CISSP®

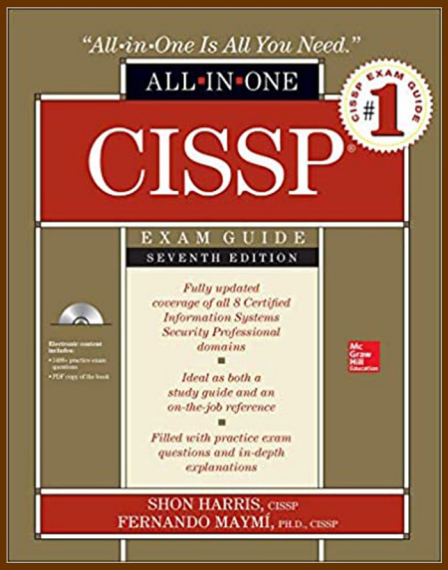
Certified Information Systems Security Professional

ملخص كتاب

CISSP All-in-One Exam Guide

Seventh Edition

م. أحمد خليل عبدالله



من أفضل كتب الإعداد للشهادة العالمية:
محترف أمن نظم المعلومات CISSP

@AKhalil_90

Table of Contents

DISCLAIMER

This document is presented as a free digital document only.

This document represents the effort of the author in summarizing the key points of the “CISSP All-in-One Exam Guide, 7th Edition” by “Shon Harris”, with an addtion of extra remarks and content from outside the book. Hereby, I do not have any copyright on the original “CISSP All-in-One Exam Guide”, and their original copyrights holders owns all the rights on their book and related materials.

In addition to that, reader is STRONGLY ENCOURGED to purchase the full “CISSP All-in-One Exam Guide” book by “Shon Harris” and ready it thoroughly and use this digital document as a handy document to revise and memorize the most important topics and definitions from the book.

Please exuse any typos in this digital document as it is a result of a personal effort, which was mainly generated for a personal prepare for the exam use, and have not gone through a formal reviewing process. Though, the author believes that putting in on the Internet for public use can support people prepaing for their CISSP exam.

CHAPTER 1: Security and Risk Management

Vulnerability	Weakness in the system that allows a threat source to compromise its security.
Threat	Potential damage that is associated with the exploitation of a vulnerability.
Threat Agent	The entity that takes advantage of a vulnerability.
Risk	Likelihood of a threat source exploiting a vulnerability and the corresponding business impact.
Exposure	An instance of being exposed to losses.
Control	Countermeasure that is put in place to mitigate (reduce) the potential risk.

Types of controls:

- Technical
- Administrative
- Physical

Functions on controls:

- Preventative
- Detective
- Corrective
- Deterrent
- Recovery
- Compensating

Corrective vs. Recovery Controls:

- Corrective control: fix components after an incident has occurred.
- Recovery control: bring the environment back to regular operations.

Security Program Development:

- **ISO/IEC 27000 series:** how to develop and maintain ISMS). It uses the Plan – Do – Check – Act approach.

Enterprise Architecture Framework/Development (how to map security to business):

- **Zachman:** generic model. Two-dimensional that uses 6 communication interrogation (What, How, Where, Who, When, Why) intersecting with different perspective (Executives, Business owners, Engineers, etc.).
- **TOGAF:** develop business, data, applications, and technology architectures.
- **DoDAF (military-oriented)**
- **MODAF (military- oriented)**

- **SABSA:** similar to Zachman framework. It is a layered framework with its first layer defining business requirement from a security perspective. It is security enterprise architecture framework.

For enterprise security architecture to be successful:

- **Strategic alignment:** business requirement and the regulatory and legal requirements are being met.
- **Business enablement:** "we can do new stuff".
- **Process enhancement:** "We can do stuff better".
- **Security effectiveness:** deals with metrics, meeting SLA, achieving ROI.

Security Controls Development:

- **COBIT:** it helps organizations to optimize the value of their IT by balancing resource utilization, risk levels, and realization of benefits (contains control objectives used within the private sector).
- **NIST SP 800-53:** outlines controls that agencies need to put into place to comply with FISMA. (controls within U.S. governmental agencies). It uses the following control categories: technical, management, and operational.
- **COSO (Committee of Sponsoring Organizations):** deal with fraudulent activities and reporting.

Sarbanes-Oxley Act (SOX): U.S. federal law that could send executives to jail if it were discovered that their company was submitting fraudulent accounting findings to U.S. government. SOX is based on COSO model.

Process Management Development:

- **ITIL:** de-facto standard for best practices for IT service management.
- **Six Sigma:** process improvement methodology (internal departments are the customers).
- **CMMI (capability maturity model integration):** determines the maturity of an organization's processes.

Security program life-cycle steps:

1. Plan and organize
2. Implement
3. Operate and maintain
4. Monitor and evaluate

- **Computer-assisted crime (the crime can happen without computer):** computer was used as a tool to help carry out crime (attack banking system to steal money, obtaining intellectual property from military system).
- **Computer-targeted crime (couldn't take place without computer):** computer was the victim of the attack (DoS, capturing passwords, installing malware).

- **Computer is incidental:** computer is not the attacker or the attackee. It just happened to be involved when a crime was carried out (child pornography storage)

Safe Harbor Privacy Principles: outlines how U.S.-based companies can comply with the EU privacy principles.

- **Notice:** individuals must be informed that their data is being collected.
- **Choice:** ability for individual to opt out from data collection.
- **Onward Transfer:** transfer data to 3rd parties to only parties that follow data protection principles.
- **Security:** reasonable efforts must be made to protect collected data.
- **Data Integrity:** data must be relevant and reliable for the purpose it was collected for.
- **Access:** individual can access information held about him and correct or delete.
- **Enforcement:** there must be effective means of enforcing these rules.

Legal Systems:

- **Civil (Code) Law:** rule-based law (mostly used in Europe).
- **Common law**: based on previous interpretations of laws (used in US and UK).
  - **Criminal:** addresses behavior harmful to society. Punishment involves loss of freedom or monetary fines.
  - **Civil/tort:** defendant's breach of duty causes injury to the victim, usually physical or financial.
  - **Administrative (regulatory):** laws created by administrative agencies (international trade, manufacturing, environment, immigration). Usually applied to companies and individuals within specific industries.
- **Customary Law:** based on tradition and customs of the region.
- **Religious Law:** based on religious beliefs of the region.
- **Mixed Law:** most often civil and common law.

Trade secret: no expiration date unless information is no longer secret or no longer provide economic benefits (formula of Pepsi, new form of mathematics, source code of a program).

Copyright: protects right of the creator of an original work to control public distribution, reproduction, displays and adaption of that original work:

- It protects the *expression* of the ideal of the resource instead of the resource itself.
- Putting the © symbol is not required.
- Provides protection for life + 50 years.
- **Warez** attack: use copyrighted materials illegally (BitTorrent).

