cyber-Physical Systems

Examples of embedded systems include network-attached printers, smart TVs, HVAC controls, smart appliances, smart thermostats, vehicle entertainment/driver assist/self-driving systems, and medical devices.

Cyber-physical systems: devices that offer computational means to control thing in physical world Methods of Securing Embedded and Static Systems

Network Segmentation, Security Layers, Application Firewalls, Manual Updates, Firmware Version Control, Wrappers, Monitoring, Control Redundancy and Diversity

9.18. Essential Security Protection Mechanisms

The need for security mechanisms: software should not be trusted.
Third-party software is inherently untrustworthy, no matter who or where it comes from.
Technical mechanisms are the controls that system designers can build right into their systems.
layering, abstraction, data hiding, process isolation, and hardware segmentation

9.19. Common Security Issue

Covert Channels: A covert channel is a method that is used to pass information over a path that is not normally used for communication.

Covert Timing Channel conveys information by altering the performance of a system component or modifying a resource's timing in a predictable manner. Using a covert timing channel is generally a method to secretly transfer data and is very difficult to detect.

Covert Storage Channel conveys information by writing data to a common storage area where another process can read it. When assessing the security of software, be diligent for any process that writes to any area of memory that another process can read.

9.20. Attacks Based on Design or Coding Flaws

Trusted Recovery: ensures that all security controls remain intact in the event of a crash.
Input and Parameter Checking: Proper data validation is the only way to do away with buffer overflows.

9.20.1. Incremental Attacks

Some forms of attack occur in slow, gradual increments rather than through obvious or recognizable attempts

Data diddling: an attacker makes small, random, or incremental changes to data during storage, processing, input, output, or transaction rather than obviously altering file contents or damaging or deleting entire files.

The salami attack is more mythical. The name of the attack refers to a systematic whittling at assets in accounts or other records with financial value, where very small amounts are deducted from balances regularly and routinely.

9.20.2. Maintenance Hooks and Privileged Programs

Maintenance hooks are entry points into a system that are known only by the developer of the system. Such entry points are also called back doors.

Another common system vulnerability is the practice of executing a program whose security level is elevated during execution. Such programs must be carefully written and tested.

9.20.3. Technology and Process Integration

As systems are integrated, attention should be paid to potential single points of failure as well as to emergent weaknesses in service-oriented architecture (SOA).

An SOA constructs new applications or functions out of existing but separate and distinct software services. The resulting application is often new; thus, its security issues are unknown, untested, and unprotected. All new deployments, especially new applications or functions, need to be thoroughly vetted before they are allowed to go live into a production network or the public internet.

9.20.4. Programming

- programmer fails to check or sanitize the format and/or the size of input data.

Timing, State Changes, and Communication Disconnects

9.20.5. Electromagnetic Radiation

The easiest way to eliminate electromagnetic radiation interception is to reduce emanation through cable shielding or conduit and block unauthorized personnel and devices from getting too close to equipment or cabling by applying physical security controls.

A Faraday cage is a special enclosure that acts as an EM capacitor. When a Faraday cage is in use, no EM signals can enter or leave the enclosed area.

Jamming or noise generators it is difficult to retrieve a signal when there is too much interference. o The only issue with jamming concept is that you have to ensure that the interference won't affect the normal operations of your devices.

9.20.6. Timing, State Changes, and Communication Disconnects

The common sequence of events for an algorithm is to check that a resource is available and then access it if you are permitted.

The time of check (TOC) is the time at which the subject checks on the status of the object. There may be several decisions to make before returning to the object to access it. When the decision is made to access the object, the procedure accesses it at the time of use (TOU).

The difference between the TOC and the TOU is sometimes large enough for an attacker to replace the original object with another object that suits their own needs.

Time of check to time of use (TOCTOU) attacks is often called race conditions because the attacker is racing with the legitimate process to replace the object before it is used.

A classic example of a TOCTTOU attack is replacing a data file after its identity has been verified but before data is read. By replacing one authentic data file with another file of the attacker's choosing and design, an attacker's choosing and design, an attacker can potentially direct the actions of a program in many ways. Of course, the attacker would have to have in-depth knowledge of the program and system under attack.

10. Physical Security Requirements

Without physical security other controls are inadequate

Physical controls are your first line of defense, and people are your last

Secure Facility Plan

A secure facility plan is developed through a process known as critical path analysis

Critical path analysis identifies relationships between mission-critical applications, processes, and operations and all the necessary supporting elements

Once that analysis is complete, its results serve as a list of items to secure

Technology convergence: various technologies and systems to evolve and merge over time and leads to single point of failure

A requirement of security is first. Then cost, location, and size

Other thing that influence site selection are

Site location and construction, Proximity to other buildings and businesses, Proximity to emergency-response personnel, building design, visibility, prone to natural disaster

Crime Prevention through Environmental Design (CPTED): structure the physical environment and surroundings to influence individual decisions that potential offenders make before committing any criminal acts

Administrative physical security controls: facility construction and selection, site management, personnel controls, awareness training, and emergency response

Technical physical security controls: access controls; intrusion detection; alarms; (CCTV); monitoring; HVAC, power supplies; and fire detection and suppression.

Physical controls for physical security: fencing, lighting, locks, construction materials, mantraps, dogs, and guards.

Designing physical security

Deterrence, Denial, Detection, Delay

Equipment Failure

Non-mission-critical situations: know where to purchase for a 48-hour replacement timeline

In other situations, maintaining onsite replacement parts is mandatory.

The response time in returning a system to a fully functioning state is directly proportional to the cost involved in maintaining such a solution

In some cases, maintaining onsite replacements is not feasible. Establish SLA with vendor

Scheduled for replacement and/or repair for aging hardware based on MTTF and MTTR

MTBF is an estimation of the time between the first and any subsequent failures.

Wire distribution room/intermediate distribution facilities (IDF). Element of a cable plant management policy

Do not use closet as a general storage area

Have adequate locks (biometric elements)

Keep the area tidy

Do not store flammable items

Set up video surveillance

Door open sensor to log entries

Regular physical inspections

Include in environmental management and monitoring

A cable plant is collection of interconnected cables (cross-connects, patch panels, and switches) to establish physical network. Elements of a cable plant

Entrance facility (demarcation point), cable from provider connects internal cable plant

Equipment room: main wiring closet connected to or adjacent to the entrance facility

Backbone distribution system: connects equipment and telecom rooms (cross-floor conn.)

Telecommunications room (wiring closet) connection point between BDS and HDS

Horizontal distribution system: between telecom room and work areas, often including cabling, cross-connection blocks, patch panels, and supporting hardware infrastructure (such as cable trays, cable hangers, and conduits)

Centralized server rooms need not be human compatible.

Server rooms be located at the core of the building Avoid ground/top floor & basement

Walls one-hour minimum fire rating

Smartcards: prey to physical/logical attacks, Trojan horse, or social-engineering attacks

Proximity Readers: a passive device, a field-powered device, or a transponder

Access Abuses: security guard to prevent abuse, masquerading, and piggybacking

Electrical devices emanate signals/radiation that can be intercepted

Countermeasures and safeguards are known as TEMPEST countermeasures

Faraday Cage metal skin acts as EMI-absorbing capacitor that prevents emanations. Inside cage, mobile phones, broadcast radio or television stations won't work

White Noise means broadcasting false traffic to mask real emanations

Control Zone: a Faraday cage, white noise or both to protect a specific area

Use locked cabinet, employ a librarian or custodian, use check-in/check-out process

Reusable media: run a sanitization or zeroization when returned

Verify with hash-based integrity check

A dedicated storage system distinct from the production

Keep system offline when not in active use

Block Internet connectivity to and from the storage system

Track all activities

Calculate hashes

Limit access to the security administrator and legal counsel

Encrypt datasets

Restricted and Work Area Security

Confidential assets in the heart or center of protection
Walls or partitions to deter shoulder surfing/eavesdropping
Floor-to-ceiling walls to separate areas sensitive and confidential data
Sensitive Compartmented Information Facility (SCIF) used by Government and military contractors provides a secure environment for highly sensitive data storage and computation
SCIF purpose: store, view, and update sensitive compartmented information (SCI)

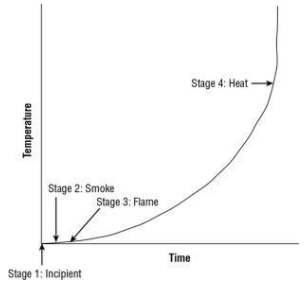
Fault: A momentary loss of power
Blackout: A complete loss of power
Sag: Momentary low voltage
Brownout: Prolonged low voltage
Spike: Momentary high voltage
Surge: Prolonged high voltage
Inrush: An initial surge of power
Noise: A steady interfering power disturbance or fluctuation
Transient: A short duration of line noise disturbance
Clean: Non-fluctuating pure power
Ground: The wire in an electrical circuit that is grounded

Noise

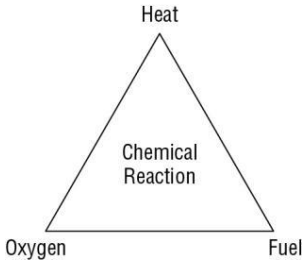
Two types of EMI
- Common mode noise: power difference between the hot (+ve) and ground wires
- Traverse mode noise: power difference between the hot and neutral (-ve) wires

Radio-frequency interference (RFI) affects system as EMI. RFI generator: fluorescent lights, electrical cables, electric space heaters, computers, elevators, motors, and electric magnets
To protect power supply and equipment: provide sufficient power conditioning, establish proper grounding, shield all cables, and limit exposure to EMI and RFI sources

60-75 deg. Fahrenheit (15-23 deg. Celsius)
Humidity between 40 and 60 percent
Too much humidity can cause corrosion.
Too little humidity causes static electricity.
Static voltage
- 40 (Destruction of sensitive circuits)
- 1,000 (Scramble monitor display)
- 1,500 (Destruction of data on HDD)
- 2,000 (abrupt system shutdown)
- 4,000 (printer jam/component damage)
- 17,000 (permanent circuit damage)



Overloaded electrical distribution outlets cause most fires in a datacenter
Different suppression
- Water suppresses the temperature
- Soda acid and other dry powders suppress the fuel supply
- CO2 suppresses the oxygen supply
- Halon substitutes suppress oxygen supply



Stage 1: The Incipient Stage, only air ionization no smoke
Stage 2: The Smoke Stage, smoke visible
Stage 3: The Flame Stage, a flame seen with the naked eye
Stage 4: The Heat Stage, there is an intense heat, everything burns

Class A: Common combustibles (water, soda acid, dry powder or liquid chemical)
Class B: Liquids (CO2, halon, soda acid)
Class C: Electrical (CO2, halon)
Class D: Metal (dry powder)
Water on Class B fires: liquids usually float on water
Water on Class C fires: potential for electrocution
Oxygen suppression not on metal fires because burning metal produces its own oxygen

Fire Detection Systems

Fixed-temperature detection triggers suppression when a specific temperature is reached

Rate-of-rise detection triggers when temperature change reaches a specific level
Flame-actuated triggers based on the infrared (heat) energy of flames
Smoke-actuated use photoelectric or radioactive ionization sensors as trigger
Incipient smoke detection (aspirating sensors) able to detect early stage of combustion

Water Suppression Systems

Wet pipe (closed head system) always full of water. Water discharges immediately
Dry pipe contains compressed air. Once triggered pipes fill and discharges water
Deluge dry pipe with larger pipes (high volume water). Inappropriate for electronics
Preaction combination of dry pipe/wet pipe. Exists as dry pipe until the initial stages of a fire (smoke, heat, and so on) are detected, and then the pipes are filled with water.

Preaction systems are the most appropriate water-based system for environments that house both computers and humans together.

More effective than water discharge systems. Should not be used where people are located
Halon is effective, but it degrades into toxic gases at 900 degrees Fahrenheit
Halon substitute is low-pressure water mists, don't use in computer/electrical equipment
Smoke damaging to storage devices. Heat damages any electronic or computer component
100 deg. Fahrenheit damage storage tapes, 175 deg. damage computer hardware (CPU and RAM), and 350 deg. damage paper products (warping and discoloration)
Suppression media can cause short circuits, initiate corrosion, or render equipment useless

Perimeter Security Control: Single entrances: for security, multiple entrances: for evacuation

Fences, Gates, Turnstiles, and Mantraps

Fences 3 to 4 feet high deter casual trespassers
Fences 6 to 7 feet high deter most intruders, except determined ones
Fences 8+ feet high with three strands of barbed wire deter even determined intruders
A gate is a controlled exit and entry point in a fence
Deterrent level of a gate must be equivalent to the deterrent level of the fence
When not protected by guards, use of dogs or CCTV
Turnstile prevents more than one person at a time and restricts movement in one direction
Mantrap: double set of doors protected by a guard and prevents piggybacking/tailgating

Lightening

Discourages casual intruders
Combine with guards, dogs, CCTV
Illuminate critical areas with 2 foot-candles of power

Guards are able to adapt and react to situations
Guards are vulnerable to social engineering
Guards are unaware of the scope of the operations
Security guards are expensive.
Dogs an alternative to guards. Dogs: detection/deterrent. Costly, high maintenance

Internal Security Controls: Keys and Combinations Locks

Key-based (preset locks) common & inexpensive, subject to picking, shimming attack
Programmable/combination locks more control than preset. Electronic access control lock contains
- electromagnet to keep the door closed,
- credential reader to authenticate subjects and to disable the electromagnet, and
- sensor to reengage the electromagnet when the door is closed

Locks an alternative to security guards as a perimeter entrance access control device

Badges, identification cards, and security IDs: Physical and/or electronic access control devices

Motion detector, or motion sensor: device that senses movement or sound

An infrared motion detector monitors for significant changes in the infrared lighting pattern
A heat-based motion detector monitors for significant changes in the heat levels
A wave pattern motion detector transmits a low ultrasonic or high microwave frequency signal and monitors for significant changes or disturbances in the reflected pattern
A capacitance motion detector changes in electrical/magnetic field
A photoelectric motion detector changes in visible light levels. Usually deployed in internal rooms
A passive audio motion detector listens for abnormal sounds

Deterrent Alarms locks, shut doors
Repellant Alarms audio siren/bell & lights on. Discourages attackers from continuing their activities
Notification Alarms often silent but records incident and notify administrators/guards. Catch attacker

Alarms categorized by location: local, centralized or proprietary, or auxiliary

Local Alarm System broadcast audible signal (up to 120 db) heard up to 400 feet away. Protect from tampering and disablement. Guards be present to respond when the alarm is triggered

Central Station System usually silent locally, but offsite monitoring agents are notified

Auxiliary Station if security perimeter is breached, emergency services is notified. Fire, police etc.

Secondary Verification Mechanisms: Reduces false alarm and increases the likelihood of actual intrusion

DOMAIN 4: Communication and Network Security

11. Secure Network Architecture and Securing Network Components

11.1. OSI Model

Communications over networks are made possible by protocols

A protocol is a set of rules and restrictions that define how data is transmitted over a network

Physical Layer

Controls throughput rates, handles synchronization, manages line noise and medium access, and determines whether to use digital/analog signals or light pulses

Electrical specifications, protocols, and interface standards includes

EIA/TIA-232 and EIA/TIA-449, X.21, High-Speed Serial Interface (HSSI), SONET, V.24 and V.35, FHSS, DSSS, PSK, OFDM, QAM

NICs, hubs, repeaters, concentrators, radios, antenna, and amplifiers

Ethernet (IEEE 802.3), Token Ring (IEEE 802.5), ATM, FDDI, and CDDI

Media Access Methods happen here: CSMA, Token Passing, Polling

Some protocols and devices

- SLIP, PPP, ARP, L2F, L2TP, PPTP, ISDN, X.25
- Switches, bridge, Wireless access point, DTEs/DCEs

3-bytes in MAC address denote vendor; known as Organizationally Unique Identifier (OUI)

Network Layer

Adds routing and addressing information to the data and packet includes source and destination IP

ICMP, RIP, OSPF, BGP, IGMP, IP, IPSec, IPX, NAT, SKIP

Manages error detection and node data traffic (traffic control)

Routers and brouters

Alternative to IP at the layer 3

Internetwork Packet Exchange (IPX), AppleTalk, and NetBIOS Extended User Interface (NetBEUI)

Potential security risk firewalls are unable to perform content filtering, must either block all or allow

Routing Protocols

Distance vector routing protocols maintain a list of destination networks along with metrics of direction and distance as measured in hops. RIP, IGRP

Link state routing protocols maintain a topography map of all connected networks and use this map to determine the shortest path to the destination. OSPF, IS-IS

Manages integrity of connection & controls session. Accepts a PDU (data passed between network)

Controls addressing/referencing, establishes connections between nodes & defines session rules

Session rules: data flow, integrity verification, and determine data loss

Session rules established by handshaking process

Includes mechanisms for segmentation, sequencing, error checking, controlling the flow of data, error correction, multiplexing, and network service optimization

TCP, UDP, Sequenced Packet Exchange (SPX), SSL, TLS

Responsible for establishing, maintaining, and terminating communication sessions

It manages dialogue discipline or dialogue control (simplex, half-duplex, full-duplex), establishes checkpoints for grouping and recovery, and retransmits PDUs that have failed or been lost since the last verified checkpoint

NFS, SQL, RPC, NetBIOS, PAP

Responsible for encryption/decryption and compression/decompression

Most file/data formats operate within this layer.

ASCII, EBCDICM, TIFF, JPEG, MPEG, MIDI

Application Layer

HTTP, FTP, LPD, SMTP, Telnet, TFTP, EDI, POP3, IMAP, SNMP, Network News Transport Protocol (NNTP), S-RPC, Secure Electronic Transaction (SET)
Network device: gateway.

- IP-to-IPX gateway takes inbound communications and translates to IPX/SPX for outbound

11.2. TCP/IP Protocol Suite

TCP/IP can be secured using virtual private network (VPN) links between systems.
Protocols used to establish VPNs are PPTP, L2TP, SSH, OpenVPN (SSL/TLS VPNs), and IPSec
Another method to provide protocol-level security is to employ TCP wrappers
An application that serves as basic firewall by restricting access to ports based on IDs
Using TCP wrappers is a form of port-based access control
The TCP is full-duplex connection-oriented protocol, UDP is a simplex connectionless protocol
Socket: combination of IP address and a port. 192.168.2.2:80
The first 1,024 ports (0–1,023) are well-known/service ports
Ports 1,024 to 49151 are registered software ports. Ports 49152 to 65535 are ephemeral ports
Transmission window: Number of packets transmitted in TCP before an acknowledge packet is sent
Sliding windows: mechanism to control data flow.
Larger windows faster data transmission (use on reliable connections where corrupted data is less)
Smaller windows when the communication connection is unreliable
A TCP header is 20 to 60 bytes long. TCP Flag bit are as follows

Flag bit	Name	Description
CWR	Congestion Window Reduced	Used to manage transmission over congested links
ECE	ECN-Echo (Explicit Congestion Notify)	Used to manage transmission over congested links
URG	Urgent	Indicates urgent data
ACK	Acknowledgment	Acknowledges synchronization or shutdown request
PSH	Push	Indicates need to push data immediately to application
RST	Reset	Causes immediate disconnect of TCP session
SYN	Synchronization	Requests synchronization with new sequencing numbers
FIN	Finish	Requests graceful shutdown of TCP session

The IP header protocol field value for TCP is 6 (0x6) and UDP is 17 (0x11).
A UDP header is 8 bytes long. UDP offers no error detection or correction, does not use sequencing, does not use flow control mechanisms, does not use a pre-established session, and is considered unreliable. UDP has very low overhead and thus can transmit data quickly.
TCP header contains: Source Port, Destination Port, Sequence number, Data offset, flags, window size. UDP header contains: Source Port, Destination Port, Message Length and Checksum

Network Layer Protocol and IP

Class	First binary digits	Decimal range
A	0	1–126
B	10	128–191
C	110	192–223
D (Multicasting)	1110	224–239
E (Reserved)	1111	240–255

IPv4 is 32 bits while IPv6 is 128 bits.

Network Layer Protocol: ICMP

Used to determine the health of a network. Utilized by ping, traceroute, pathping, and other network management tools.
Ping of death sends a malformed ping larger than 65,535 bytes
Smurf attacks enormous amounts of traffic on a target network by spoofing broadcast pings
Ping floods DoS attack relying on consuming all of the bandwidth that a target has available.
IP header protocol for ICMP is 1 (0x01)

Type	Function	Type	Function	Type	Function
0	Echo reply	3	Destination unreachable	5	Redirect

8	Echo request	9	Router Advertisement	10	Router solicitation
11	Time exceeded	12	Bad IP header	13	Communication prohibited

Network Layer Protocol: IGMP

Allows systems to support multicasting

IGMP: used by IP hosts to register dynamic multicast group membership. It is also used by connected routers to discover these groups
The IP header protocol field value for IGMP is 2 (0x02).
"Publish and subscribe" model

Telnet, TCP Port 23 supports remote connectivity to execute commands and running applications but does not support transfer of files
FTP, TCP Ports 20 (Passive Data)/Ephemeral (Active Data) and 21 (Control Connection)
TFTP, UDP Port 69 Exchange of files that does not require authentication
SMTP, TCP Port 25
Post Office Protocol (POP3), TCP Port 110
IMAP, TCP Port 143 IMAP is more secure than POP3
HTTP, TCP Port 80
DHCP, UDP Ports 67 and 68. 67 as the destination port on the server to receive client communications and port 68 as the source port for client requests
DNS: TCP port 53 for zone transfers, UDP port 53 for DNS queries
SSL, TCP Port 443
Line Print Daemon (LPD), TCP Port 515 used to spool print jobs
X Window, TCP Ports 6000–6063 GUI API for command-line operating systems
NTP, TCP port 123
LDAP: Port 636 (secure), 389 (unsecure)
Global directory: Port 3269 (secure), 3268 (unsecure)
Diameter: TCP Port 3868
NFS, TCP Port 2049 supports file sharing between dissimilar systems
SNMP, UDP Port 161 (UDP Port 162 for Trap Messages) collects network health and status
RADIUS: UDP 1812 port. TCP 2083 over TLS
Windows File Sharing: 135, 137-139, 445; Microsoft SQL Server: 1433/1434; Oracle: 1521; H.323 1720; PPTP: 1723; L2TP UDP 1701; HP JetDirect Printing: 9100; RIP UDP 520

[Ethernet[IPSec[IP[TCP[SSL[HTTP]]]]]]
Benefits
- A wide range of protocols can be used at higher layers
- Encryption can be incorporated at various layers
- Flexibility and resiliency in complex network structures is supported

Drawbacks
- Covert channels are allowed
- Filters can be bypassed
- Logically imposed network segment boundaries can be overstepped

DNP3

DNP3 (Distributed Network Protocol) used in electric and water utility and management industries
Supports communication between data acquisition systems and the system control equipment
DNP3 is a multilayer protocol and has link, transport, and transportation layers

Record	Description
AAAA	FQDN to IPv6
A	FQDN to IPv4
CNAME	FQDN alias to another FQDN
PTR	IP to FQDN
MX	Mail FQDN to IP
NS (Name server record)	Designates FQDN and IP address of an authorized name server
SOA (start of authority)	Specifies authoritative information about zone file

11.3. Domain Name System

An FQDN consists of three main parts:
- Top-level domain (TLD)—The com in www.google.com
- Registered domain name—The google in www.google.com
- Subdomain(s) or hostname—The www in www.google.com

The total length of an FQDN can't exceed 253 characters (including the dots).
Single section can't exceed 63 characters. FQDNs can only contain letters, numbers, and hyphens

DNSSEC

Provides reliable authentication during DNS operations

The goal is to prevent range of DNS abuses

DNSSEC will significantly reduce server-focused DNS abuses

DNS Poisoning

DNS name to IP resolution process

Check the local cache (which includes content from the HOSTS file).

Send a DNS query to a known DNS server.

Send a broadcast query to any possible local subnet DNS server. (isn't widely supported) DNS queries are not authenticated, but contain a 16-bit QID. A rogue DNS to include QID in the false reply

Perform DNS poisoning. Attack real DNS server and placing incorrect information into its zone file

Alter the HOSTS file

Corrupt the IP configuration can result in a client having a false DNS server definition. This can be accomplished either directly on the client or on the network's DHCP server.

Use proxy falsification works only against web communications

DNS pharming redirects valid URL or IP address to a fake website

Limit zone transfers. Block inbound TCP port 53 and UDP port 53

Limit the external DNS servers from which internal DNS servers pull zone transfers

Deploy NIDS

Properly harden all DNS, server, and client systems

Use DNSSEC

Resolve all domain through internal DNS i.e. block outbound UDP 53, open outbound TCP 53

Domain Hijacking

Domain hijacking/theft is malicious action of changing the registration of a domain name without the authorization of the valid owner

Accomplished by stealing owner's logon credentials, using XSRF, hijacking a session, using MitM, or exploiting a flaw in the domain registrar's systems

Register immediately after original owner's registration expires (domain hijacking). Unethical

11.4. Converged Protocols

Merging of specialty or proprietary protocols with standard protocols

Ability to host special or proprietary services without the need for unique deployments

This can result in significant cost savings

Fibre Channel is a form of SAN/NAS that allows for high-speed file transfers upward of 128 Gbps

FCoE is used to encapsulate Fibre Channel communications over Ethernet networks

It typically requires 10 Gbps Ethernet in order to support the Fibre Channel protocol

Operates as layer 3 protocol, replacing IP as the payload of a standard Ethernet network

Converged Protocols: MPLS (layer 2.5)

A high-throughput high-performance network technology that directs data based on short path labels

Network is not limited to TCP/IP protocols. This enables the use of many other networking technologies, including T1/E1, ATM, Frame Relay, SONET, and Digital Subscriber Line (DSL)

Internet Small Computer System Interface (iSCSI) is a networking storage standard based on IP

Used to enable location-independent file storage, transmission, & retrieval over LAN/WAN/Internet

iSCSI is often viewed as a low-cost alternative to Fibre Channel.

Tunneling mechanism used to transport voice/data over a TCP/IP network

Some are software only, such as Skype. Others more hardware, such as magicJack

VoIP-to-VoIP calls are free, whereas VoIP-to-landline calls are usually charged a per-minute fee

Converged Protocols: SDN

It aims at separating the infrastructure layer (i.e., hardware and hardware-based settings) from the control layer (i.e., network services of data transmission management).

It offers a new network design that is directly programmable from a central location, is flexible, is vendor neutral, and is open-standards based. It is effectively network virtualization.

11.5. Content Distribution Network (CDN)

It is a collection of resource services deployed in numerous data centers across the Internet in order to provide low latency, high performance, and high availability of the hosted content

- Concept of distributed data hosts
- Rather than media content stored in single location is distributed to numerous locations
- This results in a type of geographic and logical load-balancing

- The overall result is lower-latency and higher-quality throughput
- CDN providers CloudFlare, Akamai, Amazon CloudFront, CacheFly, and Level 3 Comm.

Client-based CDN is also possible often referred as P2P (peer-to-peer). BitTorrent

11.6. Wireless System

802.11 (2 Mbps, 2.4 GHz)	802.11a (54 Mbps, 5 GHz)	802.11b (11 Mbps, 2.4 GHz)
802.11g (54 Mbps, 2.4 GHz)	802.11n (200+ Mbps, 2.4 or 5 GHz)	802.11ac (1 Gbps, 5 GHz)

Security Wireless Access Points

Deploy wireless access points configured to use infrastructure mode rather than ad hoc mode.

- Ad hoc mode two wireless devices can communicate without a centralized control authority
- Infrastructure mode wireless access point is required

Within the infrastructure mode

- Stand-alone mode infrastructure WAP connects wireless clients but no any wired resources
- Wired extension mode infrastructure WAP connects wireless clients to the wired network
- Enterprise extended mode infrastructure multiple WAPs are used to connect a large physical area to the same wired network

  Each WAP uses same ESSID while NICs change associations
- Bridge mode infrastructure wireless connection is used to link two wired networks

SSID

ESSID: name of wireless network when WAP is used (i.e., infrastructure mode)
Independent service set identifier (ISSID): name of a wireless network when in ad hoc or P2P mode
In infrastructure mode, the BSSID is the MAC address of the base station to differentiate networks
The SSID is broadcast by the WAP via a special transmission called a beacon frame

Broadcasting of the SSID should be disabled
Use WPA2 as a reliable authentication and encryption solution

Site Survey

The process of investigating the presence, strength, and reach of wireless access points
Involves walking around with a portable wireless device, taking note of the wireless signal strength, and mapping this on a plot or schematic of the building
It is useful for evaluating existing wireless network deployments, planning expansion of current deployments, and planning for future deployments

Methods wireless clients can use to authenticate to WAPs

open system authentication (OSA) and
shared key authentication (SKA)

OSA - no real authentication required. OSA typically transmit everything in clear text
SKA - authentication must take place

Protects against packet sniffing and eavesdropping
Uses predefined shared key, is static and shared among all WAP
The WEP IV is only 24 bits long and is transmitted in plaintext
WEP doesn't check for packet freshness, allows live WEP crack to be successful in 60 seconds

Wi-Fi Protected Access (WPA)

Based on LEAP and TKIP cryptosystems and often employs a secret passphrase for authentication
Brute-force attack possible

It uses a new encryption scheme known as the *Counter Mode Cipher Block Chaining Message Authentication Code Protocol* (CCMP), which is based on the AES encryption scheme
KRACK (Key Reinstallation AttaCK)

802.1x/EAP

Standard port-based network access control to ensure no communication without proper authenticatn
Through the use of 802.1X, other techniques and solutions like RADIUS, TACACS, certificates, smart cards, token devices, and biometrics can be integrated into wireless networks to provide MFA
Extensible Authentication Protocol (EAP) is an authentication framework
EAP allows for new authentication technologies to be compatible with existing wireless technologies

Wireless methods supported LEAP, EAP-TLS, EAP-SIM, EAP-AKA, and EAP-TTLS
EAP-MD5 and a pre-release EAP (LEAP) are crackable

PEAP/LEAP/MAC Filter

Protected Extensible Authentication Protocol (PEAP) encapsulates EAP methods within a TLS tunnel that provides authentication and potentially encryption

Lightweight Extensible Authentication Protocol (LEAP) is a Cisco proprietary alternative to TKIP for WPA. Attack tool Asleap could exploit the ultimately weak protection provided by LEAP.

Avoid LEAP; use of EAP-TLS. If LEAP is used, use complex password

A MAC filter is a list of authorized MAC addresses used by a WAP to block unauthorized devices

TKIP/CCMP

Temporal Key Integrity Protocol (TKIP) was implemented into 802.11 wireless networking under the name WPA (Wi-Fi Protected Access).

TKIP improvements include a key-mixing function that combines the initialization vector (IV) with the secret root key before using that key with RC4 to perform encryption;

A sequence counter is used to prevent packet replay attacks; and a strong integrity check named Michael is used

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) was created to replace WEP and TKIP/WPA.

CCMP uses AES (Advanced Encryption Standard) with a 128-bit key

11.7. Determining Antenna Placement

Use a central location.

Avoid solid physical obstructions.

Avoid reflective or other flat metal surfaces.

Avoid electrical equipment.

External omnidirectional antennas should be positioned pointing straight up vertically.

Directional antenna should point the focus toward the area of desired use.

Wireless signals are affected by interference, distance, and obstructions

Standard straight or pole antenna is an omnidirectional antenna that can send and receive signals in all directions perpendicular to the line of the antenna itself. Also called base or rubber duck antenna

A Yagi (traditional roof TV antennas). Catch specific radio frequencies in direction of the main bar

Cantennas are constructed from tubes with one sealed end. They focus along the direction of the open end of the tube. Some of the first cantennas were crafted from Pringles cans.

Panel antennas are flat devices that focus from only one side of the panel

Parabolic antennas are used to focus signals from very long distances or weak sources

Security standard for wireless networks intended to simplify effort in adding new clients to network.

WPS is enabled by default (Wi-Fi Alliance certification requirement). Disable it

If disable is not possible, upgrade or replace the base station's firmware or replace the whole device

Using Captive Portals

Authentication technique that redirects a newly connected wireless client to access control page

Page requires user to input payment information, provide logon credentials, or input an access code.

Also used to display an acceptable use policy, privacy policy, and tracking policy to the user

Often located on wireless networks implemented for public use, such as at restaurants, airports

General Wi-Fi Security Procedure

Change the default administrator password

Disable the SSID broadcast

Change the SSID to something unique

Enable MAC filtering

Consider using static IP addresses, or configure DHCP with reservations

Turn on the highest form of authentication and encryption supported

Treat wireless as remote access, and manage access using 802.1X

Treat wireless as external access, and separate the WAP from the wired network using a firewall

Treat wireless as an entry point for attackers, and monitor all WAP-to-wired-network with IDS

Require all transmissions between wireless clients and WAPs to be encrypted; require a VPN link

11.8. Wireless Attacks

War Driving

It is an act of using a detection tool to look for wireless networking signals

It is performing a site survey for possibly malicious or unauthorized purposes

War Chalking

It's a way to physically mark an area with information about the presence of a wireless network

A closed circle indicated a closed/secured network, & two back-to-back half circles an open one

Replay

Retransmission of captured communications in the hope of gaining access to the targeted system

Replay attacks can be mitigated by updating the firmware of base station and with wireless-NIDS

IV: Used to increase security by reducing predictability and repeatability

Rogue Access Points

Setting SSID to an alternate name that appears legitimate

if original is "ABCcafe," then the rogue could be "ABCcafe-2," "ABCcafe-LTE,"

The defense against rogue WAPs is to be aware of the correct and valid SSID

Hacker operates a false access point that will automatically clone, or twin, the identity of an access point based on a client device's request to connect

Pay attention to wireless network you connect. Prune unnecessary and old wireless profiles

Secure Network Components

Boosting Performance Network segmentation can improve performance. Systems that often communicate are located in the same segment, while systems that rarely in other segments.

Reducing Communication Problems Network segmentation often reduces congestion and contains communication problems, such as broadcast storms, to individual subsections of the network

Providing Security Network segmentation can also improve security by isolating traffic and user access to those segments where they are authorized

The goals of NAC

Prevent/reduce zero-day attacks

Enforce security policy throughout the network

Use identities to perform access control

The goals of NAC can be achieved through the use of strong detailed security policies

NAC can be implemented with a preadmission/postadmission philosophy, or both:

The preadmission philosophy requires a system to meet all current security requirements before it is allowed to communicate with the network

The postadmission philosophy allows and denies access based on user activity, which is based on a predefined authorization matrix

11.9. Firewall

Static Packet-Filtering

Filters traffic by examining data from a message header.

Rules are concerned with source, destination, and port addresses.

Unable to provide user authentication and it is easily fooled with spoofed packets.

Known as first-generation firewalls; they operate at layer 3

They can also be called screening routers.

Filters traffic based on the internet service used to transmit or receive the data

Negatively affects network performance

Known as second-generation firewalls, and operate at the layer 7

Used to establish communication sessions between trusted partners. Operate at the layer 5

SOCKS (from Socket Secure, as in TCP/IP ports) is a common implementation

Also known as circuit proxies, manage communications based on the circuit, not on traffic content

They permit/deny forwarding decisions based on socket

Considered second-generation firewalls

Stateful Inspection Firewalls (also known as dynamic packet filtering firewalls)

It evaluates the state or the context of network traffic. Source/destination IP, application usage, source of origin, & relationship between current and previous packets of the same session etc.

It generally operate more efficiently than application-level gateway firewalls.

Known as third-generation firewalls, and operate at layers 3 and 4

Operates at application layer in order to filter the payload contents of a communication

It can also be known as complete packet inspection and information extraction (IX).

It is able to block domain names, malware, spam, or other identifiable elements in the payload of a communication.

Kernel Proxy Firewall

Considered a fifth-generation firewall and operates at application layer

It creates dynamic, customized network stacks when a packet needs to be evaluated.

A new virtual network stack is created, which is made up of only the protocol proxies necessary to examine this specific packet properly. If it is an FTP packet, then the FTP proxy is loaded in the stack. The packet is scrutinized at every layer of the stack.

Next-Gen Firewalls

It is a multifunction device (MFD). Can include IDS, IPS, a TLS/SSL proxy, web filtering, QoS management, bandwidth throttling, NATing, VPN anchoring, and antivirus

etc. **Multihomed firewall**

Multihomed devices are commonly used to house firewall software

It must have at least two interfaces to filter traffic (dual-homed firewalls). All multihomed firewalls should have IP forwarding disabled. This will force the filtering rules to control all traffic rather than allowing a software-supported shortcut between one interface and another.

When a packet comes to the external NIC from an untrusted network on a firewall and the operating system has forwarding enabled, the operating system will forward the traffic instead of passing it up to the firewall software for inspection.

Bastion Host

A bastion host is a computer or appliance that is exposed on the internet and has been hardened by removing all unnecessary elements, such as services, programs, protocols, and ports.

A screened host is a firewall-protected system logically positioned just inside a private network. All inbound traffic is routed to the screened host, which in turn acts as a proxy for all the trusted systems within the private network. It is responsible for filtering traffic coming into the private network as well as for protecting the identity of the internal client.