Trademark: protect a word, name, symbol, sound, shape, color, or combination of these (protect brand identity).

Patent: given to individuals or companies to grant them legal ownership of an invention:

- Usually 20 years from date of approval.

- Strongest form of intellectual property protection.
- Non-Practicing Entities (NPE) perform *patent trolls* by getting patents without the intention to manufacture the product, but with an aim to sue others if the patent was used.

Freeware: publicly available software free of charge and can be used, used, modified, etc.
Shareware/Trialware: used by vendors to market their software.
Commercial software: sold for or serves commercial purposes.
Academic software: provided for academic purposes at a reduced cost. It can be open source, freeware, or commercial software.

End User License Agreement (EULA) specifies more granular restrictions that a master agreement.

Personally Identifiable Information (PII): data that can be used to uniquely identify, contact, or locate a single person.

Laws:

- **Federal Privacy Act:** agencies can collect and hold individual's private date if it is relevant to accomplish agency's purpose. Agency cannot disclose this information without written permission from the individual.
- **Gramm-Leach-Bliley Act:** also known as Financial Services Modernization Act. Required financial institutions to develop privacy notices and give customers the option to prohibit sharing their information with nonaffiliated third parties.
- **Health Insurance Portability and Accountability Act (HIPAA**): provide national standards and procedures for the storage, use, and transmission of personal medical information and healthcare data. (Another name: ***Kennedy-Kassebaum Act***).
- **FISMA:** law that requires every federal agency to create, document, and implement agency's wide security program.
- **Department of Veterans Affairs Information Security Protection Act:** narrow scope (only applies to the VA) but it is an example to bolt security after a breach (the stolen laptop).
- **Health Information Technology for Economic and Clinical Health (HITECH) Act:** promote the adaption and meaningful use of health information technology.
- **USA PATRIOT Act:** Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. (reduce restriction of agencies searching telephones, email, medical, etc. deporting immigrants).
- **Personal Information Protection and Electronic Documents Act (PIPEDA):** *Canadian* law that deals with the protection of personal information. This law put trust on Canadian businesses for international trading.
- **Payment Card Industry Data Security Standard (PCI DSS):** credit card companies joint force and came up with a separate entity to look after this standard. It is a private-sector industry initiative and it is not a law.

- **Federal Sentencing Guidelines:** extended to cover computer crimes. Senior management can be held responsible if company did not comply with the laws set out for them.

Privacy vs. Security: privacy is the ability of an individual/group to control who has certain types of information about them. Security is used to enforce these privacy rights.

Pretexting is social engineering attack.

Employee Privacy:

- Monitoring must be work related.
- All employees are subjected to monitoring, not just one or two employees.
- Clearly explained for employees through security policy and constant reminder.

Reasonable Expectation of Privacy document (ERP).

Data Breach can happen to PII, IP, PHI, classified information.

HIPAA does not require notifications for data breaches.

HITECH states that company must report data breach to HHS and to the affected individuals within 60 days. For companies who complies with HITECH recommendations, it is not required to report a data breach.

GLBA requires notification to the federal regulators, law enforcement authorities, and affected customers.

Economic Espionage Act enables FBI to investigate industrial and corporate espionage cases. This act protects corporation's IP.

European Union requires notification to the affected parties to take place within 24 hours of discovery of breach. A complete detailed notification may be distributed no later than 3 days.

Security policy: an overall general statement produced by senior management. The organizational security policy provides scope and direction for all future security activities within the organization.

Organizational security policies also referred as *master* security policies.

Issue-specific policy: also called functional policy. Addresses specific issue that management feels it needs more detailed explanation (e.g. email security policy, access control policy, change control policy).

System-specific policy: presents the management's decision that are specific to the actual computers, networks, and applications (e.g. how sensitive data in database must be protected, who can access it, how to audit it. How laptops should be locked down).

Types of polices:

- **Regulatory:** ensures that the organization is following standards set by specific industry regulations (HIPAA, GLBA, SOX, PCI DSS).
- **Advisory:** advises employees as to which types of behaviors and activities should and should not take place within the organization.
- **Informative:** not an enforceable policy, but rather teaches individuals about specific issues relevant to the company (e.g. how the company interacts with partners, general reporting structure).

Standards: mandatory activities, actions, or roles (e.g. employee must wear ID badge, must encrypt data).

Baselines: a point in time that is used as a comparison for future changes. All further comparison and development are measured against the baseline.

Guidelines: recommended actions and operational guides to users. IT staff, operations staff, and others when a specific standard does not apply. They can also be used as a recommended way to achieve specific standards when those do apply.

Procedures: detailed step-by-step tasks that should be performed to achieve a certain goal (e.g. how to install operating systems). It is considered as the lowest level in the documentation chain.

Risk Management: the process of identifying and assessing risk, reducing it to an acceptable level, and ensuring it remains at that level.

NIST SP 800-39 defines 3 tiers of risk management: Organizational, Business Process, Information Systems. It describes 4 components that comprise the risk management process:

1. **Frame risk:** What are the assumptions? What are the priorities? What management wants?
2. **Assess risk:** assessing the risks.
3. **Respond to risk:** mitigate risk, accept risk, transfer risk, etc.
4. **Monitor risk:** continuously monitor the effectiveness of our controls against the risk.

Information Systems Risk Management (ISRM) policy: is a subset of the risk management policy, which is a subset of the organizational security policies.

Threat modelling: the process of describing feasible adverse effects on our assets caused by threat sources. (vulnerability-threat-attack triad).

Attack tree: expressive way in that show many ways which an attacker can accomplish each objective (the main objective is in the root).

Reduction analysis: reduce the number of conditions we need to mitigate by finding these commonalities. Also, the closer you implement the countermeasure to the root of the attack tree, the more leaf conditions you will defeat with that one control. (goal is to reduce threats and viable attacks).

Risk analysis provides *cost/benefit* comparison.

Illogical processing (threat): incorrect application processing.
Cascading errors: invalid results are passed on to another process.

Delayed loss: secondary in nature and takes place well after a vulnerability is exploited (e.g. company reputation, loss of market share, late penalties, civil suites).

Risk Assessment Methodologies:

NIST 800-30 (IT-based): guide for risk assessment mainly focused on computer systems and IT security issues.

Facilitated Risk Analysis Process (FRAP):

- intended to be used to analyze one system, application, or business process at a time.
- Threats are prioritized based upon their criticality.
- Does not support the idea of calculating exploitation probability numbers or ALE values.
- Criticality of the risks are identified by the team's experience.
- Simple and cost effective.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (Corporate-based):

- Relies on the idea that the people within the organization are best understand what is needed and what kind of risks they are facing.
- Self-directed team approach.
- Used to assess all systems, applications, and business processes within the organization.

AS/NZS 4360 (Corporate-based):

- Can be used to understand financial, capital, human safety, and business decision risks (not only IT).
- More focused on the health of the company from a business point of view, not security.

ISO/IEC 27005:

- International standards for how the risk management should be carried out in the framework of an information security management system (ISMS).

- Deals with IT and softer security issues (documentation, personnel security, training).

Failure Modes and Effect Analysis (FMEA):

- Mainly used in product development and operational environment.
- Identify where something is most likely going to break.

Central Computing and Telecommunication Agency Risk Analysis and Management Method (CRAMM):

- Automated tools sold by Siemens.

Risk Analysis Approaches:

- Quantitative
- Qualitative

Qualitative and quantitative can be used in <u>hybrid</u>: quantitative for tangible assets and qualitative for intangible assets.

SLE = Value of Asset x Exposure Factor (EP)
ALE = SLE x Annualized Rate or Occurrence (ARO)

Uncertainty: the degree to which you lack confidence in an estimate (from 0 to 100 percent).

Delphi Technique: a group decision method used to ensure that member gives an honest opinion of what he or she thinks the result of a threat would be. This is performed anonymously.

Residual Risk: left over risk to deal with.

Controls gap: protection the control cannot provide.

<u>Handling Risk;</u>

- **Risk avoidance:** terminate the activity that is introducing the risk.
- **Risk mitigation (reduction):** risk is reduced to an acceptable level.
- **Risk acceptance:** company will accept the risk when the cost/benefit ratio indicates that the cost of the control outweighs the potential loss value.
- **Risk transfer:** transfer the risk to third party.

You cannot **<u>outsource</u>** risk.

SAS 70: Internal controls audit carried out by a third-party auditing organization.

Risk Management Frameworks:

- **NIST RMF (SP 800-37r1):** agencies are required to implement it.

- **ISO 31000:2009:** not focused on IT.
- **ISACA Risk IT:** very well integrated with COBIT.
- **COSO Enterprise Risk Management—Integrated Framework:** not focused on IT.

NIST RMF (SP 800-37r1):

1. **Categorize Information Systems:** identify and categorize all systems, applications, their interfaces, and how they fit in the business.
2. **Select Security Controls:** in case of introduction of new system, a risk assessment must be done to see if changes or additions to security control is required.
3. **Implement Security Controls:** implement security controls and proper documentation.
4. **Assess Security Controls:** assess effectiveness of security controls and ensure proper documentation in place.
5. **Authorize Information System:** determine if the risk exposure is acceptable by decision maker(s).
6. **Monitor Security Controls:** monitoring of the controls' effectiveness and continuous improvement.

Disaster Recovery Plan:

- Minimize the effects of a disaster or disruption.
- Taking the necessary steps to ensure that resources, personnel, and business processes can resume operation in a timely manner.
- Very IT focused.

Business Continuity Plan:

- Getting critical systems to another environment while repair of the original facilities.
- Perform business in a different mode until regular conditions are back in place.

Business Continuity Management (BCM): the holistic management process that should cover both of DRP and BCP.

BCM Standards:

- **NIST SP 800-34:**
  1. Develop the continuity planning policy statement.
  2. Conduct BIA.
  3. Identify preventive controls: implement preventive controls to reduce the risk.
  4. Create contingency strategies: critical systems can be brought online quickly.
  5. Develop an information system contingency plan.
  6. Ensure plan testing, training, and exercises.
  7. Ensure plan maintenance.
- **ISO/IEC 27031:2011**
- **ISO 22301:2012**
- **Business Continuity Institute's Good Practice Guidelines (GPG)**

- **DRI International Institute's Professional Practices for Business Continuity Planners**

BCP Project:

1. BCP leader is identified (preferably have good social skills).
2. BCP Committee is formed from different departments and must be aware of the work.

BCP Policy: supplies the framework for and governance of designing and building the BCP effort. The policy helps the organization understand the importance of BCP by outlining the BCP's purpose.

Due care: taking the precautions that a reasonable and competent person would take (e.g. not ignoring a warning message) (normally applicable to everyone and could be used to show negligence).

Due diligence: doing everything within one's power to prevent a bad thing from happening (e.g. setting appropriate policies, researching threats, ensures audit happen in the right time) (normally associated with leaders, laws, and regulations).

Business Impact Analysis (BIA):

1. Selects individuals to interview for data gathering.
2. Create data-gathering techniques (surveys, interviews, etc.).
3. Identify the company's critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources (*maximum tolerable downtime MTD* or *maximum period time of disruption MPTD*).
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.

Separation of duties: makes sure that one individual cannot perform a critical task by himself (preventive).

Collusion: at least two people are working together to cause some type of destruction or fraud.

Split knowledge: no one person knows or has all the details to perform a task (preventive).

Dual control: two people must be available and active in their participation to complete the task or mission (preventive).

Rotation of duties: no person should stay in one position for a long time. This is used to uncover fraudulent activities (administrative/detective).

Mandatory vacation: used to detect fraudulent activities by the employees filling the position of the employee on vacation (usually 2 weeks).

Employee termination:

- Disable account and change passwords on all systems must be changed *immediately*.
- Escort terminated employee by manager or a security guard.
- Employee cannot be compelled to perform exit interview or return company property.

Security-awareness training:

- should be tailored to 3 typical audiences: management, staff, and technical employees.
- Should happen during the hiring process, and at least annually after that.

Security governance:

- A framework that allows the security goals of an organization to be set and expressed by senior management, communicated throughout the different levels of the organization.
- Provides a way to verify the performance of the security activities.
- Coherent system of integrated processes that helps ensure consistent oversight, accountability, and compliance.

ISO/IEC 27004:2009 used to assess the effectiveness of an ISMS and its controls (security metrics and measurement).

NIST SP 800-55r1 covers performance measuring for information security.

ISC2 Code of Ethics:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorable, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

ISO/IEC 27799: referred to as health informatics. Its purpose is to provide guidance to health organizations that holds PHI on how to protect such data via implementation of **ISO/IEC 27702**.

ISO/IEC 27001 (based on BS 7799 Part 2): ISMS requirement
ISO/IEC 27002 (17799): Code of practice for information security management
ISO/IEC 27003: Guidelines for ISMS implementation
ISO/IEC 27004: Guidelines for information security management measurement and metrics framework
ISO/IEC 27005: Guidelines for information security risk assessment
ISO/IED 27006: Guidance for bodies providing audit and certification of information security management systems.

Software Protection Association (SPA) and Business Software Affiliation (BSA): formed to protect software vendors and their licenses from piracy.

Proximate causation: for a company to be liable, proximate causation must be proven.

Internet Architecture Board (IAB): Internet is a privilege and should be treated and used with respect (group of researchers, engineers, executives, etc.).

Blue Boxing Attack: hackers use automated tone simulator that telephone switches perceived it as authorization for long distance charges (other attacks followed are *Red Boxes* and *Black Boxes*).