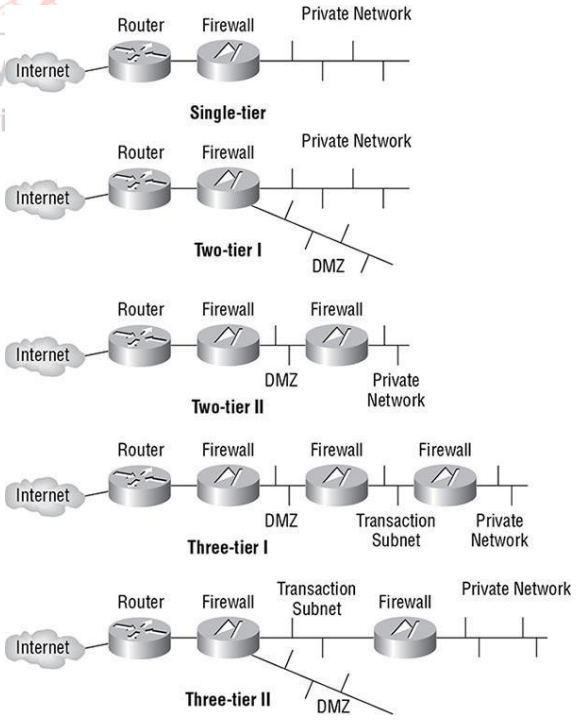
A Bastion Host between an internal and an external firewall. MOST SECURE

Silent rule Drops "noisy" traffic without logging it. This reduces log sizes

Stealth rule Disallows access to firewall software from unauthorized systems.

Cleanup rule Last rule in rule base, drops and logs any traffic that does not meet preceding rules.

Negate rule Used instead of the broad and permissive "any rules," provides tighter permission rights by specifying what system can be accessed and how.



11.9.1. Firewall Deployment Architecture

11.9.2. Secure Operation of Hardware

A collision domain is a group of networked systems that could cause a collision if any two (or more) of the systems in that group transmitted simultaneously.

A broadcast domain is a group of networked systems in which all other members receive a broadcast signal when one of the members of the group transmits it.

Collision domains are divided by using any layer 2 or higher device, and broadcast domains are divided by using any layer 3 or higher device.

Repeaters, Concentrators, and Amplifiers are used to strengthen the communication signal over a cable segment as well as connect network segments that use the same protocol. Systems on either side are part of the same collision domain and broadcast domain.

Hubs connect multiple systems and network segments that use same protocol. A hub is a multiport repeater. Systems on either side are part of the same collision and broadcast domains

Modems (layer 1) modulator-demodulator support computer communications of PSTN lines

Bridge connect two networks. Systems on either side: same broadcast but different collision domain

Switches: Connect network segments that use same protocol. Same broadcast, different collision

Routers controls traffic flow. Different broadcast and different collision domains

Brouters attempts to route first, but if that fails, it defaults to bridging

Gateway connects networks using different network protocols. IP-to-IPX gateway. different broadcast and collision domains

A proxy does not translate across protocols. A mediator, filter, caching server, & NAT/PAT server

Different broadcast domains and different collision domains

Coaxial Cable

Type	Max speed	Distance	Installation Difficulty	EMI
10Base2 (thinnet)	10 Mbps	185 m	Medium	Medium
10Base5 (thicknet)	10 Mbps	500 m	High	Low
10BaseT (UTP)	10 Mbps	100 m	Low	High
STP	155 Mbps	100 m	Medium	Medium
100BaseT/100BaseTX	100 Mbps	100 m	Low	High
1000BaseT	1000 Mbps	100 m	Low	High
Fiber	2+ Gbps	2+ km	Medium to high	None

Problems with coax cable

Bending past maximum arc radius breaks center conductor

Cannot deploy greater than its maximum recommended length

Terminate ends cable with 50 ohm resistor

Not grounding at least one end of a terminated coax cable

11.9.3. Baseband/Broadband

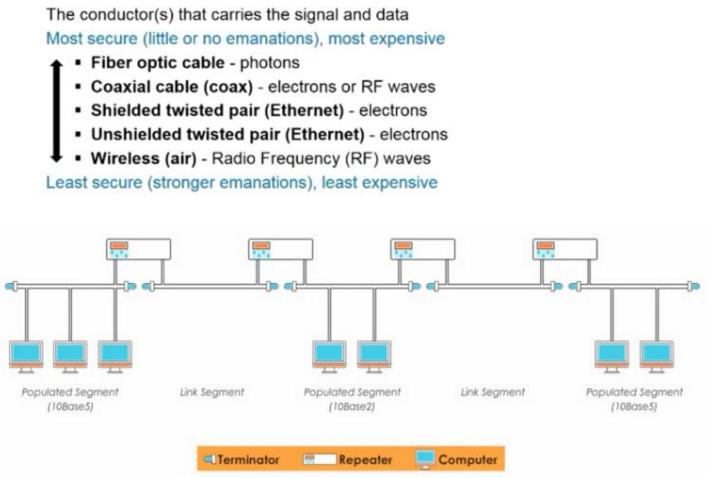
Baseband cables: single signal at a time, and Broadband cables: multiple signals simultaneously

Ethernet is a baseband technology

Broadband is suitable for high throughput rates, especially when several channels are multiplexed. Broadband is a form of analog signal. Cable television and cable modems, ISDN, DSL, T1, and T3 are examples of broadband technologies.

11.9.4. Transmission Media: Twisted Pair

UTP category	Throughput	Notes
Cat 1	Voice only	Not suitable for networks but usable by modems
Cat 2	4 Mbps	Not suitable for most networks; often employed for host-to-terminal connections on mainframes
Cat 3	10 Mbps	Primarily used in 10BaseT Ethernet networks (offers only 4 Mbps when used on Token Ring networks) and as telephone cables
Cat 4	16 Mbps	Primarily used in Token Ring networks
Cat 5	100 Mbps	Used in 100BaseTX, FDDI, and ATM networks
Cat 6	1,000 Mbps	Used in high-speed networks
Cat 7	10 Gbps	Used on 10 gigabit-speed networks



Category 5e and Category 6 UTP cable are both rated to 1000 Mbps.

Transmission Media: 5-4-3 Rule

Defines the number of repeaters/concentrators and segments that can be used in a network design

Between any two nodes, there can be a maximum of five segments connected by four repeaters/concentrators, and it states that only three of those five segments can be populated

The 5-4-3 rule does not apply to switched networks or bridges or routers

Connects each system as points on a circle. Unidirectional transmission loop

Traffic management is performed by a token. If one segment is broken, all communication ceases

Dual loops running in opposite directions prevents single points of failure

To avoid collision the systems employ a CA mechanism

All systems on the network hears the data

Benefit - single segment fails, comm. is uninterrupted. But central trunk line is single point of failure

Network Topologies: Star

If any one segment fails, the other segments can continue to function

The central hub is a single point of failure

Network Topologies: Mesh

Connects systems to other systems using numerous paths

Redundant connections to systems, allows multiple segment failures without affecting connectivity

11.10. Wireless Communication Concepts and Security

Spread spectrum: communication occurs over multiple frequencies at the same time

FHSS

Transmits data in a series while constantly changing the frequency in use
Entire range of available frequencies is employed, but one at a time

Employs all the available frequencies simultaneously in parallel. Higher throughput than FHSS
Special encoding (chipping code) allows receiver to reconstruct data if parts were distorted
Same way as that the parity of RAID-5

- Digital multicarrier modulation of compacted transmission. Peak of one occurs at null of others
- Modulated signals are perpendicular (orthogonal) and thus do not cause interference with each other
- OFDM requires a smaller frequency set (aka channel bands) but can offer greater data throughput
- Used in 802.11ac, 4G, 5G, cell phone technologies, WiMax, Satellite etc.

Bluejacking: an attacker transmits unsolicited SMS to engage/annoy
Bluesnarfing: More damage. connects and access contact lists, data, and even conversations
Bluebugging: grants remote control and ability to turn on microphone to use phone as an audio bug

RFID

A radio transmitter when current is generated in an antenna when placed in a magnetic field
Triggered/powered and read from a considerable distance away
RFID can be attached to devices and allows for quick inventory tracking

Near-field communication establishes radio communications between devices in close proximity
NFC attacks can include man-in-the-middle, eavesdropping, data manipulation, and replay attacks

LAN Technologies: Ethernet

IEEE 802.3 is a shared-media LAN technology (broadcast technology). Allows devices to communicate over the same medium using collision detection and avoidance
Ethernet employs broadcast and collision domains.
Supports full-duplex communications. Ethernet data are called frames

A high-speed token-passing technology employs two rings with traffic flowing in opposite directions
FDDI is expensive but often used in campus environments before Fast Ethernet was developed
A less-expensive, distance-limited, and slower version CDDI uses twisted-pair cables
CDDI is also more vulnerable to interference and eavesdropping

Synchronous communications rely on timing & are able to support very high rates of data transfer
Asynchronous rely on stop & start delimiter & is best suited for smaller amounts of data. E.g. PSTN

Broadcast, Multicast, and Unicast

Broadcast technology supports communications to all possible recipients.
Multicast technology supports communications to multiple specific recipients.
Unicast technology supports only a single communication to a specific recipient.

The host listens to the LAN media to determine whether it is in use.
If the LAN media is not being used, the host transmits its communication.
The host waits for an acknowledgment.
If no acknowledgment is received after a time-out period, the host starts over at step 1.
CSMA does not directly address collisions

LAN Media Access: CSMA/CA

Uses inbound and outbound connection. Host listens on inbound to determine if LAN media is used
Used by AppleTalk and 802.11 wireless networking
Requires master system to responds to the requests and grants permission to send data transmissions

LAN Media Access: CSMA/CD

Ethernet networks employ the CSMA/CD technology.
Collision causes delays in transmissions as well as a required repetition of transmissions
This results in about 40 percent loss in potential throughput

LAN Media Access: Polling

Uses a master-slave configuration. Synchronous Data Link Control (SDLC) uses polling

Polling addresses collisions. Polling is an inverse of the CSMA/CA method.

12. Secure Communications and Network Attacks

Communications security is designed to detect, prevent, and even correct data transportation errors

12.1. Network and Protocol Security

Secure communication protocols: Protocols that provide security services for application-specific channels

IPsec uses public key cryptography to provide encryption, access control, nonrepudiation, and message authentication, all using IP-based protocols.

Kerberos offers a single sign-on solution for users and provides protection for logon credentials

SSH Secure Shell end-to-end encryption technique. Encrypts numerous plaintext utilities (such as rcp, rlogin, rexec), serve as a protocol encrypter (such as with SFTP), and function as a VPN

Signal Protocol provides end-to-end encryption for voice comm., videoconferencing, text message

SSL and TLS can be implemented at layer 3 to operate as a VPN known as OpenVPN

SIP is a protocol associated with VoIP

Used over Point-to-Point Protocol (PPP) links and encrypts usernames and passwords

Authentication using a challenge-response dialogue that cannot be replayed

Periodically re-authenticates the remote system to verify a persistent identity Password Authentication Protocol (PAP): Protocol for PPP. Usernames/passwords in cleartext

Extensible Authentication Protocol (EAP)

This is a framework for authentication instead of an actual protocol

EAP assumes that the channel is already protected

Allows customized authentication security solutions, supports smart cards/tokens/ biometrics

Protected Extensible Authentication Protocol (PEAP)

Encapsulates EAP in a TLS tunnel. PEAP is preferred to EAP and LEAP

It is used for securing communications over 802.11 wireless connections.

Secure Voice Communications

VoIP

SecureRTP (SRTP) is a security improvement over the RTP used in VoIP.

SRTP aims to minimize the risk of VoIP DoS through robust encryption and reliable authentication

Private branch exchange (PBX) Fraud and Abuse

PBX systems can be exploited to avoid toll charges and hide identity. Phreakers uses

Black boxes manipulates line voltages to steal long-distance services

Red boxes simulate tones of coins being deposited into a pay phone. Just small tape recorders

Blue boxes simulate 2600 Hz tones to interact directly with telephone network trunk systems. This could be a whistle, a tape recorder, or a digital tone generator.

White boxes are used to control the phone system. A white box is a DTMF generator (keypad)

Email Security Solutions

Secure Multipurpose Internet Mail Extensions (S/MIME)

Offers authentication and confidentiality through (RSA) public key encryption and digital signatures

Authentication: X.509 digital certificates. Privacy: Public Key Cryptography Standard encryption

Two types of messages:

A signed message provides integrity, sender authentication, and nonrepudiation

An enveloped message provides integrity, sender authentication, and confidentiality MIME Object Security Services (MOSS)

Provides authentication, confidentiality, integrity, and nonrepudiation for email messages

Employs MD2/MD5; RSA public key; and DES to provide authentication and encryption services

Privacy Enhanced Mail (PEM)

Provides authentication, integrity, confidentiality, & nonrepudiation. Uses RSA, DES & X.509.

Domain Keys Identified Mail (DKIM)

Asserts that valid mail is sent by an organization through verification of domain name identity

Pretty Good Privacy (PGP)

Provides confidentiality and authentication by IDEA. RSA for digital signatures & key distribution

Instead of a central Certificate Authority (CA), PGP uses a decentralized trust model

1st version used RSA, 2nd, IDEA, but later versions offered a spectrum of algorithm options

Opportunistic: A TLS connection will be established if both email servers have TLS capabilities

Mandatory: Email server will only communicate with other email servers if TLS capabilities exists

Sender Policy Framework (SPF)

Protects against spam and email spoofing

It checks that inbound messages originate from a host authorized to send messages

I receive a message from mark.n@abc.com then SPF checks with the administrators of smtp.abcc.com that mark.n is authorized to send messages through their system before the inbound message is accepted and sent into a recipient inbox

Remote Access Security

Include restricted *allowed addresses, geolocation, caller ID, callback, and multi-factor authentication*.

Remote Connectivity Technology: Fully examine every aspect of your connection options

Transmission Protection: VPNs, TLS, SSH, IPsec

Authentication Protection: PAP, CHAP, EAP, or PEAP or LEAP, RADIUS, and TACACS+.

Dial-up Protocols Point -to-Point Protocol (PPP)

Full-duplex protocol to transmit packets over non-LAN connections (modem, ISDN, VPN)

Protocol dial-up internet connections. Authentication is protected through CHAP/PAP

PPP is a replacement for SLIP and can support any LAN protocol, not just TCP/IP

Serial Line Internet Protocol (SLIP)

TCP/IP communications over asynchronous serial connections (serial cables or modem dial-up)

Supports only IP, requires static IP addresses, no error detection/correction, & no compression

Centralized Remote Authentication Services

RADIUS

UDP 1812 port by default. TCP 2083 over TLS

Only password in encrypted

Terminal Access Controller Access-Control System (TACACS+)

TACACS integrates the authentication and authorization processes.

XTACACS keeps the authentication, authorization, and accounting processes separate.

TACACS+ adds 2FA. TCP port 49

VPN: Common Protocols

Point-to-Point Tunneling Protocol (PPTP)

Operates at layer 2. It does not support TACACS+ and RADIUS.

It offers protection for authentication traffic through the same authentication protocols supported by PPP:

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)

Challenge Handshake Authentication Protocol (CHAP)

Password Authentication Protocol (PAP)

Extensible Authentication Protocol (EAP)

Shiva Password Authentication Protocol (SPAP)

TABLE 12.1 VPN characteristics

VPN Protocol	Native Authentication Protection	Native Data Encryption	Protocols Supported	Dial-Up Links Supported
PPTP	Yes	No	PPP	Yes
L2F	Yes	No	PPP/SLIP	Yes
L2TP	Yes	No (can use IPsec)	PPP	Yes
IPsec	Yes	Yes	IP only	No

The VPN protocols which encapsulate PPP are able to support any subprotocol compatible with PPP, which includes IPv4, IPv6, IPX, and AppleTalk.

The initial tunnel negotiation process used by PPTP is not encrypted. Third party can intercept session establishment packets (IP address sender/receiver, usernames, hashed passwords)

Layer 2 Forwarding Protocol and Layer 2 Tunneling Protocol

Cisco's L2F, a mutual authentication tunneling mechanism, does not offer encryption.

L2TP creates a point-to-point tunnel between communication endpoints. Supports TACACS+ and RADIUS. IPsec is commonly used as a security mechanism **IP Security (IPsec)**

Authentication Header (AH) provides authentication, integrity, and nonrepudiation.

Encapsulating Security Payload (ESP) provides confidentiality and limited authentication

In transport mode, the IP packet data is encrypted but the header of the packet is not.

In tunnel mode, the entire IP packet is encrypted and a new header is added

Virtual LAN

A hardware-imposed network segmentation created by switches and used for traffic management

Communications between VLANs require a routing function

VLANs work like subnets but not an actual subnets

The routing function blocks broadcasts between subnets and VLANs and protect broadcast storms. ○

A broadcast storm is a flood of unwanted Ethernet broadcast network traffic

Virtualization

VM escaping occurs when software within a guest OS is able to breach the isolation protection provided by the hypervisor in order to violate the container of other guest OSs or to infiltrate a host OS. VM escaping can be a serious problem, but steps can be implemented to minimize the risk.

First, keep highly sensitive systems and data on separate physical machines.
Second, keep all hypervisor software current with vendor-released patches
Third, monitor attack, exposure, and abuse indexes for new threats to your environment.

Virtual Software

A *virtual application* is a software product deployed in such a way that it is fooled into believing it is interacting with a full host OS.

V*irtual desktop* refers to at least three different types of technology:

- A remote access tool
- Multiple applications encapsulation for portability or cross-OS operation
- An extended or expanded desktop allowing multiple application

Virtual Networking

- Is the combination of hardware and software networking components into a single integrated entity
- The resulting system allows for software control over all network functions: management, traffic shaping, address assignment, and so on.

SDN

- SDN is that it is effectively network virtualization. It allows data transmission paths, communication decision trees, and flow control to be virtualized in the SDN control layer rather than being handled on the hardware on a per-device basis.

12.2. Network Address Translation

Stateful NAT: Maintains information about communication sessions between clients and external systems **NAT vs. PAT (**Port address translation or NAT overloading)

NAT maps one internal IP address to one external IP address.
PAT maps one internal IP address to an external IP address and port number combination
PAT can theoretically support 65,536 simultaneous communications

NOTE: *IPv6 over IPv4 Networks=Tunneling, IPv4 over IPv6 Networks=Translation*

NAT is not directly compatible with IPsec because it modifies packet headers, which IPsec relies on to prevent security violations.
NAT-Traversal was designed to support IPsec VPNs through the use of UDP encapsulation of IKE

Static NAT and Dynamic NAT

Static NAT specific internal client's IP is assigned permanent map to specific external public IP
Dynamic NAT to grant multiple internal clients access to a few leased public IP addresses

Automatic Private IP Addressing APIPA

APIPA, link-local address assignment, assigns an IP address in the event of a DHCP failure.
APIPA is primarily a feature of Windows.
IP range 169.254.0.1 to 169.254.255.254. Allows to communicate with other APIPA clients only

Loopback Address

Allows for the testing of local network settings in spite of missing/damaged device drivers
127.0.0.1 address is widely used.