CHAPTER 2: Asset Security

Information life cycle:

1. **Acquisition:** information either created from scratch or copied from somewhere else.
2. **Use:** the most challenges in terms of ensuring confidentiality, integrity, and availability.
3. **Archival**
4. **Disposal**

After the information is acquired and before it can be used:

- Attach system metadata (e.g. author, date/time of creation, permissions, etc.).
- Attach business metadata (e.g. classification, project, owner, etc.).

Backup vs. Archive:

- Backup is a copy of the data set currently in use that is made for the purpose of recovering from the loss of the original data.
- Archive is a copy of the data set that is no longer in use. Usually data is removed from its original location so the storage space is available for data in use.

Information classification: information is classified by *sensitivity*, *criticality*, *or both*.

- **Sensitivity:** losses to an organization is that information was revealed to unauthorized individuals.
- **Criticality:** an indicator of how the loss of the information would impact the business processes for the organization to continue operation.

Classification levels:

- **Commercial business:** Confidential – Private – Sensitive - Public
- **Military:** Top secret – Secret – Confidential - Sensitive but unclassified (SBU) – Unclassified

Not only data need to be classified, sometime applications and whole systems may need to be classified.

Executive management are ultimately responsible for everything that happens in their organization.

Chief Information Officer (CIO) is responsible for the strategic use and management of information systems and technology within the organization. He may report to either the CEO or CFO.

Chief Privacy Officer (CPO) is usually an attorney and is directly involved with setting policies on how data is collected, protected, and given out to third parties.

Chief Security Officer (CSO) is responsible for understanding the risks that the company faces and for mitigating these risks to an acceptable level.

Data owner is usually a member of management who is in charge of a specific business unit. The data owner *decides on the classification of data* under his responsibility.

Data custodian is responsible for maintaining and protecting data. This role is usually filled by the IT or security department.

Date retention policy take addresses: *legal*, *regulatory,* and *operational* requirement.

e-Discovery: discovery of electronically stored information (ESI) is the process of producing for a court or external attorney all ESI to a legal proceeding.

Electronic Discovery Reference Model (EDRM):

1. **Identification** of data required under the order.
2. **Preservation** of this data to ensure it is not accidentally or routinely destroyed.
3. **Collection** of the data from the various stores.
4. **Processing** to ensure the correct format is used.
5. **Review** of the data to ensure it is relevant.
6. **Analysis** of the data for proper context.
7. **Production** of the final data set.
8. **Presentation** of the data to external audience to prove or disprove a claim.

NIST 800-88: Guidelines for media sanitization.

Data remanence elimination:

- **Overwriting:** data with *random or fixed patterns* of 1's and 0's (DoD 5220.22M required the overwriting to happen 7 times) (may not be effective with solid-state devices).
- **Degaussing:** removing the magnetic field patterns on conventional disk drives or tapes. (optical media is not susceptible to degaussing).
- **Encryption:** delete the encryption key only. Good for mobile devices.
- **Physical destruction:** *shred* or *expose to caustic/corrosive chemicals*.

NIST 800-111: Guide to storage encryption technologies for end user devices.

States of data:

- **Data at rest:** resides in secondary storage.
- **Data in motion:** sent over a network.
- **Data in use:** RAM, memory cache, CPU registers.

Clear/erase/sanitize media means removing all its data.

Side-channel attack exploits information that is being leaked by a cryptosystem.

Heartbleed security bug demonstrated how failing to check the boundaries of requests to read from memory could expose information from one process to others running on the same system.

Media management (by library or others):

- **Tracking - audit logging:** who have the data and when.
- **Effectively implementing access controls:** restrict access to each piece of media.
- **Tracking the number and location of backup versions:** to ensure proper disposal, find backup if the stored data is corrupted.
- **Documenting the history changes to the media:** even is the media or its data is no longer needed, retaining a log for that may be useful to demonstrate due diligence.
- **Ensuring environmental conditions do not endanger media.**
- **Ensuring media integrity:** media have lifespan. Availability of the hardware to read the content of the media must be taken into consideration. Cryptographic signature can be used to ensure data integrity.
- **Inventorying the media on a scheduled basis.**
- **Carrying out secure disposal activities.**
- **Internal and external labelling:** date created, retention period, classification level, creator, date to be destroyed, name, version.

Data Leak Prevention (DLP): comprises the actions that organizations take to prevent unauthorized external parties from gaining access to sensitive data.

DLP is concerned with *external parties only*.

DLP steps:

1. Conduct a data inventory.
2. Determine data flows.
3. Data protection strategy.
4. Implementation, testing, and tuning (DLP products implementation).

Data protection strategies:

- **Backup and recovery:** adversaries may be focusing on stealing the data from the backups and not from the primary storage.
- **Data life cycle:** taking care of data protection while transition from one state to another (e.g. secure transfer of backup tape from main site to offsite location).
- **Physical security.**
- **Privacy:** balance the need to monitor data with the need to protect users' privacy (e.g. will be monitor activities while employee uses his personal email?).
- **Organizational change:** mergers and acquisitions of companies need to re-evaluate the overall security posture of the new organization.

DLP products can be compared by:

- **Sensitive data awareness:** analysis of documents and data for sensitive content (e.g. keyword, regular expressions, tags, statistical methods).
- **Policy engine:** some allow extremely granular control but required obscure methods to defining these policies.
- **Interoperability.**
- **Accuracy.**

Misuse case describes threat actors and tasks they want to perform on the system.

DLP resiliency: the ability to deal with challenges, damage, and crisis and bounce back to normal or near-normal condition in short time.

Network DLP (NDLP): applies data protection policies to *data in motion*. Usually implemented as appliance that are deployed at the network perimeter.

Endpoint DLP (EDLP): applied protection policies to *data at rest* and *data in use*. Usually called a DLP agent and it communicates with the DLP policy server to update policies and report events.

Hybrid DLP: deploy both NDLP and EDLP across the enterprise.

Safes: Wall safe - Floor safe – Chests – Depositories – Vaults

Passive relocking: it can detect when someone attempts to temper with it and engages an extra bolt to ensure it cannot be compromised.
Thermal relocking: when a temperature is met, an extra lock is implemented.

CHAPTER 3: Security Engineering

System architecture: describes the major component of the system and how they interact with each other, with the users, and with other systems.

System development: refers to the entire life cycle of a system: planning, analysis, building, testing, deployment, maintenance, and retirement phases.

ISO 42010:2011 Systems and software engineering – Architecture description:

- **Architecture:** a tool to conceptually understand the structure and behavior of a complex entity through different views.
- **Architecture description:** a formal description and representation of a system (collection of documents).
- **Stakeholders:** individual, team, or organization with interests in a system.
- **View:** a representation of a whole system from the perspective of a related set of concerns.
- **Viewpoint:** a specification of the conventions for constructing and using a view (a template from which to develop individual views).

Central Processing Unit (CPU) is the brain of a computer.

Registers are temporary storage location:

- **General registers** are used to hold variables and temporary results as the ALU works through its execution steps.
- **Special registers** hold information such as the *program counter (PC)*, *stack pointer (SP)*, *program status word (PSW)*.

Program counter register contains the memory address of the next instruction to be fetched.

Program status word (PSW) register holds different condition bits. One of the bits indicates whether the CPU should be working in *user mode* (*problem state*) or *privileged mode* (*kernel/supervisor mode*).

Arithmetic Logic Unit (ALU) is where actual execution of the instructions.

Control unit manages and synchronizes the system while different applications' code and operating system instructions are being executed.

The CPU is connected to *address bus* (hardwired connection to the RAM chips or I/O devices). CPU can send fetch request by sending the memory address in the address bus and receive the requested data in the *data bus*.

The address and data busses can be 8, 16, 32 or 64 bits wide.

Multiprocessing (more than one CPU):

- **Symmetric mode:** each processor is handed work as needed by OS (it is like load-balancing environment).
- **Asymmetric mode:** one, or more, processor is dedicated to a specific task or application (good for time-sensitive applications).

Memory:

Random access memory (RAM):

- Temporary storage.
- Holds data and instructions.
- Volatile.

Dynamic RAM (DRAM):

- data being held in the RAM memory cells must be continually and dynamically refreshed.
- Refreshing takes time, so DRAM is slower than SRAM.

Static RAM (SRAM):

- doesn't require refreshing as it doesn't use capacitors.
- Needs more transistors, thus require more space on the RAM chip.
- SRAM more expensive and faster.
- Used in cache.

Synchronous DRAM (SDRAM): timing of the CPU and timing of memory are synchronized. This increases the speed of transmission and executing data.

Extended data out DRAM (EDO DRAM): DRAM can only access one block of data at a time, while EDO DRAM can capture the next block of data while the first block is being sent to the CPU for processing (look ahead).

Burst EDO DRAM (BEDO DRAM): works like EDO DRAM, but it can send more that at once (burst). It reads and sends up to 4 memory addresses.

Double data rate SDRAM (DDR SDRAM): carries out read operations on the rising and falling cycles of a clock pulse.

Tharshing: when a computer spends more time moving data from one small portion of memory to another than actually processing the data.

Hardware segmentation: memory is separated physically instead of just logically. This adds another layer of protection to ensure lower privileged process cannot interfere with higher level process' memory addresses.

Read-only memory (ROM):

- Non-volatile
- Data cannot be altered.
- Software that is stored within ROM is called *firmware*.

Programmable ROM (PROM):

- Data can be modified after it has been manufactured.
- Can be programmed *only one time* because the voltage that is used to write bits burns out fuses that connects memory cells.

Erasable programmable ROM (EPROM):

- Data can be erased, modified, and upgraded.
- To erase the data in the memory chip, *UV light device* is used against the *quartz* windows. This erase ***all*** data.
- Electronically erasable programmable ROM (EEPROM) that can be modified by *onboard programming circuitry and signals* and ***can erase 1 byte at a time*** (*slow*).

Flash memory:

- Solid-state technology (no moving parts).
- Erasing function takes place in ***blocks*** or ***on the entire chip***.

Cache memory:

- Memory used for high-speed writing and reading activities.
- L1 and L2 caches are usually built into the *processors* and the *device controllers*.

Absolute addresses: physical memory addresses that the CPU uses.

Logical addresses: the indexed memory addresses that software uses.

Relative addresses: based on a known address with and offset value applied (base + offset).

Memory stack: each process has its own stack in the memory. Stack can be read from and written **to in a last in, first out (LIFO)** fashion.

Buffer is an allocated segment of memory (e.g. memory stack). It allows communication between the requested application and the procedure/subroutine.

Return pointer (RP) is the first thing goes into stack (*down*), and followed by the parameters.

Bounds-checking is to ensure that inputted data is of an acceptable length.

Buffer overflow attack that work on an Intel chip will not necessary work on an AMD chip.

Address space layout randomization (ASLR) where OS is changing the memory addresses used by specific process continuously, so an attacker don't know where to send his attack within memory.

Data execution prevention (DEP) is implemented via hardware (CPU) or software (OS) to allow marking certain memory locations as "off limits" with the goal of reducing the "playing field" for hackers and malware.

Memory leaks:

- some applications are not indicating to the system that certain memory is no longer in use (OS can starve for free memory space).
- Countermeasures:
  - developing better code that releases memory properly.
  - Garbage collection.

Process:

- a set of instructions that is actually running. Program is not considered a process until it is loaded into memory and activated by the OS.
- Collection of instructions + assigned resources = process

Multiprogramming means that more than one program (or process) can be loaded into memory at the same time.

Mutlitasking means that more than one application can be in memory at the same time **and** OS can deal with requests from these different applications *simultaneously*.

Types of multitasking:

- **Cooperative multitasking:** processes voluntarily release resources they were using.
- **Preemptive multitasking:** OS controls how long a process can use a resource.

Unix and Linux allow their processes to create new children processes, which is called ***spawning***.

Process states:

- **Running:** CPU is executing its instructions and data.
- **Ready:** waiting to send instructions to the CPU.
- **Blocked:** waiting for input data such as keystrokes from a user.

Process table maintained by OS. Include a record for each process with the following information: state, memory allocation, stack pointer, program counter, status of open files in use.

System has *hardware* and *software* interrupts.

OS can assign priorities to processes to help in decide whether to respond to a process interrupt.

Categories of interrupts:

- **Maskable** interrupt assigned to an event that is not important.
- **Non-maskable** interrupt can never be overridden by an application.

Watchdog timer is an example of a critical process that must always do its thing. This process will reset the system with a *warm boot* if the OS hangs and cannot recover itself.

Thread:

- made up of individual instruction set and the data must be worked on by the CPU.
- When a process needs to send something to the CPU for processing, it generates a *threat*.
- Each thread shares the same resources of the process that created it.

An **application** that carry out several tasks at one time is called *multi-threaded*.

OS is responsible for controlling ***deadlocks*** between processes attempting to use the same resources (e.g. *process A commits resource 1 and needs to use resource 2 to complete its task, but process B has committed resource 2 and needs resource 1 to finish its job*).

OS implements **process isolation** to protect processes from each other (It is required in *preemptive multitasking*):

- **Encapsulation of objects:** when a process is encapsulated, no other objects understands or interacts with its internal programming code. It provides *data hiding*.
- **Time multiplexing of shared resources:** a technology that allows processes to use the same resource.
- **Naming distinctions:** different processes have their own name or identification value (e.g. *process identification, PID*).
- **Virtual address memory mapping:** each process has their own memory space.

Memory manager is a portion of the OS that keeps track of how hierarchy of memories is used (CPU registers, Cache, Main memory, Swap space in secondary memory).