12.3. Switching Technologies

Virtual Circuits: logical pathway over a packet-switched network
PVC is like a dedicated leased line; circuit always exists
SVC like a dial-up connection, circuit has to be created

TABLE 12.2 Circuit Switching vs. Packet Switching

Circuit Switching	Packet Switching
Constant traffic	Bursty traffic
Fixed known delays	Variable delays
Connection oriented	Connectionless
Sensitive to connection loss	Sensitive to data loss
Used primarily for voice	Used for any type of traffic

12.4. WAN Technologies

Connection Type	Speed
Partial T1 (DS-0)	64 Kbps upto 1.544 Mbps
T1 (DS-1)	1.544 Mbps
T3 (DS-3)	44.736 Mbps
E1	2.108 Mbps
E3	34.368 Mbps
Cable modem or routers	10+ Mbps

Non-Dedicated WAN

Digital subscriber line (DSL)

Speeds from 144 Kbps to 20 Mbps. ADSL, xDSL, CDSL, HDSL, SDSL, RASDSL, IDSL, & VDSL
The maximum distance of a DSL line: 5,000 meters

Integrated Services Digital Network (ISDN): Supports both voice and high-speed data communications

Basic Rate Interface (BRI) offers two B channels (64Kbps) and one D channel (16 Kbps). ○

B channels: used for data transmission.

- D channel: used for call establishment, management, and teardown
- Offers 144 Kbps of total throughput

Primary Rate Interface (PRI) multiple 64 Kbps B channels (2 to 23) & single 64 Kbps D channel.

Offers as little as 192 Kbps and up to 1.544 Mbps

Satellite connections

Offer high-speed solutions in locales that are inaccessible by cable, radio, and LoS communications

Are usually insecure because of their large surface footprint

WAN Connection Technologies

A WAN switch, specialized router, or border connection device provides interfacing needed between the network carrier service and a company's LAN

The border connection device is called the channel service unit/data service unit (CSU/DSU).

These devices convert LAN signals into the format used by the WAN carrier network and vice versa.

The CSU/DSU contains data terminal equipment/data circuit-terminating equipment (DTE/DCE), which provides the actual connection point for the LAN's router (the DTE) and the WAN carrier network's switch (the DCE).

The CSU/DSU acts as a translator, a store-and-forward device, and a link conditioner.

X.25 WAN Connection

A packet-switching technology that uses PVC to establish connections

X.25 use is declining because of its lower performance and throughput rates

Frame Relay

Packet-switching technology that supports multiple PVCs over single WAN carrier

Cost is based on the amount of data transferred

The committed information rate (CIR) is the guaranteed minimum bandwidth provide to customer

Frame Relay requires the use of DTE/DCE at each connection point.

Asynchronous transfer mode (ATM)

Cell-switching WAN technology that fragments communications into 53-byte cells.

The use of fixed-length cells allows ATM to be very efficient and offer high throughputs.

ATM can use either PVCs or SVCs.

Switched Multimegabit Data Service (SMDS)

A connectionless packet-switching technology

It is used to connect multiple LANs to form a metropolitan area network (MAN) or a WAN

Preferred mechanism for linking remote LANs that communicate infrequently.

Supports high-speed bursty traffic and bandwidth on demand. It fragments data into small cells

Specialized WAN Protocols

Synchronous Data Link Control (SDLC)

Permanent physical connections of dedicated lines for mainframes, IBM Systems Network Architecture (SNA) systems

Uses polling, operate at OSI layer 2, and is a bit-oriented synchronous protocol

High-Level Data Link Control (HDLC)

Designed for serial synchronous connections

Supports full-duplex communications and supports both point-to-point and multipoint connections

Uses polling, operate at OSI layer 2 and offers flow control, error detection/correction

Synchronous Digital Hierarchy (SDH) and Synchronous Optical Network (SONET)

SDH and SONET are fiber-optic high-speed networking standards.

A high-availability, high-speed, multiplexed, low-latency technology used on fiber-optic networks.

Use synchronous time-division multiplexing (TDM)

12.4 Bandwidth levels of SDH and SONET

SONET	SDH Data	Rate
STS-1 / OC-1	STM-0	51.84 Mbps
STS-3 / OC-3	STM-1	155.52 Mbps
STS-12 / OC-12	STM-4	622.08 Mbps
STS-48 / OC-48	STM-16	2.488 Gbps
STS-96 / OC-96	STM-32	4.876 Gbps
STS-192 / OC-192	STM-64	9.953 Gbps
STS-768 / OC-768	STM-256	39.813 Gbps

12.5. Access Points

Root mode: Default configuration. The AP is directly connected to the wired network, and wireless clients access the wired network via the wireless access point. Also known as infrastructure mode.

Repeater mode: The AP doesn't connect directly to the wired network, but instead provides an upstream link to another AP, effectively extending the range of the WLAN. Also known as stand-alone mode.

Bridge mode: A rare configuration that isn't supported in most APs. Bridge mode is used to connect two separate wired network segments via a wireless access point.

Mesh mode: Multiple APs work together to create the appearance of a single Wi-Fi network for larger homes and workspaces.

12.6. Security Control Characteristics

Transparency: a service, security control, or access mechanism that ensures that it is unseen by users

Security Boundary: intersection betn. any two areas/subnets/environments having different security needs.

Impersonation, or masquerading Attacks

Act of pretending to be someone or something you are not to gain unauthorized access to a system
- This is different from spoofing, where an entity puts forth a false identity but without any proof (such as falsely using an IP address, MAC addresses, email address, system/domain name, etc.).
- Impersonation is often possible through the capture of usernames and passwords
- Prevention: onetime pads and token authentication systems, Kerberos, and encryption

Replay Attacks: Use onetime authentication mechanisms and sequenced session identification

Modification attacks:
- Captured packets are altered and then played against a system to bypass the restrictions of improved authentication mechanisms and session sequencing.
- Countermeasures: use digital signature and packet checksum verification

ARP Spoofing

Define static ARP mappings for critical systems, monitor ARP caches for MAC-to-IP-address mappings, or use IDS to detect anomalies in system traffic and changes in ARP traffic

DNS

DNS poisoning and DNS spoofing are also known as resolution attacks

Allow only authorized changes to DNS, restricting zone transfers, and log privileged DNS activity

Homograph attack leverage similarities in character sets to register phony international domain names (IDNs) that to the naked eye appear legitimate

Upgrade DNS to DNSSEC

An attack related to phishing is **pretexting**, which is the practice of obtaining your personal information under false pretenses

Hyperlink Spoof

Use DNSSEC

12.6.1. Domain 4: Miscellaneous Points

Value-added network (VAN): extranet to share information or integrate shared processes

Electronic Data Interchange (EDI) allows exchange order forms/purchase orders etc.

Layer 7: identifying/establishing communication partners, determining resource availability

RIP employs three other mechanisms to prevent routing loops:

Split horizon: Prevents router from advertising a route back

Route poisoning: Sets hop count on bad route to 16

Holddown timers: avoid problems associated with *flapping*.

Flapping occurs when route repeatedly change state (up/down) over a short period

Data Link Layer: Logical Link Control (LLC) and MAC sub-layers

Root mode (infrastructure), **Repeater mode** (stand-alone), **Mesh mode** (enterprise)

Bit error ratio (BER) ratio of incorrectly received bits to total received bits

Using (Real time black-hole list) RBLs is only one method to combat spam

Facsimile transmissions relates to fax machines

SDLC supports NRM transmission only

The three modes of HDLC are:

Normal Response Mode (NRM) Secondary nodes transmit when primary gives permission
- Asynchronous Response Mode (ARM) Secondary nodes initiate communication to primary
- Asynchronous Balanced Mode (ABM) initiating transmissions without receiving permission

Personal Digital Assistants (PDAs) are small computers network that offer calendar and notepad

DHCPDISCOVER: request IP lease (broadcast)

DHCPOFFER: response to above. Offers ip (broadcast)

DHCPREQUEST: accepts the ip and ack request DHCP server (broadcast)

DHCPACK: ack by DHCP server
MPLS: to create VPNs without the need of end-user applications. Layer 2.5 protocol
CIDR is also referred to as supernetting.
Ethernet uses CSMA\CD, Token Ring uses tokens, FDDI uses tokens, Wi-Fi uses CSMA\CA, and mainframe media access technology uses polling
ICMP type 30 is for Traceroute, 37 Domain name request, 38 Domain name reply, 39 SKIP
SNMP: *Management Information Base* (MIB) logical grouping of managed objects
A *nonrecursive query:* request is not passed from DNS server to another and answer or error is returned. A *recursive query* request passed from one DNS to another until correct information
Mail servers use a *relay agent* to send a message from one mail server to another.
BGP uses a combination of link-state and distance-vector routing algorithms.
Wormhole: attacker capture packet at one location and tunnel it to another location in the network
- The **leash** restricts the packet's maximum allowed transmission distance

Many bridges use the *Spanning Tree Algorithm (STA)*, which adds more intelligence to the bridges
Kernel proxy firewall: 5th gen. Creates dynamic network stacks when a packet needs to be evaluated
Kernel proxy firewalls are faster than application-level as processing takes place in the kernel
Silent rule Drops "noisy" traffic without logging
Stealth rule Disallows access to firewall from unauthorized systems
Cleanup rule Last rule in rule base; drops and logs any traffic that does not meet preceding rules
Negate rule specifies what system can be accessed and how
The *control plane:* routing decisions. The *forwarding plane:* traffic forwarding decisions are made

Approaches to SDN
Open relies on open-source code, **API**, **Overlays** on a traditional one, virtualize all network nodes

QoS has three basic levels:
Best-effort service No guarantee of throughput, delay, or delivery
Differentiated service has more bandwidth, shorter delays, and fewer dropped frames
Guaranteed service Ensures specific data throughput at a guaranteed speed
High-Speed Serial Interface (HSSI) speeds up to 52 Mbps, as in T3 WAN connections
Multiservice access technologies data, voice, and video over one transmission line
WLAN-oriented standards. 802.16 is a MAN wireless standard
802.15 is Bluetooth. PAN
Sink tree: set of optimal routes from all sources to a given destination
Finger table is used for node lookup in peer-to-peer (P2P) networks
X.400: is standard for internet email security
Tunnel mode VPNs are used to connect networks to networks or networks to hosts. Transport mode is used to connect hosts to hosts.

DOMAIN 5: Identity and Access Management

13. Managing Identity and Authentication

13.1. Access Control

Deterrent Access Control attempts to discourage security policy violations
- Policies, awareness training, locks, fences, security badges, guards, mantraps, cameras

Preventive Access Control attempts to thwart or stop unwanted activity from occurring.
Fences, locks, biometrics, mantraps, lighting, alarm, separation-of-duties policies, job rotation policies, data classification, penetration testing, access control methods, encryption, auditing, presence of CCTV, smartcards, callback procedures, security policies, security awareness training, antivirus software, firewalls, and IPS

Detective Access Control attempts to discover or detect unwanted activity
Security guards, motion detectors, recording and reviewing of events, job rotation policies, mandatory vacation policies, audit trails, honeypots or honeynets, IDS, violation reports, supervision and reviews of users, and incident investigations.

Corrective Access Control returns systems to normal after an unwanted activity (during)
Terminating malicious activity, rebooting system, antivirus removing virus, backup and restore plans, and active IDS that modifies environment to stop an attack in progress

Recovery Access Control repair or restore resources, functions, and capabilities after a security event

– Backups and restores, fault-tolerant drive systems, system imaging, server clustering, antivirus software, and database or virtual machine shadowing.

Directive Access Control direct actions of subjects to encourage compliance with security policies

– Security policy requirements or criteria, posted notifications, escape route exit signs, monitoring, supervision, and procedures

Compensating Access Control provides an alternative when it isn't possible to use a primary control

Implementation Type Access Control

Administrative Access Controls are the policies and procedures. Management controls.

– Policies, procedures, hiring practices, background checks, classifying and labeling data, security awareness and training efforts, reports and reviews, personnel controls, and testing

Logical/Technical Controls are the hardware or software mechanisms

– Authentication methods (such as passwords, smartcards, and biometrics), encryption, constrained interfaces, ACL, protocols, firewalls, routers, IDS, and clipping levels.

Physical Controls mechanisms to prevent/monitor/detect direct contact with systems/ facility.

– Guards, fences, motion detectors, locked doors, sealed windows, lights, cable protection, laptop locks, badges, swipe cards, guard dogs, video cameras, mantraps, and alarms.

A Type 1 authentication factor is something you know. Password/PIN

A Type 2 authentication factor is something you have. Smartcard/hardware token/memory card

A Type 3 authentication factor is something you are or something you do. Fingerprints/signature

Cognitive Passwords

Series of challenge questions about facts or predefined responses that only the subject should know.

What is the name of your first pet?

What is your favorite sport?

Tokens: a password-generating device

Synchronous Dynamic Password Tokens: Time-based and synchronized with an authentication server.

Asynchronous Dynamic Password Tokens: hardware token generates passwords based on an algorithm and an incrementing counter. When using an incrementing counter, it creates a dynamic onetime password that stays the same until used for authentication.

- **HMAC-based One-Time Password (HOTP)**

Includes a hash function used by HOTP standard to create onetime passwords.

Similar to asynchronous dynamic passwords. The HOTP value remains valid until used

Time-based One-Time Password (TOTP)

Similar to HOTP. But uses timestamp and remains valid for a timeframe, as 30 seconds.

Expires if not used. This is similar to the synchronous dynamic passwords used by tokens

13.1.1. Biometrics

Retina Scans: focus on the pattern of blood vessels at the back of the eye. most accurate and can differentiate between twins. Reveal medical condition,

Iris Scans: Focusing on the colored area around the pupil, iris scans are second most accurate. Accuracy affected by changes in lighting and usage of glasses/contact lenses.

Fingerprint:

Face scans: use the geometric patterns of faces for detection and recognition. Casinos use it to identify card cheats.

Palm scan: use near-infrared light to measure vein patterns

Hand geometry: physical dimensions of the hand; captures a silhouette of hand, but not fingerprints or vein patterns. Difficult to uniquely identify an individual

Heart Pulse: often employed as a secondary biometric to support another type of authentication

Voice pattern: additional authentication mechanism but is rarely used by itself

13.1.2. Biometric Factor Error Ratings

False Rejection Rate occurs when a valid subject is not authenticated. (False negative). The ratio of false rejections to valid authentications is FRR. Type I error.

False Acceptance Rate occurs when an invalid subject is authenticated. (False positive). The ratio of false positives to valid authentications is FAR. Type II error

When too sensitive, false rejections (false negatives) are more common.

When not sensitive, false acceptance (false positives) are more common.

The point where the FRR and FAR percentages are equal is the CER, and the CER

Devices with lower CERs are more accurate than devices with higher CERs

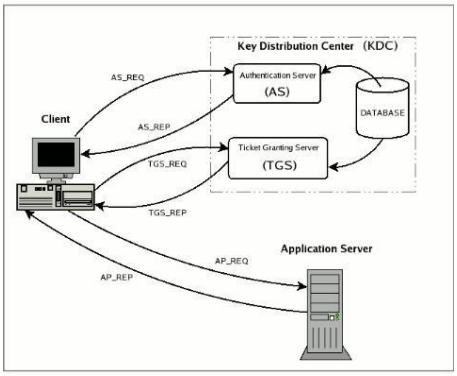
Throughput rate is amount of time the system requires to scan a subject and approve or deny access
Subjects typically accept a throughput rate of about 6 seconds or faster
Enrollment: a subject's biometric factor is sampled and stored. Reference profile/template
Enrollment times over 2 minutes are unacceptable.

MDM systems use context-aware authentication methods to identify devices
802.1x is another method used for device authentication

Service account has a high level of privileges so configure with a strong, complex password
Configure the account to be non-interactive
Services can be configured to use certificate-based authentication

13.2. Implementing Identity Management

Centralized access control all authorization verification is performed by a single entity
Decentralized access control (distributed) various entities throughout a system perform authorization
Centralized: Administrative overhead is lower
Decentralized: Administrative overhead is higher. Maintaining consistency difficult



Centralized technique that allows subject to be authenticated once and access multiple resources
Disadvantage: once an account is compromised, an attacker gains unrestricted access

Relies on symmetric-key cryptography AES
Provides confidentiality and integrity
Ticket-Granting Ticket (TGT) provides proof that a subject has authenticated through a KDC and is authorized to request tickets to access other objects.
Service ticket (ST): encrypted message that provides proof that a subject is authorized to access an object
Kerberos presents a single point of failure—the KDC. Also, if a KDC goes offline, no subject authentication can occur.

Note: The client's password is never transmitted over the network, but it is verified. The server encrypts a symmetric key using a hash of the user's password, and it can only be decrypted with a hash of the user's password. As long as the user enters the correct password, this step works. However, it fails if the user enters the incorrect password.

13.2.1. FIM and SSO

Federated identity management (FIM) is a form of SSO
A federation can be composed of multiple unrelated networks that can agree on a common FIM
A challenge with multiple companies communicating in a federation is finding a common language.

HTML

Hypertext Markup Language (HTML) is commonly used to display static web pages.
HTML describes how data is displayed using tags. <H1>I Passed The CISSP Exam</H1>

XML describes how to display the data by actually describing the data. <Results>Passed</Results>
Databases from multiple vendors can import and export data to and from an XML format

Security Assertion Markup Language (SAML)

XML-based language commonly used to exchange authentication and authorization information between federated organizations. Often used to provide SSO capabilities for browser access

Designed for exchanging user information for federated identity SSO purposes.
It is based on the Directory Service Markup Language (DSML), which can display LDAP-based directory service information in an XML format

Used to define access control policies within an XML format.
It commonly implements policies as an attribute/Role-based access control system

Note: SAML is a popular on the Internet while XACML with SDN applications. OAuth and OpenID Connect are used with many web-based applications to share authentication information without sharing credentials.

13.2.2. OAuth 2.0, OpenID and Scripted Access

OAuth 2.0 (open authentication) is an open standard used for access delegation. Example: App can interact with your Twitter account and when you use this feature Twitter asks you if you want to authorize the app and tells you what permissions you are granting.

OpenID provides decentralized authentication, allowing users to log into multiple unrelated websites with one set of credentials maintained by a third-party service referred to as an OpenID provider.

OpenID Connect is an authentication layer using the OAuth 2.0 framework.

It uses JSON Token (JWT), also called an ID token.

OpenID Connect uses Representational State Transfer (REST)- compliant web service to retrieve the JWT. In addition to authentication, JWT also provide profile information about user

Scripted access or logon scripts can be used to implement SSO in environments where true SSO technologies are not available.

OpenID is also an open SSO standard but it is maintained by the OpenID Foundation rather than as an IETF RFC standard. OpenID can be used in conjunction with OAuth or on its own.

13.2.3. Credential Management Systems

It provides a storage space for users to keep their credentials when SSO isn't available

13.2.4. Integrating Identity Services

Identity services provide additional tools for identification and authentication.

Identity as a service (IDaaS), is a third-party service that provides identity and access management

IDaaS effectively provides SSO for the cloud and useful when accessing cloud-based SaaS app

- One Google Account for everything Google.
- Office 365 provides
- Centrify provides third-party IDaaS services that integrate with Microsoft Active Directory

13.2.5. RADIUS

The network access server is the RADIUS client and a RADIUS server acts as an authentication server. The RADIUS server provides AAA services for multiple remote access servers

It uses UDP and encrypts only the exchange of the password not the entire session

RADIUS provides AAA services between network access servers and a shared authentication server

13.2.6. TACACS+

It separates authentication, authorization, and accounting into separate processes

It encrypts all of the authentication information

TACACS and XTACACS use UDP port 49, while TACACS+ uses TCP port 49

13.2.7. DIAMETER

It supports a wide range of protocols, including traditional IP, Mobile IP, and Voice over IP (VoIP).