Memory manager responsibilities:

- **Relocation:**
  - Swap contents from RAM to the hard drive as needed.
  - Provide pointers for applications if their instructions and memory segment have been moved to a different location in the main memory.
- **Protection:**
  - Limit processes to interact only with memory segment assigned to them.
  - Provide access control to memory segments.
- **Sharing:**
  - Ensure confidentiality and integrity when processes need to use the same shared memory segments.

  - Allow many users with different levels of access to interact with the same application running in one memory segment.
- **Logical organization:**
  - Segment all memory types and provide addressing scheme for each at an abstraction level.
  - Allow for sharing of specific software modules (e.g. DLLs).
- **Physical organization:**
  - Segment the physical memory space for application and OS processes.

CPU uses *base register* and *limit register* to ensure the process is accessing its segment of memory only.

Virtual memory:

- When RAM and secondary storage are combined, the result is a virtual memory.
- **Swap space** is the reserved hard drive space used to extend RAM capabilities (Windows use *pagefile.sys*).
- data sent back and forth between RAM and hard drive in units, called ***pages***. The process called ***virtual memory paging***.
- When the page is sent back from hard disk to main memory, this process called **page fault**.
- **Security issue:** data is kept in the swap space after the process is terminated or the system is shut down. A routine should be there to ensure data deletion in such cases.

I/O devices:

- **Block devices** work with data in *fixed-size* blocks (disk drive).
- **Character devices** works with stream of characters (printer, NIC, mouse).

OS uses a *device driver software* to communicate with a *device controller*.

OS has a table called **interrupt vector** or all I/O devices connected to it.

Types of I/O devices:

- **Programmable I/O:** pools the device to see if it is ready to accept more data.
- **Interrupt-driven I/O:** CPU sends a character over to the printer and then goes and work on another process's request. Printer sends interrupt to CPU when it is ready to accept more data.
- **I/O using DMA:** transferring data between I/O devices and the systems memory without using the CPU. This speed up the data transfer rate significantly (referred to as *unmapped I/O*).
- **Pre-mapped I/O:** CPU sends the *physical address* of the requesting process to the I/O device and the I/O device is *trusted* enough to interact with the content of memory directly.
- **Fully mapped I/O:** OS *does not trust* the I/O device. The device works purely with *logical addresses* and works on behalf of (under the security context) the requesting process.

Pre-mapped and fully mapped I/O *does not pertain to performance* and provide two approaches that can directly affect *security*.

Instruction set is a language an OS must be able to speak to properly communicate with CPU (*x86 is a family of instruction sets*).

Microarchitecture contains the things that made up the physical CPU (registers, logic gates, ALU, cache, etc.).

Ring-based architecture: OS kernel (ring 0), OS (ring 1), OS utilities and file system drives (ring 2), other applications (ring 3).

CPU operation modes: OS assigns a process a *status* level (*stored as PSW*): *user* and *kernal* modes.

CPU vendor determines the number of available rings, and the *OS vendor* determines how it will use these rings.

Process domain: a collection of resources assigned to the process when it is loaded into memory (run time).

Monolithic architecture: all of the OS processes work in kernel mode (e.g. MS-DOS):

- Complexity
- Portability issues
- Extensibility issues
- Security issues

Layered Operating system architecture: separates system functionality into hierarchical layers (e.g. THE, VAX/VMS, Multics, Unix):

- Full OS works in kernel mode (ring 0).
- Provides *data hiding*: instructions and data at various layers do not have direct access to the instructions and data at any other layers.
- Provides more modularity.
- Provide more portability from one hardware to another (Hardware Abstraction Layer HAL).
- Downfalls: performance (many layers), complexity (many layers), and security (all OS in kernel mode).

Microkernel architecture: smaller subset of critical kernel processes, which focus mainly on memory management and IPC, are running in kernel mode (ring 0):

- More secure
- Complexity is reduced

- Portability is increased
- Performance issues due to *mode transitions*.

Mode transition takes place every time a CPU has to move between executing instructions for a processes that work in kernel mode versus user mode.

Hybrid microkernel architecture:

- All of the other OS services work in a client/server model (e.g. Windows).
- The OS services act as *servers*, and application processes act as *clients*.
- All OS processes run in kernel mode.
- Core processes run within a microkernal, and others run in a client/server model.

Thunking: when a 32-bits application wants to run on a 64-bits OS, OS creates a virtual environment to simulates a 32-bits OS and once a request is received from the application, a translation happen from 32-bits to 64-bits.

Virtual machine is an instance of an OS. It called *guest* that runs on a *host* environment.

Hypervisor within the host environment is responsible for managing system resources.

Trusted Computing Base (TCB):

- collection of all the hardware, software, and firmware components within a system that provides some type of security and enforces the system's security policy.
- The term originate from the Orange Book and contains the protection mechanisms within the system.

TCB is not the kernel only. TCB can include trusted commands, programs, configuration files, etc.

When installing Unix system and enabling installing TCB configuration:

- **Trusted path:** communication channel between the user, or program, and the TCB.
- **Trusted shell:** someone works on the shell cannot bust out of it and other processes cannot bust into it.
- **Integrity-checking capabilities**

Security perimeter: an imaginary boundary that divides the trusted from the untrusted (e.g. strict APIs must be implemented).

Reference monitor: an abstract machine that mediates all access subjects have to objects, both to ensure that the subjects have the necessary access rights and to protect the objects from unauthorized access and destructive modifications (an access control concept).

Security kernel:

- made up of hardware, software, and firmware components that fall within the TCB, and implements and enforce the reference monitor concept.
- It is the core of TCB.
- Has 3 main requirements:
  - Provide isolation to processes carrying out the reference monitor concept, and processes must be tamperproof.
  - Must be invoked for every access attempt.
  - Must be small enough to be tested and verified.

Multilevel (multistate) security policies: policies that prevent information from flowing from a high security level to a lower security level.

Security Models:

Bell-LaPadula:

- Enforces *confidentiality* aspects of access control.
- Multilevel security system
- **Simple security rule:** subject cannot *read* data at higher security level.
- ***-property rule:** subject cannot *write* information to a lower security level.
- **Strong star property rule:** subject with read/write capabilities can only perform both of these functions at the same security level.

Biba:

- Enforces the *integrity* of data within a system.
- ***-integrity axiom:** a subject cannot *write* data to an object at a higher integrity level (no write up).
- **Simple integrity axiom:** a subject cannot *read* data from a lower integrity level (no read down).
- **Invocation property:** a subject cannot request service (*invoke*) at a higher integrity (ensure that a dirty subject cannot invoke a clean tool to contaminate a clean object).

Clark-Wilson:

- **Users:** active agents
- **Transformation procedures (TPs):** programmed abstract operations (e.g. read, write, modify).
- **Constrained data items (CDIs):** can be manipulated by TPs.
- **Unconstrained data items (UDIs):** can be manipulated by users using primitive read and write operations.
- **Integrity verification procedures (IVPs):** check the consistency of CDIs with external reality.

- **Well-formed transaction** is a series of operations that transform a data item from one consistent state to another.
- **Separation of duties** is implemented by adding a type of procedure (the IVPs) that audits the work done by the TPs and validates the integrity of the data.
- User uses TPs to operate on CDIs.
- Access triple: subject (user), program (TP), and object (CDI).

Noninterference:

- Implemented to ensure any actions that take place at a higher security level do not affect, or interfere with, actions that take place at a lower level.
- Mainly focused on addressing *covert channels*.

Covert channel: *storage* and *timing* channels.

Brewer and Nash (Chinese wall):

- A subject can write to an object if, and only if, the subject cannot read another object that is in a different dataset.
- Focus to protect against conflicts of interest by users' access attempts.

Graham-Denning:

- Defines set of basic rights in terms of commands that a specific subject can execute on an object.
- 8 primitive protection rights:
    - How to securely create an object
    - How to securely create a subject
    - How to securely delete an object
    - How to securely delete a subject
    - How to securely provide the read access right
    - How to securely provide the grant access right
    - How to securely provide the delete access right
    - How to securely provide transfer access right

Harrison-Ruzzo-Ullman (HRU):

- Deals with access rights of subjects and the integrity of those rights.
- Shows how a finite set of procedures can be available to edit the access rights of a subject.

Common Criteria (CC) codified as **ISO/IEC 15408**.

Once a product is evaluated, it receives an Evaluation Assurance Level (EAL).

ITSEC uses E-F rating.
Orange Book (TCSEC) uses A-D ratings. Rate A is the best:

- A: Verified protection
- B: Mandatory protection
- C: Discretionary protection
- D: Minimal protection

(Red Book) address network components and products.
(Orange Book) addresses operating systems for governmental and military use.

EAL has 7 levels. EAL 7 is the strongest (CC).

The Common Criteria uses **protection profiles** in its evaluation process, which contains the following:

- **Security problem description:** describes the threats
- **Security objectives**: list the functionalities that the complied product must provide.
- **Security requirement:** detailed requirement that are enough for system developers and for evaluation by independent laboratories.

Certification: the comprehensive technical evaluation of the security components and their compliance for accreditation.

Accreditation: the formal acceptance of the adequacy of a system's overall security and functionality by management.

Certification and Accreditation is a core component of FISMA compliance. Usually moving to continuous monitoring instead of a formal process of C&A.

Distributed system is a system in which multiple computing nodes, interconnected by a network, exchange information for the accomplishment of collective tasks.

Parallel computing is the simultaneous use of multiple computers to solve a specific task by dividing it among the available computers.

Bit-level parallelism: when the CPU perform instruction on a value stored in a register, each bit is processed separately through set of parallel gates.

Instruction-level parallelism: allows two or more program instructions to be executed simultaneously (require two or more processors).

Task-level parallelism: a program can divide tasks into threads and run them in parallel.

Data parallelism: distribution of data among different nodes that then process it in parallel (related to task parallelism).

Databases:

Aggregation the act of combining information from separate sources to form new information, which the subject does not have the necessary access rights to it.

Inference is the ability to derive information not explicitly available (the intended result of aggregation).

Countermeasure to database inference attack:

- **Cell suppression:** hide specific cells that contain information that could be used in inference attack.
- **Partitioning:** dividing the database into parts (makes it harder for attacker to connect pieces of data).
- **Noise and perturbation:** inserting bogus information in the hopes of misdirecting an attacker.

Content-dependent access control is based on the sensitivity of the data.

Context-dependent access control means that the software understands what actions should be allowed based upon the state and sequence of the request.

In event of an error in a website, it should be designed to behave in predictable manner (**failing securely**) (e.g. display friendly error message, without revealing internal system details).

Cyber-physical system is a system in which computers and physical devices collaborate via the exchange of inputs and outputs to accomplish a task.

Embedded systems are usually built around *microcontrollers*.

IoT: each node is connected to the internet and is uniquely addressable.

Industrial control systems (ICS): efficiency and safety is important. **NIST 800-82** tackle this.

Programmable logic controllers (PLC):

- Computer designed to control electromechanical processes such as assembly lines, etc.
- Can be re-programmed easily.
- Usually connects to devices over a standard interface RS-232.

Distributed control system (DCS):

- a network of control devices within fairly close proximity that are part of one or more industrial processes.
- PLCs are controlling the physical devices.
- A supervisory computer is controlling the PLCs.
- Those days, people think about physical security only.

Supervisory control acquisition and data acquisition (SCADA):

- Controls large-scale physical processes involving nodes separated by large distances.
- 3 kind of devices:
  - **Endpoint** (remote terminal unit, RTU, connects directly to the sensor/actuator).
  - **Backends** (data acquisition servers, DASs, receive all data from endpoints).
  - **User stations** (human-machine interface, HMI, where user controls the system).

Maintenance hook:

- A type of a *back-door*. Usually, enables developer to execute commands by using a specific sequence of keystrokes.
- **Countermeasures:**
  - Host-based IDS to watch for any attacker using back-doors.
  - Use file system encryption to protect sensitive information.
  - Implement auditing to detect any type of back door use.

Time-of-check/Time-of-use (TOC/TOU) attacks:

- Takes advantage of the dependency on the timing of events that take place in a multitasking OS.
- **Example:** process 1 validates the authorization of a user to open a noncritical text file and process 2 carries the open command. If attacker can get between these two actions, attacker may be able to change the text file to password file.
- Attacker tries to jump in between two tasks and modifies something to control the result.
- Referred to as *asynchronous attack* (asynchronous because the the timing of each step may vary).
- **Countermeasures:**
  - Apply software locks on the items it will use when it is carrying out its *checking* tasks.

Race condition attack:

- is when two different processes need to carry out their task on one resource.
- **Example:** process 1 needs to carry out its work before process 2 accesses the same resource. If process 2 goes before process 1, the outcome could be very different.
- Attacker tries to make processes execute out of sequence to control the result.
- **Countermeasures:**
  - To protect against race condition attacks, it is best to not split up critical tasks that can have their sequence altered (use atomic operations).

Caesar cipher: shifts each alphabet by 3 positions (*monoalphabetic* cipher).

Vigenere cipher (*polyalphabetic* cipher).

ROT13 shifts each alphabet by 13 positions (was used in online forum only).

Cryptosystem: software – protocols – algorithms – keys.

Kerckhoff's principle: the only secrecy involved with the cryptosystem should be they key. The algorithms should be publicly known.

Another name of cryptography strength is *work factor*.

One-time pad (Vernam cipher):

- The pad must be used one time only.
- The pad must be as long as the message.
- The past must be securely distributed and protected at its destination.
- The pas must be made up of truly random values.

Running key cipher could use a key that does not require an electronic algorithm but uses components in physical world around you (e.g. algorithm could be set of books agreed upon by sender and receiver).