Because it supports extra commands, it is popular where roaming is desirable, with wireless devices

Diameter is not backward compatible to RADIUS

Diameter uses TCP port 3868 or Stream Control Transmission Protocol (SCTP) port 3868

It also supports IPsec and TLS for encryption

13.3. Identity and Access Provisioning Lifecycle

Identity & access provisioning lifecycle refers to creation, management, and deletion of accounts.

Access control administration is the collection of tasks and duties involved in managing accounts, access, and accountability during the life of the account.

Provisioning: An initial step in identity management is the creation of new accounts and provisioning them with appropriate privileges. Called an enrollment or registration.

Account Review: Accounts should be reviewed periodically to ensure that security policies are being enforced. Guard against two problems: excessive privilege and creeping privileges.

Account Revocation: When employees leaves disable their user accounts as soon as possible

14. Controlling and Monitoring Access

Permissions, Rights, and Privileges

Permissions access granted for an object

Rights ability/right to take an action on an object

Privileges combination of rights and permissions. Admin perform any actions and access any data

Authorization Mechanisms

Implicit Deny

Access Control Matrix table that includes subjects, objects, and assigned privileges

Capability Tables focused on specific subjects (users, groups, or roles)

Constrained Interface restricts what users can do/see based on their privileges

Content-dependent access controls restrict access based on the content of object. A database

Context-dependent access controls require specific activity before granting users access.

- Checkout is complete only after payment. Restrict access to app based on time

Need to Know subjects are granted access only to what they need to know for their work tasks

Least Privilege subjects are granted only the privileges they need to perform their work tasks

Separation of Duties and Responsibilities sensitive functions are split into two or more employees

14.1. Access Controls Models

Discretionary Access Control

Every object has an owner and the owner can grant or deny access to any other subjects. NTFS Microsoft

A DAC model is implemented using ACLs on objects.

Does not offer a central management as owners can alter the ACLs on their objects

Every object has an owner (data custodian), and owners have full control

Workflow-based access control

Provisioning that occurs through an established workflow, such as through an HR process

Nondiscretionary Access Control

Administrators centrally administer non-DAC. Changes affect entire environment

Access does not focus on user identity. Instead, static set of rules governing whole

Any model that isn't a discretionary model is a nondiscretionary model

Permission assigned based on roles or groups instead of users

Enforces principle of least privilege by preventing privilege creep

Useful in dynamic environments with frequent personnel changes. Can grant multiple permissions **Rule-Based Access Control:** Global rules that apply to all subjects. Firewall. Rules/restrictions/filters

Attribute Based Access Control

- Use of rules that can include multiple attributes. Many SDN use the ABAC model
- Admin create rules using plain language. *Allow Managers to access WAN using a mobile device*
- User attributes: group membership, work department, and devices used (desktop PC)
- Network attribute: local internal network, a wireless network, an intranet, or WAN
- Devices: firewalls, proxy servers, web servers, database servers

Mandatory Access Control

- Use of classification labels. Each classification label represents a security domain/realm
- Security domain: collection of subjects and objects sharing common security policy
- *Lattice-based, Prohibitive/implicit-deny philosophy* (**not an explicit-deny**).
- Labels applied to both subjects and objects
- More secure than the DAC model, but it isn't as flexible/scalable

Hierarchical Environment: Clearance in one level grants access to objects in that and level below

Compartmentalized environment: To access an object, the subject must have specific clearance

Hybrid Environment

- Combines both. Each hierarchy may contain numerous subdivisions that are isolated from rest
- A subject must have the correct clearance and need to know within specific compartment
- A hybrid MAC environment provides granular control but becomes difficult to manage as it grows

14.2. Attacks and Prevention

Access Aggregation Attacks

Collecting multiple pieces of non-sensitive information and combining to learn sensitive info

Reconnaissance attacks are access aggregation attacks

Prevention: defense-in-depth, need-to-know, and least privilege principles

A strong password helps prevent password attacks

Dictionary Attacks

Brute-Force Attacks

Birthday Attack: A birthday attack focuses on finding collisions

Rainbow Table Attacks: Bcrypt/Password-Based Key Derivation Function 2 (PBKDF2) algo. to salt

Sniffer Attacks

Encrypt all sensitive data, Use onetime passwords, Protect with physical security

Monitor the network for signatures from sniffers

IP spoofing: attackers replace a valid source IP address with a false one

Email Spoofing: Spammers commonly spoof the email address in the **From** field

Phone Number Spoofing: Caller ID services allow users to identify the phone number

Social Engineering Attacks: Phishing

Social engineering attempts to trick users into giving up sensitive information

14.2.1. Social Engineering

Drive-by download malware that installs itself without the user's knowledge when visiting website
Spear phishing targeted to a specific group of users
Whaling targets senior or high-level executives
Vishing uses the phone
Smartcards: side-channel attack a passive, noninvasive attack intended to observe device operation
Attacker can learn information contained within the card, encryption key
Can measure the power consumption of a chip, timing attack, fault analysis attacks

14.3. Protection Mechanisms

Control physical access to systems
Control electronic access to files
Create a strong password policy
Hash and salt passwords
Use password masking
Deploy multifactor authentication
Use account lockout controls
Use last logon notification
Educate users about security

14.3.1. Domain 5: Miscellaneous Points

Remote Access Service (RAS) servers utilize the Point-to-Point Protocol (PPP) to encapsulate IP packets and establish dial-in connections over serial and ISDN links.

Contactless smart cards: The *hybrid* has two chips, can utilize contact/contactless formats. A *combi* one microprocessor chip that can communicate to contact or contactless readers

Software attacks are also considered noninvasive attacks.

Kerberos must be **transparent, scalable**, **reliable**, and **secure**

The KDC can be a single point of failure.

Secret keys are temporarily stored; intruder can keys
vulnerable to password guessing
Network traffic is not protected by Kerberos if encryption is not enabled
If the keys are too short, they can be vulnerable to brute-force attacks.

Single **Sign-On Technologies: A Summary**

Kerberos based on symmetric key cryptography
Security domains managed by group
Directory services standard resource naming and central access control ○
Thin clients central server for access control, processing, and storage

Simple Object *Access Protocol (SOAP)* web service information is exchanged in structured manner

Service oriented architecture (SOA) way to provide independent services residing on different systems in different business domains in one consistent manner. For example, if your company has a web portal that allows you to access the company's CRM, an employee directory, and a help-desk ticketing application, this is most likely being provided through an SOA.

A meta-directory within an IdM physically contains the identity information within an identity store

Wearable devices includes watches, fitness device, video glasses etc.

DOMAIN 6: Security Assessment and Testing

15. Security Assessment and Testing

15.1. Security Testing

Security tests verify that a control is functioning properly. Consider following

Availability of testing resources
Criticality/Sensitivity of the systems/applications
Likelihood of a technical failure/misconfiguration
Risk of configuration change/attack
Changes in the technical environment

Difficulty and time required to perform test
Impact of the test on normal business operations

Then, security teams design and validate a comprehensive assessment and testing strategy
frequent automated tests supplemented by infrequent manual tests
PCI system: vulnerability scanning nightly with immediate alerts to admin when new vulnerability.
Penetration test annual basis

15.2. Security Assessment

Review of threat environment, current/future risks, and the value of the targeted environment
Outcome: assessment report addressed to management

Specifications documents. Policies/procedures/requirements/specifications/designs
Mechanisms controls used to meet the specifications. Hardware/software/firmware
Activities actions carried out. Backups/exporting log files/reviewing account histories
Individuals people who implement specifications, mechanisms, and activities

15.3. Security Audits

Performed by independent auditors
Assessment and testing results are meant for internal use only
Audits to demonstrate the effectiveness of controls to a third party. Avoids conflict of interest
Reports intended for board of directors, government regulators, and other third parties.

Internal audits: performed by an organization's internal audit staff
External audits: performed by an outside firm and have a high degree of external validity
- Ernst & Young, Deloitte & Touche, Pricewater house Coopers, KPMG

Third-party audits by/on behalf of, another organization Organization selects the auditors and designs the scope of the audit

15.4. Describing Vulnerabilities

The Security Content Automation Protocol (SCAP) is a suite of specifications used to handle vulnerability and security configuration information.
Common Vulnerabilities and Exposures (CVE)
Common Vulnerability Scoring System (CVSS)
Common Configuration Enumeration (CCE) provides a naming for system configuration issues
Common Platform Enumeration (CPE) a naming system for OS, applications, and devices
Extensible Configuration Checklist Description Format XCCDF, language of security checklist
Open Vulnerability & Assessment Language OVAL language describing security testing procedures

15.5. Vulnerability Scans

15.5.1. Network Discovery Scans

TCP SYN Scan "half-open" scanning
TCP Connect Scan Opens a full connection on the specified port half-scan permission not allowed
TCP ACK Scan Sends packet with ACK flag set (open connection). Done to *determine the rules enforced by a firewall and the firewall methodology*.
Xmas Scan Sends a packet with the FIN, PSH, and URG flags set

Open port is open and application is actively accepting connections
Closed port is accessible (firewall allowing access), but there is no application accepting connection
Filtered unable to determine open or closed because a firewall is interfering

Scanners use a technique called banner grabbing

15.5.2. Network Vulnerability Scans

Way to improve the accuracy: perform authenticated scans (has read-only access)
Nessus, Qualys, Rapid7 NeXpose, OpenVAS is a vulnerability scanner.
Aircrack testing the encryption and security parameters of wireless networks

15.5.3. Web Vulnerability Scanning

Nessus, Acunetix, Nikto, Wapiti, Burp Suite proxy tool.

15.5.4. Database Vulnerability Scanning

Scans databases and web applications for vulnerabilities that may affect database security. **sqlmap**

15.5.5. Vulnerability Management Workflow

Detection: identification of a vulnerability
Validation: confirm that it is not false positive
Remediation: validated vulnerabilities should then be remediated

The goal is to ensure that vulnerabilities are detected and resolved in an orderly fashion

Prioritize vulnerability based on severity, likelihood of exploitation, and difficulty of remediation

15.6. Penetration Testing

Planning Testing team and management agreement on scope of test and rules of engagement
Information gathering and discovery collect information about the target environment
Vulnerability scanning probes for system weaknesses
Exploitation exploit tools to attempt to defeat system security
Reporting summarize the results of the penetration testing and makes recommendations

Metasploit uses a scripting language to allow the automatic execution of common attacks

White Box Penetration Test Provides the attackers with detailed information
Gray Box Penetration Test (partial knowledge) when black box results are desired but costs or time constraints mean that some knowledge is needed to complete the testing
Black Box Penetration Test Does not provide attackers with any information

Use OWASP Guide, OSSTMM, NIST 800-115, FedRAMP Penetration Test Guidance

15.7. Software Testing

15.7.1. Code Review

Fagan inspections found only in highly restrictive environments where code flaws have catastrophic impact

Planning, Overview, Preparation, Inspection, Rework, Follow-up

Use of automated review tools to detect common application flaws before moving to production **Static Testing** evaluates the security of software without running. Usually involves automated tools

Dynamic Testing

Evaluates security of software in a runtime environment. The only test option written by some else
Testers often do not have access to the underlying source code

Use of WebApp scan to detect XSS, SQL injection
The use of synthetic scripted transactions to verify system performance **Fuzz Testing**: a specialized dynamic testing technique

Provides different/invalid input to software to stress its limits and find previously undetected flaws

- Mutation/Dumb manipulates original input to create fuzzed input.

zzuf tool automates the process
Generational/Intelligent develops data models and creates new fuzzed input based on data used

Fuzz testing typically doesn't result in full coverage. Limited to detecting simple vulnerabilities

15.7.2. Interface Testing

Assesses the performance of modules against the interface specifications

API test to ensure that they enforce all security requirements.
User Interfaces (UIs) GUIs and command-line interfaces (ability to interact with the software)
Physical Interfaces Exist in apps that manipulate machinery, logic controllers, or other objects in physical world. Tester carefully because of the potential consequences if they fail

15.7.3. Misuse Case Testing

Misuse/abuse evaluates vulnerability of software to known risks. Like manipulate banking software to gain access to another user's account.

15.7.4. Test Coverage Analysis

Common types of structural coverage include statement, branch or decision coverage, loop coverage, path coverage, and data flow coverage.

- Test coverage = number of use cases tested/total use cases

Branch coverage: Has every if statement been executed under all if and else conditions?
Condition coverage: Has every logical test in the code been executed under all sets of inputs?
Function coverage: Has every function in the code been called and returned results?
Loop coverage: Has every loop in the code been executed under conditions that cause code execution multiple times, only once, and not at all?
Statement coverage: Has every line of code been executed during the test?

15.8. Website Monitoring

Passive monitoring

Analyzes actual network traffic sent to a website, which provides real-world monitoring data.
Real user monitoring (RUM) is a variant of passive monitoring where the monitoring tool reassembles the activity of individual users to track their interaction with a website.

Detects issues after they occur. Useful for troubleshooting issues identified by users

Synthetic monitoring (or active monitoring)

Performs artificial transactions against a website to assess performance

May miss issues experienced by real users

But is capable of detecting issues before they actually occur

15.9. Security Management Processes

Log Reviews – NetFlow log is useful

Backup Verification – Managers to periodically inspect to ensure protection needs. (log review/hash)

Account Management Reviews

Key performance and risk indicators

15.9.1. Account Management Reviews

Conduct full review (done for highly privileged accounts)

May use sampling. Pull random sample and perform verification.

Use IAM account review automated workflow

15.9.2. Key Performance and Risk Indicator

KPIs: how well things are going now, while KRIs: how badly things could go in the future

Number of open vulnerabilities

Time to resolve vulnerabilities

Vulnerability/defect recurrence

Number of compromised accounts

Number of software flaws detected in preproduction scanning

Repeat audit findings

User attempts to visit known malicious sites

15.10. Miscellaneous

SOC 1 Pertains to financial controls

SOC 2/3 Pertains to trust services (Security/Availability/Confidentiality/Process Integrity/Privacy)

SOC 3 is commonly used as a "seal of approval"

Personnel testing includes reviewing employee tasks

Kernel flaws: Can provide full access to attacker. Ensure security patch

File descriptor attacks File descriptors are numbers many operating systems use to represent open files in a process.

The checklist test is also called the desk check test.

A double-blind test (stealth assessment) is a blind test in which the network security staff is not notified that testing will occur.

Smishing. These are phishing messages that are delivered through SMS

Lishing. These are messages created using fraudulent LinkedIn user profiles.

Types of auditing:

Observation. Auditors passively observe activities performed by personnel

Inquiry. Auditors ask questions of control to understand how key activities are performed. ○

Inspection. Auditors inspect documents, records, and systems to verify key controls

Reperformance. Auditors perform tasks on their own to see whether the results are correct

DOMAIN 7: Security Operations

16. Managing Security Operations

Need-to-know focuses on permissions/ability to access information, least privilege focuses on privileges

Transitive Trust

A relationship between two security domains allows subjects in one domain (named primary) to access objects in the other domain (named training).

A nontransitive trust enforces principle of least privilege & grants trust to a single domain at a time

Separation of duties and responsibilities

It ensures that no single person has total control over a critical function (checks-and-balance)

Helps reduce fraud by requiring collusion

Applies it to applications and processes

Administrators grant specific processes only the privileges necessary to perform certain functions

Segregation of duties

Combination of separation of duties policy and principle of least privilege

Ensures that individuals do not have excessive system access that result in a conflict of interest

Two Person Control

Requires the approval of two individuals for critical tasks

Ensures peer review and reduces the likelihood of collusion and fraud

It combines separation of duties and two-person control

Information/privilege required to perform an operation be divided among two or more users

Ensures that no single person has sufficient privileges to compromise the security of environment

16.1. Privileged Account Management

NOTE: Principles such as least privilege and separation of duties help prevent security policy violations, and monitoring helps to deter and detect any violations that occur despite the use of preventive controls.

16.2. Managing the Information Lifecycle

Creation or Capture Data
Classification
Storage Data
Usage
Archive/backup Data
Destruction or Purging

16.3. Service-Level Agreements

MOU is similar to an SLA, less formal and doesn't include any monetary penalties

If plans to transmit sensitive data, use an ISA to specify the technical requirements

ISA provides information on how the two parties establish, maintain, and disconnect the connection.

It can also identify the minimum encryption methods used to secure the data.

16.4. Addressing Personnel Safety and Security

Duress systems are useful when personnel are working alone. A guard can raise an alarm

Emergency management plans

Security awareness and training of duress systems, travel best practices, emergency management plans, and general safety and security best practices

Sensitive Data

Ideally, the mobile devices should not contain any sensitive data. If needed, protect with strong encryption

16.5. Managing Hardware and Software Assets

Hardware Inventories

Bar-code systems and RFID methods

Before disposing of equipment sanitize it

Software Licensing: monitor license compliance to avoid legal issues **16.6. Managing Virtual Assets**

Virtual Machines (VMs)

Virtual Desktop Infrastructure (VDI) hosts a user's desktop as a VM on a server

Software-Defined Networks (SDNs) SDNs decouple the control plane from the data plane

Virtual Storage Area Network

Virtual mobile infrastructure (VMI) is a technology where OS of mobile device is virtualized

16.7. Managing Cloud-Based Assets

SaaS – services accessible via web browser. CSP is responsible for maintenance

PaaS – CSP provides computing platform, including hardware, OS, and applications. Consumers manage their applications and CSP is maintains host and the underlying cloud infrastructure

IaaS - servers, storage, and networking resources. Consumers install OS and apps and perform all required maintenance on OS and apps. CSP maintains the cloud-based infrastructure

Public Cloud: assets available for any consumers to rent or lease and is hosted by an external CSP

Private Cloud: cloud-based assets for a single organization. Consumer maintains

Community Cloud: cloud-based assets to two or more organizations. Shared maintenance

Hybrid Cloud: combination of two or more clouds. Shared maintenance

IaaS: customer retains responsibility for most server security. Managing OS security, maintaining host firewalls, configuring server access control. Vendor responsible for security mechanisms at hypervisor layer

16.8. Media and Configuration Management

Tape Media

Highly susceptible to loss due to corruption. keep at least two copies of backups

cleanliness of the storage area directly affect life span

- Keep it sealed
- Avoid sharp object and not twisting or flexing the media
- Avoid exposing to extreme temperature
- Do not use damaged media
- Transportation from one site to another in temperature-controlled vehicle
- Protect from exposure
- Take precaution from theft
- Encrypt backups

Mobile Devices

Mobile Device Management (MDM)

Enable Encryption, Screen Lock, Global Positioning System (GPS), and remote wipe.

Once backup media has reached its mean time to failure (MTTF), it should be destroyed.

Managing Configuration: Images for Baseline

16.9. Change Management

Request the change

Review the change

Approve/reject the change

Test the change

Schedule and implement the change

Document the change

There may be instances when an emergency change is required. Here, make changes and document change **Versioning:** keeps track of changes over time to deployed software

Configuration documentation: identifies who is responsible, system's purpose, changes to baseline **16.9.1. Patch Management Lifecycle**

Evaluate the patches

Test the patches

Approve the patches

Deploy the patches

Verify that patches are deployed and functioning correctly

16.9.2. Vulnerability Management

Identifying vulnerabilities, evaluating them, and taking steps to mitigate risks associated with them

Vulnerability Scans: tools used to test systems and networks for known security issues

Vulnerability Assessments: more than scans.

E.g. an annual VA may analyze all scan reports of past year to determine if things are addressed

Often done as part of a risk analysis.

VA can look at how sensitive information is marked, handled, stored, and destroyed

17. Preventing and Responding to Incidents

17.1. Managing Incident Response

One of the primary goals of any security program is to prevent security incidents

The primary goal of incident response is to minimize the impact on the organization

Incident

Any event that has a negative effect on the CIA of an assets

Security incident is defined within security policy or incident response plans

17.2. Incident Response Steps

preparation,
detection and analysis,
containment, eradication, and recovery, and
post-incident recovery.

Detection: Incident is triggered and admin is notified. Admin verifies if it really is an incident of interest
Response: Response varies depending on severity of the incident. CIRT handles
Mitigation: contain an incident. E.g. disconnecting a network
Reporting: within/outside organization. Upper management need to know about serious security breaches**.**
Many incidents are not reported because they are not recognized and incidents.
Recovery: recover the system to a fully functioning state. simple reboot/rebuilding a system
If investigators suspect an attacker may have modified code, rebuilding system may be a good option
Remediation: root cause analysis. identify what allowed it to occur, and implement methods to prevent it from happening again
Lesson Learned: it took a long time to contain incident, why? personnel don't have adequate training?

17.3. Basic Preventive Measures

Keep Systems and application up-to-date
Remove or disable unneeded services and protocols
User intrusion detection and prevention systems
Use up-to-date anti-malware software
Use firewalls
Implement configuration and system management processes

17.4. Understanding Attacks

Botnets: defense-in-depth/update-to-date software.
DRDoS: distributed reflective DoS don't attack victim directly, but manipulates traffic so that attacks are reflected back to the victim from other sources. DNS poisoning/smurf attacks
Smurf:

It floods the victim with ICMP echo packets.
Specifically, it is a spoofed broadcast ping request using IP address of victim as source IP
All systems respond with echo replies to the spoofed IP address, flooding the victim with traffic

Fraggle Attacks

Similar to smurf attacks but uses UDP packets over UDP ports 7 and 19
Attack will broadcast a UDP packet using the spoofed IP address of the victim
All systems on the network will then send traffic to the victim

A ping flood attack floods a victim with ping requests.
Very effective when launched by zombies within a botnet as a DDoS attack
Handle this by blocking ICMP traffic. Active IDS can detect a ping flood and block ICMP traffic

Ping of Death

Employs an oversized ping packet.
Ping packets are normally 32 or 64 bytes. PoD changed the size of ping packets to over 64 KB
Patches and updates remove the vulnerability

An attacker fragments traffic in such a way that a system is unable to put data packets back together.
Install system patches. IDS can check for malformed packets

Attacker sends spoofed SYN packets to victim using victim's IP address as both source/destination
Keeping a system up-to-date and filter traffic to detect traffic with identical source/destination **Zero-Day Exploit:** Attack on a system exploiting a vulnerability that is unknown to others
Honeypots and padded cells give administrators an opportunity to observe attacks and may reveal an attack using a zero-day exploit.
MITM: thwarted by keeping systems up-to-date with patches
Sabotage: criminal act of destruction/disruption committed against an organization by an employee
Espionage: malicious act of gathering proprietary/secret/private/sensitive/confidential information

17.5. Malicious Code

drive-by download
Malvertising to spread malware

Pay-per-install: Criminals pay website operators to host their malware and pay for every installation

17.6. Intrusion Detection and Prevention Systems

IDSs are an effective method of detecting many DoS and DDoS attacks

IDS Types

Knowledge-based detection uses signatures and pattern matching

Behavior-based detection compares against baseline. Statistical/anomaly/heuristics

Response Types

Passive Response Notifications sent to admin via email/SMS

Active Response IPS

17.6.1. Host and Network Based IDS

HIDS monitors a single computer or host

NIDS monitors a network by observing network traffic patterns

Application-based IDS monitors specific application traffic between two or more servers

HIDSs can detect anomalies on the host system that NIDSs cannot detect

Switches are often used as a preventive measure against rogue sniffers.

The port used for port mirroring is referred to as a Switched Port Analyzer (SPAN) port *It is unethical and risky to launch counterstrikes against an intruder or to attempt to reverse-hack an intruder's computer system.*

17.6.2. Specific Preventive Measures

Honeypots/Honeynets

Enticement: Placing a system on Internet with open security vulnerabilities and active services

Entrapment: is illegal, occurs when owner solicits visitors to access the site and then charges them. It is entrapment when you trick/encourage someone into performing an illegal or unauthorized action.

False vulnerabilities intentionally implanted in a system in an attempt to tempt attackers

Understanding Padded Cells

A padded cell system is similar to a honeypot, but it performs intrusion isolation using a different approach. When an IDS detects an intruder, that intruder is automatically transferred to a padded cell

Offers fake data to retain an intruder's interest, similar to a honeypot

IDPS transfers intruder into padded cell without informing the intruder that the change has occurred

Can be used as detection methods and to gather evidence for possible prosecution of attackers

Warning Banners

Warning banners inform both authorized and unauthorized users

Typically remind authorized users of the content in acceptable-use agreements

A security boundary for applications. Prevents application from interacting with other applications

Anti-malware applications use sandboxing techniques to test unknown applications.

Application developers use virtualization techniques.

Third party security services

Penetration Testing: A significant danger with penetration tests is that some methods can cause outage.

Ethical Hacking

17.7. Logging, Monitoring, and Auditing

Helps an organization prevent incidents and provide an effective response when they occur

17.7.1. Audit Trails

Audit trails can help detect a wide variety of security violations, software flaws, and performance problems.

Monitoring and Accountability: ensure that subjects can be held accountable for their actions and activities.

17.7.2. Monitoring Techniques

Log Analysis

SIEM

Sampling

Clipping Levels: a form of nonstatistical sampling. It selects events that exceed a level

Keystroke Monitoring

Traffic Analysis and Trend Analysis: monitors flow of packets rather than actual packet content

Egress Monitor outgoing traffic to prevent data exfiltration. DLP/watermarking/ steganography

DLP

Statistical sampling is more reliable and mathematically defensible.

17.7.3. DLP

DLP system doesn't have the ability to decrypt data but can look in the zip files.

Network-Based DLP

Endpoint-Based DLP

17.7.4. Other Terms

Steganography

The practice of embedding a message within a file.

Use hash for detection

Watermarking

Embedding an image or pattern in paper that isn't readily perceivable

It is often used with currency to thwart counterfeiting attempts.

17.8. Auditing

Auditing is a methodical examination or review of an environment to ensure compliance with regulations and to detect abnormalities, unauthorized occurrences, or crimes.

Dual Administrator Accounts: One account for regular day-to-day use and second account have privileges

Security Audits & Reviews: ensure accounts are managed appropriately & management controls are place

Patch Management

Vulnerability Management

Configuration Management

Change Management

17.8.1. Reporting Audit Results

Reports should address

The purpose of the audit

- The scope of the audit
- The results discovered or revealed by the audit

In addition, audit reports often include many details specific to the environment, such as time, date, and a list of the audited systems. They can also include

Problems, events, and conditions

- Standards, criteria, and baselines
- Causes, reasons, impact, and effect
- Recommended solutions and safeguards

Audit reports contain sensitive information, *classify*

18. Disaster Recovery Planning

BCP: art of helping organization assess priorities and design resilient processes that will allow continued operations in the event of a disaster.

DRP includes technical controls that prevent disruptions and facilitate the restoration of service as quickly as possible after a disruption occurs.

A primary goal of system resilience and fault tolerance is to eliminate single points of failure.

Fault tolerance ability of system to suffer a fault but continue to operate

System resilience ability of system to maintain acceptable level of service during an adverse event

18.1. Protecting Various Components

18.1.1. Protecting Hard-Drives

RAID-0 (striping) two or more disks, improves disk subsystem performance, but no fault tolerance

RAID-1 (mirroring) It uses two disks, which both hold the same data. If one disk fails, the other disk includes the data so a system can continue to operate after a single disk fails.

RAID-5 (striping with parity) three or more disks, one holds parity information. Handle 1 disk fail

RAID-10 (RAID 1 + 0 or stripe of mirrors) at least four disks but can support more as long as an even number of disks are added. Continue to operate even if multiple disks fail, as long as at least one drive in each mirror continues to function.

Hot swapping: allows to replace failed disks without powering down the system.

Cold swappable RAID requires the system to be powered down to replace a faulty drive

18.1.2. Protecting Servers

Fault tolerance can be added for critical servers with failover clusters.

A failover cluster includes two or more servers, and if one of the servers fails, another server in the cluster can take over its load

18.1.3. Trusted Recovery

Trusted recovery provides assurances that after a failure or crash, the system is in fail secure state

A fail-secure system will default to a secure state in the event of a failure, blocking all access.

A fail-open system will fail in an open state, granting all access.

Firewalls are typically designed to be fail secure

If availability is more important than security, the firewall be configured fail-open state

In the context of physical security with electrical hardware locks, the terms fail-safe and fail-secure are used. Specifically, a fail-safe electrical lock will be unlocked when power is removed, but a fail-secure electrical lock will be locked when power is removed

Two elements of the recovery process are addressed to implement a trusted solution.

Failure preparation system resilience & fault-tolerant methods in addition to a reliable backup

System recovery The system should be forced to reboot into a single-user, nonprivileged state

The Common Criteria defines four types of trusted recovery:

Manual Recovery If a system fails, it does not fail in a secure state. Instead, an administrator is required to manually perform the actions necessary to implement a secured or trusted recovery after a failure or system crash.

Automated Recovery The system is able to perform trusted recovery activities to restore itself against at least one type of failure. E.g. RAID

Automated Recovery without Undue Loss similar to automated recovery but it includes mechanisms to ensure that specific objects are protected to prevent their loss. Mechanisms to restore corrupted files, rebuild data from transaction logs, and verify integrity of key system and security components

Function Recovery Systems automatically recover specific functions. Complete the recovery for the functions, or roll back the changes to return to a secure state

18.1.4. Quality of Service

Quality of service (QoS) controls protects the integrity of data networks under load.

Bandwidth

Latency delay in delivering packet

Jitter variation in latency between different packets.

Packet Loss disappearance of packet in transit that requires retransmission

Interference Electrical noise, faulty equipment may corrupt the contents of packets

For example, a QoS device might be programmed to prioritize videoconference traffic from the executive conference room over video streaming from an intern's computer.

18.2. Alternate Processing Sites

18.2.1. Cold Sites

Standby facilities to handle processing load and equipped with electrical/environmental support

A cold site has no computing facilities (hardware or software) preinstalled

18.2.2. Hot Sites

Backup facility maintained in constant working order, with a full complement of original site

The hot site has up-to-date data

Means to reduce cost of host site. 1) Shared hot site facility managed by an outside contractor. 2) Use hot site as a development or test environment.

18.2.3. Warm Sites

They always contain the equipment and data circuits necessary to rapidly establish operations.

Warm sites do not typically contain copies of the client's data.

Activation of a warm site typically takes at least 12 hours from the time a disaster is declared.

18.2.4. Mobile Sites

Typically consist of self-contained trailers or other easily relocated units.

These sites include all environmental control systems necessary to maintain a safe environment

If your disaster recovery plan depends on a workgroup recovery strategy, mobile sites are an excellent way to implement that approach.

18.2.5. Service Bureaus

A service bureau is a company that leases computer time.
Any organization can purchase a contract

18.2.6. Alternate Processing Sites: Cloud Computing

Many organizations now turn to cloud computing as their preferred disaster recovery option

18.2.7. Mutual Assistance Agreements

Reciprocal agreements: two organizations sharing computing facilities. It is cheapest
Drawbacks:
Difficult to enforce. Trust issue
Confidentiality concerns
Proximity concerns

18.3. Database Recovery

Electronic Vaulting

Database backups are moved to a remote site using bulk transfers
Significant delay in database being ready
Introduces the potential for significant data loss. Only able to recover backup of last vault

Remote Journaling

Data transfers occurs in a bulk, but on a more frequent basis, hour/more frequently
Transfer copies of the database transaction logs/journal

Remote Mirroring

The most expensive! a live database server is maintained at the backup site
Popular database backup strategy for a hot site

18.4. Recovery Plan Development

Executive summary providing a high-level overview of the plan
Department-specific plans
Technical guides for implementing and maintaining critical backup systems
Checklists for individuals on the disaster recovery team
Full copies of the plan for critical disaster recovery team members

18.5. Emergency Response

Put the most essential tasks ("Activate the building alarm") first on the checklist.
Emergency-response plans in the form of checklists
A list of personnel to contact in the event of a disaster.
First tasks assess the situation

18.6. Backups and Offsite Storage

Full Backups store a complete copy of the data contained on the protected device.
Full backups duplicate every file on the system regardless of the setting of the archive bit
Once a full backup is complete set to 0.

Incremental Backups store only those files that have been modified since last backup
Only files that have the archive bit turned on, enabled, or set to 1 is duplicated
Once an incremental backup is complete set to 0

Differential Backups backs up only the files that changed since last full back
Only files that have the archive bit turned on, enabled, or set to 1 is duplicated.
This process does not change the archive bit

Full and differential backups: *only two backups*; recent full backup and recent differential backup.
Full backups with incremental backups: *recent full backup and all incremental backups*
Differential backups don't take long to restore, but take longer to create than incremental ones

18.6.1. Disk-to-Disk Backup

Virtual tape libraries (VTL) support use of disks by using software (makes disk storage appear as tapes) Hire managed service providers to manage remote backup locations.
Alternative: cloud-based backup solutions

18.6.2. Best Backup Practices

Schedule during the low peak periods
Build sufficient capacity to handle a growth
Murphy's law: server never crashes immediately after a successful backup. It is always just before the next backup begins. Use real-time continuous backup like RAID, clustering, or server mirroring
Test recovery processes

18.6.3. Tape Rotation

Grandfather-Father-Son (GFS) [Month, week, day], Tower of Hanoi, and Six Cartridge Weekly Backup

An hierarchical storage management (HSM) system is an automated robotic backup jukebox consisting of 32 or 64 optical or tape backup devices. All the drive elements within an HSM system are configured as a single drive array (a bit like RAID).

Software Escrow Arrangements: Protects a company against the failure of a software developer

External Communications: contact vendors to provide supplies

Utilities: electric power, water, natural gas, sewer service, and so on

Logistics and Supplies: moving large numbers of people, equipment, and supplies to alternate recovery sites

Separate disaster recovery tasks from disaster restoration tasks

Recovery: brings business operations and processes back to a working state

Restoration: brings a business facility and environment back to a workable state

Disaster recovery team: to implement and maintain operations at the recovery site

Salvage team: to restore the primary site to operational capacity

18.7. Training, Awareness and Documentation

Orientation training for all new employees

Initial training for employees taking on a new disaster recovery role for the first time

Detailed refresher training for disaster recovery team members

Brief awareness refreshers for all other employees

Loose-leaf binders are an excellent way to store disaster recovery plans

18.8. Testing and Maintenance

Read-Through/Checklist Test

Simplest but critical. Distribute copies of plans to recovery team for review

Ensures key personnel are aware of their responsibilities

Opportunity to review obsoletes information and update

Identify situations in which key personnel have left the company and nobody reassigned.

A good reason to include recovery responsibilities in job descriptions

Structured Walk-Through Test: Table-top exercise, role-play a disaster scenario

Simulation Test:

Similar to structured.

Team members are presented with a scenario and asked to develop an appropriate response

May involve interruption of noncritical business activities and the use of some operational personnel

Parallel Test

Relocating personnel to alternate site and implementing activation procedures

Main facility are not interrupted

Involves shutting down operations at primary site and shifting to recovery site

Involve a significant risk

Disaster recovery plan is a living document.

As needs change plan must be adapted to meet those needs

19. Investigations and Ethics

19.1. Types of Investigations

Administrative Investigations

Internal investigations that examine operational issues or policies violation

Operational investigations examine issues related to the organization's computing infrastructure and have the primary goal of resolving operational issues. E.g. Performance issues on web servers

Operational investigations: loosest standards and are not intended to produce evidence

Operational investigations: conducts root cause analysis

Do not involve law enforcement

They use weaker preponderance of the evidence standard. outcome of case is more likely than not

Regulatory Investigations

Government agencies may conduct if administrative law is violated

Some may not involve government agencies. PCI DSS

19.2. Electronic Discovery

Facilitates the processing of electronic information for disclosure. The eDiscovery Reference Model steps:

Information Governance organize information for eDiscovery
Identification locate information when litigation is likely
Preservation protect integrity of discoverable information
Collection gather information centrally
Processing *rough cut* irrelevant information
Review examines remaining information. Remove information protected by attorney-client privilege
Analysis deeper inspection of content/context of remaining information
Production place information into format that may be shared with others
Presentation display information to witnesses, the court, and other parties

19.3. Evidence

19.3.1. Admissible Evidence

relevant determining a fact
material related to the case
competent must have been obtained legally

19.3.2. Types of Evidence

Real evidence (object evidence) consists of things that may actually be brought into a court of law.

- murder weapon/clothing/ keyboard with fingerprint/HDD.
- Real evidence may also be conclusive evidence. DNA

Documentary Evidence any written items. must be authenticated like testified logs

Two additional evidence rules apply specifically to documentary evidence:

- The **best evidence rule** original document must be introduced. Copies not be accepted
- The **parol evidence rule** written agreement contains all the terms and can't be modified

Testimonial evidence consists of testimony of a witness verbal/written. Must not be **hearsay evidence**.

19.3.3. Chain of Evidence

A chain of evidence/custody: documents everyone who handles evidence. The label should include

General description of the evidence
Time and date the evidence was collected
Exact location the evidence was collected from
Name of the person collecting the evidence
Relevant circumstances surrounding the collection

19.3.4. Evidence Collection and Forensic

The International Organization on Computer Evidence (IOCE) outlines six principles

All general forensic and procedural principles be applied
Evidence should not change
Person to be trained to access original digital evidence
Seizure/access/storage/transfer evidence be fully documented/preserved/available for review
An individual in possession of evidence is responsible for all actions
Any agency seizing/accessing/storing/transferring digital evidence is responsible for compliance **Media Analysis** involves the identification and extraction of information from storage media.

Network forensic analysis depends network activity log. IDS/IPS, Netflow, Packet capture, firewall logs **Software Analysis** reviews of applications/activity that takes place within a running application

- Review of software code, looking for back doors, logic bombs, or other security vulnerabilities
- Review application/database log, SQL injection attacks, privilege escalations, or application attacks

Hardware/Embedded Device Analysis review contents of hardware and embedded devices

- Personal computers, Smartphones, Tablet computers, Embedded computers in cars, security systems

19.4. Investigation Process

Gathering Evidence

Three-confiscation process

First, voluntarily surrender it
Second, get a court to issue a **subpoena**. Evidence could be altered…
The last option is a search warrant

No investigation on actual compromised system. Make a backup, and use it to investigate
Never attempt to "hack back" and avenge a crime.
If in doubt, call in expert assistance

Interviewing Individuals

Interview: to gather information

Interrogation: gather information from suspected

Reporting and Documenting

Preparing formal documentation lays the foundation for escalation and potential legal action

19.5. Major Categories of Computer Crimes

Military and Intelligence Attacks

To obtain secret and restricted information from military and technological research sources.

Disclosure could compromise investigations, disrupt military planning, threaten national security **Business Attacks:** Focus on illegally obtaining an organization's confidential information

Financial Attacks:

To unlawfully obtain money or services

Goal is to steal credit card numbers, increase the balance in a bank account

Shoplifting and burglary are both examples of financial attacks.

Terrorist Attacks

To disrupt normal life and instill fear

Targets could be power plants or telecommunications or power distribution

Grudge Attacks

To damage an organization or a person

Loss of information or information processing capabilities or harm to organization or reputation

Thrill Attacks

Attack launched for fun. Script kiddies. - Website defacements

19.6. Ethics

(ISC)2 Code of Ethics Preamble

The safety and welfare of society and the common good, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons

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

19.6.1. Ethics and the Internet

Unacceptable and unethical activities

Seeks to gain unauthorized access to the resources of the internet

Disrupts the intended use of the internet

Wastes resources (people, capacity, computer) through such actions

Destroys the integrity of computer-based information

Compromises the privacy of users

19.6.2. Ten Commandments of Computer Ethics

Shall not use computer to… other people computing system

Harm/interfere/snoop/steal/bear false witness/copy proprietary software/appropriate intellectual o/p use computer resources without authorization/compensation

Think about the social consequences of the program

Always use a computer in ways that ensure consideration and respect

19.6.3. Domain 7: Miscellaneous Points

A system *cold start* takes place when an unexpected kernel or media failure happens

An *emergency system restart* takes place after a system failure happens in an uncontrolled manner

A *system reboot* after system shuts itself down in a controlled manner in response to a kernel failure

Gold Master image workstation/server that includes properly configured and authorized software

The *work recovery time (WRT)* is the remainder of the overall MTD value after the RTO has passed.

An RTO is the amount of time it takes to recover from a disaster, and an RPO is the amount of acceptable data, measured in time, that can be lost from that same event.

High availability (HA) some specific thing is always up and running. Database/network/Apps

Network analysis	**Software** analysis
• Traffic analysis • Log analysis ! • Path tracing	• Reverse engineering ! • Malicious code review • Exploit review

Media analysis • Disk imaging ! • Timeline analysis (modify, access, create) • Registry analysis ! • Slack space analysis ! • Shadow volume analysis	**Hardware**/embedded **device analysis** • Dedicated appliance attack points ! • Firmware and dedicated memory inspections ! • Embedded operating systems, virtualized software, and hypervisor analysis

A legal exception to hearsay rule **business records exception** rule or business entry rule

Under this rule, a party could admit any records of a business

- (1) that were made in the regular course of business;
- (2) that the business has a regular practice to make such records;
- (3) that were made at or near the time of the recorded event; and
- (4) that contain information transmitted by a person with knowledge

Cipher locks, programmable locks, use keypads to control access into an area or facility.

Disaster recovery deals with actions that need to take place right after the disaster, and business continuity deals with the actions that need to take place to keep operations running

Steps for developing a disaster recovery plan are

Develop the continuity planning policy statement ○ **Conduct the BIA**

- ○ **Identify preventative controls**
- ○ **Develop recovery strategies** ○ **Develop contingency plan**
- ○ **Test the plan and conduct training and exercise**
- ○ **Maintain the plan**

Exigent circumstances: If probable cause exists and the destruction of evidence is imminent, that evidence may be searched or seized without a warrant.

Operational-level agreements (OLAs) and underpinning contracts (UCs) are important SLA supporting documents. An OLA is essentially an SLA between the different interdependent groups that are responsible for the terms of the SLA. UCs are used to manage third-party relationships with entities that help support the SLA, such as an external service provider or vendor.

DOMAIN 8: Software Development Security

20. Software Development Security

20.1. Programming Language

C, Java, and FORTRAN are compiled languages

Python, R, JavaScript, and VBScript are interpreted languages

Compiled code is generally less prone to manipulation by a third party.

But easier to embed back doors and other security flaws in the code and escape detection

Interpreted code is less prone to the undetected insertion of malicious code

20.1.1. Object Oriented Programming

Message is a communication to or input of an object

Method is internal code that defines actions an object performs in response to a message

Behavior Behaviors are results of message being processed through a method

Class collection of the common methods that defines the behavior of objects

Instance Objects are instances of or examples of classes that contain their methods

Inheritance methods from a class (parent or superclass) are inherited by another subclass (child)

Delegation forwarding of a request. Object delegates if it does not have method to handle message

Polymorphism respond with different behaviors to the same message

Cohesion describes the strength of relationship between purposes of methods within same class

Coupling level of interaction between objects

Lower coupling provides better software design, as objects are more independent.

Lower coupling is easier to troubleshoot update.

Objects that have low cohesion require lots of assistance from other objects to perform tasks and have high coupling.

Low coupling and high cohesion is desirable

20.2. Avoiding and Mitigating System Failure

Input Validation

Input validation / limit check/ escaping input

Input validation should always occur on the server side of the transaction

Authentication and Session Management

Authentication required by an application should be tied directly to the level of sensitivity

Developers should use established methods for session management

Error Handling

Error messages may expose structure of database, addresses of internal servers, reconnaissance data

Disable detailed error messages

Logging: Applications should be configured to send detailed logging of errors/security events to SIEM The OWASP Secure Coding Guidelines

Input validation failures, Authentication attempts, especially failures, Access control failures, Tampering attempts, Use of invalid or expired session tokens, Exceptions raised by the operating system or applications, Use of administrative privileges, Transport Layer Security (TLS) failures, Cryptographic errors

Fail-Secure and Fail-Open

The fail-secure failure state puts the system into a high level of security

The fail-open state allows users to bypass failed security controls

20.3. System Development Lifecycle

All systems development processes should have several activities in common.

20.3.1. Conceptual Definition

Creating the basic concept statement for a system

Statement agreed on by all interested stakeholders (developers, customers, and management)

A very high-level SoP and should not be longer than one or two paragraphs

20.3.2. Functional Requirements Determination

Specific system functionalities are listed.

Functional requirements should be expressed in a form consumable by software developers.

Three major characteristics of a functional requirement:

Input(s) The data provided to a function

Behavior The business logic describing actions to different inputs

Output(s) The data provided from a function

20.3.3. Control Specifications Development

During the development of control specifications, analyze following

Adequate access controls must be designed into every

System must maintain the confidentiality of vital data

System should provide both an audit trail and a detective mechanism for illegitimate activity

Finally, availability and fault-tolerance issues should be addressed as corrective actions

20.3.4. Design Review

The designers determine exactly how the various parts of the system will interoperate and how the modular system structure will be laid out.

Also, during this phase the design management team commonly sets specific tasks for various teams and lays out initial timelines for the completion of coding milestones.

20.3.5. Code Review Walk-Through

Development personnel walk through specific code module, looking for problems in flow/flaws

20.3.6. User Acceptance Testing

Developers and actual users validate the system against predefined scenarios

20.3.7. Maintenance and Change Management

Once a system is operational, a variety of maintenance tasks ensure continued operation in the face of changing operational, data processing, storage, and environmental requirements.

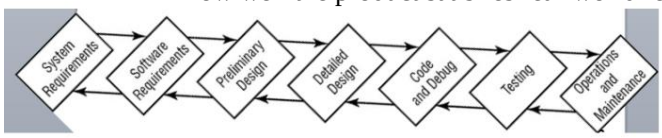
Requirements gathering	Security/Privacy risk assessment, Risk-level acceptance, Informational, functional, and behavioral requirements
Design	Attack surface analysis, Threat modeling
Development	Automated CASE tools, Static analysis
Testing/validation	Dynamic analysis, Fuzzing, Manual, Unit, integration, acceptance, regression
Release/Maintenance	Final security review

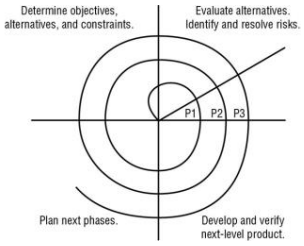
20.4. Lifecycle Model

20.4.1. Waterfall Model

It allows the developers to step back only one phase in the process
It does not make provisions for the discovery of errors at a later phase in the development cycle.
The waterfall model was improved by adding validation and verification steps to each phase.

Verification evaluates the product against specifications, whereas validation evaluates how well the product satisfies real-world requirements.





20.4.2. Spiral Model

Because the spiral model encapsulates a number of iterations of another model (the waterfall model), it is known as a metamodel, or a "model of models.

Spiral model provides a solution to the major criticism of the waterfall model—it allows developers to return to the planning stages as changing technical demands and customer requirements necessitate the evolution of a system.

20.4.3. Agile Software Development

- Individuals and interactions over processes and tools
- Working software over comprehensive documentation
- Customer collaboration over contract negotiation
- Responding to change over following a plan

20.4.4. Software Capability Maturity Model

Initial

Hardworking people charging ahead disorganized. Little/no defined software dev. process

Repeatable

Basic lifecycle management processes are introduced.
Reuse of code in organized fashion begins, and repeatable results are expected from similar projects
SEI (Software Engineering Institute) key: Requirements Management, Software Project Planning, Software Project Tracking and Oversight, Software Subcontract Management, Software Quality Assurance, and Software Configuration Management.

Defined

Software developers operate according to set of formal/documented software development process
All development projects take place within constraints of the new standardized management model
SEI key: Organization Process Focus, Organization Process Definition, Training Program, Integrated Software Management, Software Product Engineering, Intergroup Coordination, and Peer Reviews

Managed

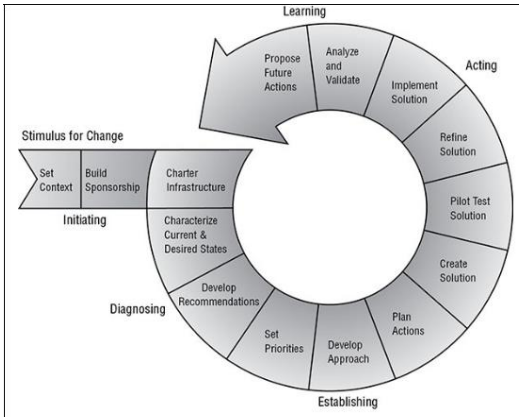
Quantitative measures are utilized to gain a detailed understanding of the development process.
SEI key: Quantitative Process Management and Software Quality Management

Optimizing

A process of continuous improvement occurs.
Sophisticated software development processes are in place that ensures that feedback from one phase reaches to the previous phase to improve future results.
SEI key: Defect Prevention, Technology Change Management, and Process Change Management.

20.4.5. IDEAL Model

IDEAL Model	Gantt Charts and PERT
	A **Gantt chart** shows interrelationships over time between projects/ schedules. **Program Evaluation Review Technique (PERT)** is a project-scheduling tool used to judge the size of a software product in development and calculate the standard deviation (SD) for risk assessment. PERT relates the estimated lowest possible size, the most likely size, and the highest possible size of each component. PERT is used to direct improvements to project management and software coding in order to produce more efficient software. As the capabilities of programming and management improve, the actual produced size of software should be smaller.



20.5. Change and Configuration Management

The change management process has three basic components:

Request Control

Users request modifications, managers conduct cost/benefit analysis, and developers prioritize tasks

Change Control

Developers re-create the situation and analyze appropriate changes to remedy situation

Change control includes conforming to quality control restrictions, developing tools for update or change deployment, properly documenting any coded changes, and restricting the effects of new code to minimize diminishment of security

Release Control

Once the changes are finalized, they must be approved for release through the release control

Ensure debugging code and/or back doors is removed

Acceptance testing

Configuration Identification admin documents configuration of covered software products

Configuration Control ensures changes are made in accordance with change control

Configuration Status Formalized procedures to keep track of all authorized changes

Configuration Audit periodic configuration audit

The DevOps Approach: Agile approach to decrease time to develop, test, and deploy software changes

API: Like passwords

20.6. Software Testing

Create test cases coordinating with developers at the initial phase

Reasonableness check: ensures values returned match specified criteria

White-box testing examines the internal logical structures of a program line by line

Black-Box Testing examines from a user perspective. Final acceptance testing is an example

Gray-Box Testing popular for software validation. Examines from user perspective but also have access to the source code to help design test cases. Do not analyze inner workings

Static Testing use of automated tools to detect common software flaws like buffer overflows

Dynamic Testing no access to the underlying source code. Web app scanning

20.7. Databases

Hierarchical Databases

Combines records and fields that are related in a logical tree structure

This results in a one-to-many data model

Distributed Databases

Data is stored in more than one database, but are logically connected.

Each field can have numerous children as well as numerous parents. Many-to-many data mapping

Relational Databases

Two-dimensional tables made up of rows and columns

Tuple is the individual row in relational database. Column is attribute.

The number of rows is cardinality, the number of columns is degree.

The domain of an attribute is the set of allowable values that the attribute can take

Candidate Keys is a *subset of attributes* used to uniquely identify any record in a table

Primary Keys is selected from the set of candidate keys used to uniquely identify the records
Foreign Keys to enforce relationships between two tables, known as referential integrity
Data Definition Language (DDL) allows for creation/modification of database's structure (schema)
Data Manipulation Language (DML) allows users to interact with data contained within that schema.
Object-oriented databases (OODBs): code reuse/troubleshooting, and reduced overall maintenance
OODBs better suited for complex applications multimedia/CAD/video/graphics/expert systems

Database Transaction

Relational databases support explicit/implicit use of transactions to ensure data integrity.
Each transaction will either succeed/fail as group

Atomicity database transactions must be *all-or-nothing*. Any part fails, rollback entire transaction
Consistency all transactions must be consistent with all database's rules
No transaction use inconsistent data that might be generated in execution of another transaction
Isolation one transaction must complete before other is allowed. Prevents working with invalid data
Durability once committed to the database must be preserved. Ensure through use of backup/logs

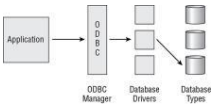
Security of Multilevel Databases

Database contamination: Mixing data with different classification levels and/or need-to-know.
Deploy a trusted front end to add multilevel security
Concurrency (edit control) information stored is always correct. Failing will result in
Lost updates two different processes make updates to database
Dirty reads a process reads a record from a transaction that did not successfully commit
Concurrency uses a *lock* feature to allow one but deny other at the same time
Database views: collate data, aggregate records, restrict user access to data

20.7.1. Other Security Mechanisms

Semantic integrity ensures actions don't violate rules, data types in valid domain, only logical values exist, and system complies with any and all uniqueness constraints
Employ timestamp to maintain data integrity and availability
Content-dependent access control is based on the contents of object. Increases processing overhead
Cell suppression hiding cells or imposing more security restrictions
Context-dependent access control based on how each object/field relates to overall activity
Database partitioning subvert aggregation and inference vulnerabilities
Polyinstantiation two or more rows in database have identical primary key with different data for use at differing classification levels. Defense against inference attacks
Perturbation (noise): false data to protect confidentiality

20.7.2. ODBC



Allows applications to communicate with different types of databases
ODBC acts as a proxy between applications and backend database drivers

20.7.3. NoSQL

Class of databases that use models other than the relational model to store data
Major classes of NoSQL
Key/value simplest form of database
Graph nodes represent object and edge represent relationships. Social networks/geographic locations
Document key/value but is more complex and in document form. XML, JSON

20.8. Storing Data and Information

Primary Memory, Secondary Storage
Virtual memory simulates additional primary memory through the use of secondary storage
Virtual storage simulates secondary storage resources through primary. Fast filesystem but volatile
Random access storage request contents from any point. RAM/hard drives
Sequential access storage magnetic tape
Volatile storage RAM
Nonvolatile storage

20.8.1. Storage Threats

implement access controls
use encryption
for multilevel security set up with fail-safe controls
In cloud computing: a single misconfiguration can publicly expose sensitive information on the web

20.9. Knowledge Based Systems

Expert System: components

Knowledge base contains rules

Inference engine analyzes knowledge base to arrive at decision. Uses a combination of logical reasoning and fuzzy logic techniques

Only as good as data in knowledge base and the decision algorithms in inference engine

Advantage: decisions not clouded by emotion. Important in emergency/stock trading

Machine Learning: Supervised, Unsupervised and Semi-Supervised

Neural Networks: imitate the biological reasoning process of the human mind

Delta rule or learning rule: neural networks are able to learn from experience

21. Malicious Code and Application Attacks

APTs attackers have access to zero-day exploits that are not known to software vendors.

Logic bombs

Trojan horse

Worms

21.1. Virus

Computer viruses have two main functions—propagation and destruction. Virus Propagation Techniques

Master Boot Record These viruses attack the MBR

File Infector Viruses Infect different types of executable files

Companion virus self-contained executable files that escape detection by using a filename. ○ For example, if you had game.exe, a companion virus might use the name game.com.

Macro Viruses Use simple, yet powerful programming languages such as VBA

Service Injection Viruses injects themselves into trusted runtime processes of the OS, such as svchost.exe, winlogin.exe, and explorer.exe.

Types

Multipartite viruses use more than one propagation technique

Stealth viruses hide themselves by actually tampering with the OS to fool antivirus packages

Polymorphic viruses modify their own code as they travel from system to system.

Encrypted viruses use cryptographic techniques to avoid detection

21.2. Code Red Worm

Code Red performed three malicious actions on the systems it penetrated:

It randomly selected hundreds of IP addresses and probed if vulnerable version of IIS is running. Any systems it found were quickly compromised.

It defaced HTML pages on the local web server, replacing normal content with the following text:

Welcome to http://www.worm.com!

Hacked By Chinese!

It planted a logic bomb that would initiate a denial-of-service attack against the IP address 198.137.240.91, which at that time belonged to the web server hosting White House's home page.

21.3. Stuxnet

Stuxnet uses the following propagation techniques:

Searching for unprotected administrative shares of systems on the local network

Exploiting zero-day vulnerabilities in the Windows Server service and Windows Print Spooler

Connecting to systems using a default database password

Spreading by the use of shared infected USB drives

21.4. Spyware

It monitors actions and transmits important details to a remote system.

Spyware might wait for you to log into a banking website and then transmit your username/password

21.5. Adware

Displays advertisements on infected computers. Display pop-up ads on your screen while you surf

May monitor your shopping behavior and redirect you to competitor websites

21.6. Application Attacks

Buffer overflow vulnerabilities exist when a developer does not properly validate user input

TOCTOU issue is a timing vulnerability

Back doors are undocumented command sequences that allow to bypass normal access restrictions.

Escalation-of-privilege attacks: expanding access from the normal user account to more admin

Rootkits: common ways that attackers wage escalation-of-privilege attacks

21.6.1. Web Application Attacks

XSS

XSRF. One way to protect against XSRF is to use secure token that attacker would not know.

SQL Injection. Use prepared statements, Perform input validation and Limit Account Privileges.

Cross-site tracing (XST) leverages the HTTP TRACE or TRACK methods and could be used to steal a user's cookies via cross-site scripting (XSS).

21.7. Reconnaissance Attacks

IP Probes, Port Scans, Vulnerability Scans

21.8. Masquerading Attacks

IP Spoofing attack. To prevent such attacks configure filters each network as

Packets with internal source IP addresses don't enter the network from the outside.

Packets with external source IP addresses don't exit the network from the inside.

Packets with private IP addresses don't pass through the router in either direction

Session Hijacking

Attacker intercepts part of the communication of authorized user and takes over the session. Techniques:

Capturing details of the authentication

Tricking the client into thinking the attacker's system is the server, acting as the middleman as the client sets up a legitimate connection with the server, and then disconnecting the client

Accessing a web application using cookie data of user who did not properly close the connection

21.8.1. Domain 8: Miscellaneous Points

Attack surface analysis identify/reduce amount of code/functionality accessible to untrusted users

V-shaped model Each phase be completed before the next phase begins. But model requires testing throughout the development phases and not just waiting until the end. It is still rigid and not flexible.

Garbage collection way for software to carry out part of its memory management tasks

Joint Analysis Development (JAD) A method that uses a team approach in application development in a workshop-oriented environment.

Modularity Autonomous objects, cooperation through exchanges of messages

A *semantic integrity* mechanism makes sure structural and semantic rules are enforced.

A database has *referential integrity* if all foreign keys reference existing primary keys.

Entity integrity guarantees that the tuples are uniquely identified by primary key values.

Path or directory traversal This attack is also known as the "dot dot slash" because it is perpetrated by inserting the characters "../" several times into a URL to back up or traverse into directories that weren't supposed to be accessible from the Web.

Object-oriented design (OOD) representation of a real-world problem and maps it to a software

The *Component* Object *Model (COM)* allows for interprocess communication within one application or between applications on the same computer system.

The *Distributed Component Object Model (DCOM)* supports the same model for component interaction, and also supports *distributed* interprocess communication (IPC)

1st gen: machine language (binary format).

2nd gen assembly language.

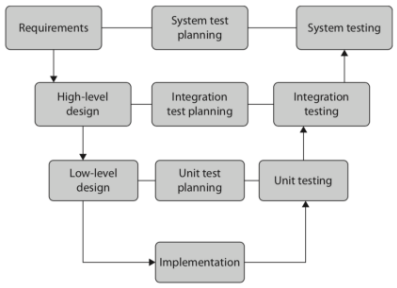
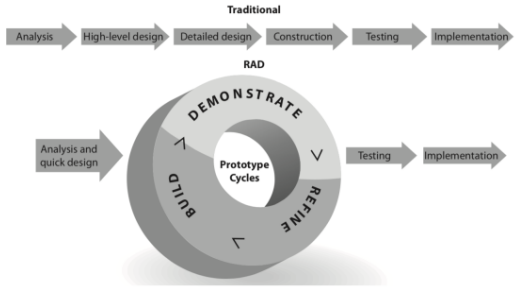
3rd gen high-level language FORTRAN, COBOL, BASIC, Pascal, C/C++ and Java.

4th gen very high-level language (provides more programming abstraction) SQL.

5th gen five is natural language (artificial intelligence purposes).

An **object request broker** (ORB) manages communications between objects and enables them to interact in a heterogeneous and distributed environment.

Common Object Request Broker Architecture (CORBA) provides a standardized way for objects within different applications, platforms, and environments to communicate. It accomplishes this by providing standards for interfaces between objects.

V-Model	RAD
	

The ***Rapid Application Development (RAD):*** combines use of prototyping and iterative development procedures (also involves customer) accelerating the software development process

Scrum works in sprints while ***Kanban*** stresses on visual tracking of all tasks

Exploratory model where clearly defined project objectives have not been presented

Joint Application Development (JAD) team approach in a workshop-oriented environment. It is common to find executive sponsors, subject matter experts, and end users in workshops

Cleanroom Attempts to prevent errors/mistakes by following structured/formal methods of developing and testing. It is used for high-quality and mission-critical applications

22. Miscellaneous Left-out Bullets

ActiveX: It is a technology from Microsoft, which enables different software applications to share information and functionality. The idea is that the applications don't need to be created from scratch; many of the functions can be shared among applications. E.g. Spell checking. It originated as OLE (object linking and embedding) that evolved from the idea of COM. Spell checker ActiveX object is simple example of COM. Spell checker is an independent module and any application can access it.

ActiveX = COM

COM Objects allow one program to be embedded into another. E.g. excel spreadsheet could be edited from within word.

An injection attack is any exploitation that allows an attacker to submit code to a target system in order to modify its operations and/or poison and corrupt its data set.

SQL injection attacks are even riskier than XSS attacks from an organization's perspective because the targets of a SQL injection attack are organizational assets, whereas the targets of an XSS attack are customers or visitors to a website. SQL injection attacks use unexpected input to alter or compromise a web application. However, instead of using this input to attempt to fool a user, SQL injection attacks use it to gain unauthorized access to an underlying database and related assets.

SQL injection is a vulnerability of the script used to handle the interaction between a front end (typically a web server) and the backend database. If the script was written defensively and included code to escape (invalidate or reject) metacharacters, SQL injection would not be possible.

XML injection is another variant of SQL injection, where the backend target is an XML application.

XML exploitation is a form of programming attack that is used to either falsify information being sent to a visitor or cause their system to give up information without authorization. One area of growing concern in regard to XML attacks is Security Association Markup Language (SAML).

Cross-site scripting (XSS) is a form of malicious code-injection attack in which an attacker is able to compromise a web server and inject their own malicious code into the content sent to other visitors.

For the administrator of a website, defenses against XSS include maintaining a patched web server, using web application firewalls, operating a host-based intrusion detection system (HIDS), auditing for suspicious activity, and, most important, performing server-side input validation for length, malicious content, and metacharacter filtering. As a web user, you can defend against XSS by keeping your system patched, running antivirus software, and avoiding nonmainstream websites.

The main purpose of XSRF is to trick the user or the user's browser into performing actions they had not intended or would not have authorized. This could include logging out of a session, uploading a site cookie, changing account information, downloading account details, making a purchase, and so on.

exploit that used XSRF is Zeus

Website administrators can implement prevention measures against XSRF by requiring confirmations or reauthentication whenever a sensitive or risky action is requested by a connected client.

A directory traversal is an attack that enables an attacker to jump out of the web root directory structure and into any other part of the filesystem hosted by the web server's host OS.

Security Architect: Responsible for the enterprise security architecture. Will it enhance core security principles

Security Practitioner: Responsible for tactical and operation elements

Security professional: Responsible for managerial oversight

Security officer: responsible to ensure that information presented to management is based upon real need

Data owners also need to determine the criticality, sensitivity, retention, backups, and safeguards for the information. Understand the risks that exist with regards to the information that they control

Information system professionals: design security controls into information systems, testing the controls, and implementing the systems in production environments through agreed upon operating policies and procedures

Security administrator: manages user request process and ensure that privileges are provided

Network/System Admin: Configures network and server hardware/os

Administrative assistant/secretaries: who greets visitors, signs packages in and out, serve as phone screener etc.

Properties of control framework: Consistent, measurable, standard, comprehensive, modular

Wassenaar Arrangement: control of arms and dual-use goods and technologies

The Organization for Economic Cooperation and Development (OECD) has broadly classified privacy principles (collection, use, retention, and disclosure of personal information) into collection limitation, data equality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

Incident: Security event that compromises CIA

Breach: incident that results in disclosure of data

Data disclosure: Breach for which it was confirmed that data was actually disclosed to unauthorized party

GLBA: applies to financial institutions and provides for the implementation of standards to limit the purposeful disclosure of and protect against un-authorized access to consumers' nonpublic personal information

The U.K. Privacy and Electronic Communication (EC Directive) Regulation (PECR) implementation contained wide-ranging rules on marketing and advertising by telephone, fax, email, and text message, as well as rules relating to cookies and security breaches. The breach notification requirements contained apply to ECS providers (telecom, ISPs). 24hrs notify

US SOX Act introduced accounting reform and requires attestation to the accuracy of financial reporting documents. If companies do not have a code of ethics, they must explain why they have not adopted one.

The computer game fallacy: If the computer or system did not take any action or have any mechanism to stop the attack, it must be OK.

The law-abiding citizen fallacy: Writing a virus is not illegal, so it must be OK.

The shatterproof fallacy: Computers cannot do any real harm. The worst that can happen is a deleted file or erased program.

The candy-from-a-baby fallacy: If it is so easy to copy a program or download a song, how can it be illegal?

The hacker fallacy: Information should be free. No one should have to pay for books or media.

National Computer Ethics and Responsibilities campaign (NCERC): electronic repository of information resources, training materials and sample ethics codes for IS managers and educators

Golden Rule: Treat other as you wish to be treated

Kant's Categorical Imperative: If an action is not right for everyone, it is not right for anyone

Descartes' rule of change (Slippery slope): If an action is not repeatable at all times, it is not right at any time.

Utilitarian Principle (Universalism): Take the action that achieves the most good.

Risk Aversion Principle: Incur least harm or cost

Avoid Harm: do no harm

No Free lunch rule: Assume property and information belong to someone.

Legalism: is it against the law?
Professionalism: Is an action contrary to codes of ethics?
Client/Customer Choice: let the people affected decide
Equity: Will the costs and benefits be equitably distributed?
Financial risks can be quantified in many cases. Calculated as: P(probability of harm)*M(Magnitude of harm)=C(cost of prevention).
COSO (Committee of sponsoring organizations of the Treadway Commission): factors that lead to fraudulent financial reporting and produced recommendations for public companies, their auditors, the security exchange commission, and other regulators. Internal controls necessary to meet financial reporting and disclosure objectives
Control environment
Risk assessment
Control activities
Information and communication
Monitoring
CRAMM (CCTA Risk analysis and Management Method): provides a staged and disciplined approach embracing both technical and non-technical aspects of security. Three stages: asset identification and valuation, threat and vulnerability assessment, and countermeasure selection and recommendation.
Failure Modes and Effect Analysis: it examines potential failures of each part/module and examines effects of failure
FRAP (Facilitated Risk Analysis Process): make a base assumption that a narrow risk assessment is the most efficient way to determine risk in a system, business segment, application, or process.
OCTAVE: is a self-directed information security risk evaluation; where people from an organization manage and direct an information security risk evaluation. OCTAVE criteria are a set of principles, attributes, and outputs.
Spanning Tree Analysis: creates a tree of all possible threats. Branches are general categories as network threat, physical threats etc.
Baiting Attack: attacker leaves a malware infected CD/USB in different location
IaaS focuses on providing "bare metal" or basic computing resources. PaaS offers OS/database. SaaS only the data

It is important for data owners to establish and document the following (if applicable):

- The ownership, intellectual property rights, and copyright of their data
- The statutory and non-statutory obligations relevant to their business to ensure the data is compliant
- The policies for data security, disclosure control, release, pricing, and dissemination
- The agreement reached with users and customers on the conditions of use, set out in a signed memorandum of agreement or license agreement, before data is released

It is important for data owners to establish and document the following (if applicable):

- The ownership, intellectual property rights, and copyright of their data
- The statutory and non-statutory obligations relevant to their business to ensure the data is compliant
- The policies for data security, disclosure control, release, pricing, and dissemination
- The agreement reached with users and customers on the conditions of use, set out in a signed memorandum of agreement or license agreement, before data is released

Specific roles associated with data custodianship includes: Project leader, data manager, GIS manager, IT specialist, Database administrator, Application developer
Lipner Model: combines Bell-LaPadula and Biba to protect confidentiality and integrity

Harrison-Ruzzo-Ullman Model: similar to Graham-Denning and composed of a set of generic rights, and finite set of commands. It is also concerned with situations in which a subject should be restricted from gaining particular privileges. To do so, subjects are prevented from accessing programs or subroutines that can execute a particular command where necessary.

State attacks are known as race condition which are caused by poorly written code

Storage covert channel: communicate via a stored object

Timing covert channel: that modify the timing of events relative to each other

The only way to mitigate covert channels is through the secure design

Middleware is a connectivity software that enables multiple processes running on one or more machines to interact. These services are collections of distributed software that are present between the application running on the OS and the network services, which reside on a network node. Middleware is the foundation of Service Oriented Architectures (SOA).

SOA is a model for distributed computing, wherein applications call other applications over the network. Functionality is distributed over the network, utilizing the ability to find the functionality and ability to connect to it.

Data mining is based on a series of analytical techniques taken from the fields of mathematics, statistics, cybernetics, and genetics. These techniques uncover information from data warehouse.

Grid computing is the sharing of CPU and other resources across a network in such a manner that all machines function as one large computer

Key clustering: When different encryption keys generate same ciphertext from same plaintext

SP-Network: substitution and permutation (transposition)

Avalanche effect: used to design algorithms where a minor change in either key or plaintext will have significant change in cihpertext. This is a feature of strong hashing algorithm

Null cipher: A null cipher option may be used in cases where the use of encryption is not necessary, but yet the fact that no encryption is needed must be configured in order for the system to work. It is used when low security is needed. Today it is regarded as **steganography**

Counter mode is used in high-speed applications such as IPSec and ATM

CAST: key between 40-128 bits, 12-16 rounds. 64 bit blocks.

Secure and Fast Encryption Routine (SAFER) is used as a block cipher in Bluetooth

Blowfish: is extremely fast cipher and can be implemented in as little as 5k memory.

Quantum cryptography: uses physics, based on Werner Heisenberg, to secure data unlike traditional technique, which used mathematics

To protect the session key with a special purpose long-term use key is called **key encrypting key (KEK).** The process of using KEK to protect session keys is called **key wrapping.** Uses symmetric ciphers. Used by SSL, PGP, S/MIME

RIPEMD-160 hashing algorithm

Differential cryptanalysis: called side channel attack, complex attack is executed by measuring the exact execution times and power required by crypto device to perform the encryption/decryption.

Linear Cryptanalysis: known plaintext attack that uses linear approximation to describe behavior of block cipher.

Crime prevention through environmental design (CPTED) provides direction to solve the challenges of crime with organizational (people), mechanical (technology and hardware), and natural design (architecture and circulation flow) methods.

LLC (Logical Link Control) manages connections between two peers. Provides error and flow control and control bit sequencing

Media Access Control (MAC): transmits and receives frames between peers. Logical topologies and hardware addresses are designed at this sublayer.

ICMP Redirect Attacks: attacker can send ICMP redirect to a host telling it to use the attacker's machine as a default route. Scapy is a powerful interactive packet manipulation program.

Network Information Service, NIS and NIS+, are directory services developed by Sun Microsystem, which are mostly used in Unix. They are commonly used for managing user credentials across a group of machines, for instances, a Unix workstation cluster or client/server environment, but they can be used for other types of directories as well.

NIS uses a flat namespace in so-called domains. It is based on RPC and manages all entities on a NIS server. NIS is known for number of vulnerabilities. The fact that NIS does not authenticate individual RPC requests can be used to spoof responses to NIS requests from a client.

NIS+ uses a hierarchical namespace. It is based on RPC. Authentication and authorization is mature here.

A technique called **Packet Loss Concealment (PLC)** is used in VoIP communication to mask the effect of dropped packets. Zero substitution is the simplest PLC technique

Non-Blind Spoofing: takes place when the attacker is on the same subnet as the victim

Bastion host may also include functionality called a "data diode". Flow in a single direction

DMZ is also knows an screened subnet.

Tagging Attack allow a user on a VLAN to get unauthorized access to another VLAN.

Random Frame Stress Attack it consists of a brute force attack that randomly varies several fields of a packet while keeping only the source and destination addresses constant

Relational database model is based on set theory and predicate logic and provides high level of abstraction

Java's Remote Method Invocation (JRMI), Enterprise JavaBean (EJB) are similar to CORBA. ORB in CORBA acts as a middleware.

Citizen Programmers: all desktop and personal computers come equipped with scripting and programming tools, allowing all users to create their own utilities. Application development in such a manner is likely to be chaotic and lack any form of assurance in regard to security. It should be addressed as a matter of policy, enforcement, awareness, and sanctions when needed.

Memory Reuse: When memory is reallocated, the OS should ensure that memory is zeroed out completely or overwritten completely before it can be accessed by a new process.

Between-the-line Attack: occurs when telecommunication lines used by an authorized user are tapped into and data is falsely inserted. Lines should be physically secured.

Hoaxes: warning about new viruses. New viruses that do not exist.

RATs: Remote-access Trojans are programs designed to be installed, usually remotely, after systems are in production and not in development.

Category 1	Less than 1 Mbps	Analog voice and basic interface rate (BRI) in Integrated Services Digital Network (ISDN)
Category 2	<4 Mbps	4 Mbps IBM Token Ring LAN
Category 3	16 Mbps	10 Base-T Ethernet
Category 4	20 Mbps	16 Mbps Token Ring
Category 5	100 Mbps	100 Base-TX and Asynchronous Transfer Mode(ATM)
Category 5e	1,000 Mbps	1000 Base-T Ethernet
Category 6	10,000 Mbps	1000 Base-T Ethernet

ASLR (Address Space Layout Randomization): Memory protection mechanism used by some operating systems. The addresses used by components of a process are randomized so that it is harder for an attacker to exploit specific memory vulnerabilities.

Behavior blocking Allowing suspicious code to execute within the OS and watch its interaction with OS, looking for suspicious activities

Channel Service Unit (CSU): A line bridging device for use with T-carriers

Data Service Unit (DSU): a piece of telecommunications circuit terminating equipment that transforms digital data between telephone company lines and local equipment

CMAC: Cipher MAC based on CBC-MAC

CMM: Block cipher that combines CTR encryption mode and CBC-MAC

EncipherK: Act of transforming data into an unreadable format

Immunizer: Attaches code to the file or application, which would fool a virus into thinking it was already infected.

Meme viruses: These are not actual virus, but types of email messages that are continually forwarded around the Internet.

Plenum cables: Cable is jacketed with a fire retardant plastic cover that does not release toxic chemicals when burned.

Program Status Word (PSW): Condition variable that indicates to the CPU what mode (kernel or user) instructions need to be carried out in

Teredo: Transition mechanism for migrating from IPv4 to IPv6. It allows systems to use IPv6 to communicate if their traffic to transverse an IPv4, but also performs its function behind NAT devices.