Concealment cipher (null cipher) is message within a message (e.g. every third word). It is a type of steganography method.

Steganography is a method of hiding data in another media type so the very existence of the data is concealed (*type of security through obscurity*):

- **Carrier:** a signal of a file that will hide information.
- **Stego-medium:** the medium in which information is hidden.
- **Payload:** the information that is to be concealed and transmitted.

Types of ciphers:

- **Substitution cipher** replaces bits, characters or blocks.
- **Transposition cipher** moves the original values around.

Simple substitution and transposition ciphers are vulnerable to **frequency analysis**.

Key derivation functions (KDFs) are used to generate keys that are made up of random values.

If more than two keys are created from a **master key**, they are called **subkeys**.

White has uses *cryptanalysis* to test the *strength of the algorithm*.

Number of keys in symmetric encryption for N users: **N(N-1)/2**

Secure message format is when the message is encrypted using the receiver's public key.

Open message format is when the message is encrypted using the sender's private key.

Confusion is commonly carried by **substitution**.

Diffusion is carried out by **transposition.**

Avalanche effect: if the input to an algorithm is slightly modified, then the output of the algorithm is changed significantly.

Stream ciphers use **keystream generators**, which produce a stream of bits that is XORed with the plaintext bits.

Characteristics of strong stream cipher:

- Easy to implement in hardware
- Long periods on no repeating patterns within keystream values.
- A keystream not linearly related to the key.
- Statistically unbiased keystream (as many zeros as ones).

Initialization vectors (IV) are random values that are used with algorithms to ensure patterns are not created during the encryption process.

Steam cipher requires **more processing power** than block ciphers, and better suited implemented as the **hardware** level.

Stream ciphers better implemented in *video*, *VoIP*, *multimedia*.

Cryptographic transformation techniques:

- **Compression:** reduce redundancy before plaintext is encrypted.
- **Expansion:** expanding the plaintext by duplicating values (e.g. to match the key size).
- **Padding:** adding material to plaintext data before encryption.
- **Key mixing:** using portion of the key (subkey) to limit its exposure. Key schedules are used to generate subkeys from master key.

Digital envelope: the use of the hybrid encryption method (symmetric and asymmetric). Encrypt message with symmetric key, and encrypt the encryption key with receiver's public key.

Session key is a single-use symmetric key that is used to encrypt messages between two users during a communication session.

Data Encryption Standard (DES):

- DEA is the algorithm name (formerly *Lucifer*).
- 64-bit block size
- 64-bit key size (56-bit key is used + 8 parity bit)
- 16 rounds of transposition and substitution functions
- It is currently broken

DES modes:

- **Electronic Code Book (ECB):**
  - Fastest and easiest
  - Used for small amount of data
  - Does not use chaining, so not good for large data (e.g. patterns will show)
  - Operations can be run in parallel
  - Cannot carry out preprocessing functions before receiving plaintext
- **Cipher Block Chaining (CBC):**
  - Ciphertext block is dependent upon all blocks before it
  - IV should be used for first block encryption to avoid patterns
- **Cipher Feedback (CFB):**
  - Great to use for sending large chunks of data at a time
  - It is a combination of block cipher and stream cipher
  - Can be used to encrypt any size blocks
  - Error propagates to all future encryptions
- **Output Feedback (OFB):**
  - Good to encrypt small amount of data when you don't want error propagation (e.g. digitized video, digitized voice signal)
  - Preprocessing is possible
- **Counter (CTR):**
  - Uses an IV counter that increments for each plaintext block
  - No chaining, so the encryption of the individual block can happen in parallel.

Synchronous cyptosystem uses keystream to encrypt plaintext one bit at a time (keystream values in sync with plaintext values) (**stream cipher**).

Asynchronous cyptosystem uses previously generated output to encrypt current plaintext values (**block cipher using chaining**).

Double-DES:

- 112-bit key length
- There is specific attack against it that reduces its work factor to about the same as DES

Triple-DES (3DES or TDES):

- 48 rounds
- performance issue (3 times DES)

- Modes:
  - **DES-EEE3:** 3 keys
  - **DES-EDE3:** 3 keys
  - **DES-EEE2:** 2 keys
  - **DES-EDE2:** 2 keys

Advanced Encryption Standards (AES):

- Rijndael is the algorithm name
- Key sizes:
  - 128 (10 rounds)
  - 192 (12 rounds)
  - 256 (14 rounds)
- low memory requirement
- defend against timing attacks

International Data Encryption Algorithm (IDEA):

- 128-bit key size
- 64-bit blocks of data
- the 64-bit block is divided into 16 smaller blocks, and each has 8 rounds
- IDEA is faster than DES (in software)
- Harder to break than DES due to its longer key size
- Used in **PGP**
- No successful practical attacks against it
- It is **patented**

Blowfish:

- 23-bit up to 448-bit key size
- 64-bit block size
- 16 rounds
- **unpatented** by its creator

RC4:

- it is a stream cipher
- variable key size
- Used in **SSL** protocol
- Was *improperly* implemented in802.11 WEP protocol standard
- Fast, simple and efficient
- Vulnerable to modification attacks

RC5:

- Block cipher
- Block sizes: 32-bit, 64-bit,128-bit

- Key size goes up to 2,048 bits
- Variable rounds up to 255 rounds

RC6:

- Block cipher
- Same attributes as RC5

Asymmetric cryptography:

- **Security services:** confidentiality, authentication, and nonrepudiation.
- **Scalability:** every user will have only pair of keys, regardless the number of users.
- **Secure key distribution:** public key can be sent to users.

Diffie-Hellman:

- Enables two systems to generate symmetric key securely without requiring prior relationship.
- Based on difficulty of calculating discrete logarithms in a finite field.
- Vulnerable to *man-in-the –middle* attack, because no authentication occurs before public keys exchanged.
  - **Countermeasure:** to have authentication take place before accepting someone's public key (e.g. certificate usage).
- key *agreement* algorithm and not key *distribution* algorithm.

Menezes-Qu-Vanstone (MQV) is an authentication key agreement function.

RSA:

- Based on the difficulty of factoring large numbers into their original prime numbers.

One-way function is a mathematical function that is easier to computer in one direction than in the opposite direction.

Public key encryption/decryption is a **one-way function** with **trapdoor**.

El Gamal:

- Used for encryption, digital signatures, and key exchange
- Based on difficulty of calculating discrete logarithms in a finite field
- *Performance* issue

Elliptic curve cryptosystem (ECC):

- Provide similar functionality to RSA
- Computes discrete logarithms of elliptic curve
- ECC is more efficient than RSA and any other asymmetric algorithm (same security level can be achieved by smaller key size)

Knapsack:

- Based on "knapsack problem", a mathematical dilemma that poses the following question: if you have several different items, each having its own weight, is it possible to add these items to a knapsack so the knapsack has a specific weight?
- It is *insecure* and not currently used.

Zero knowledge proof:

- Example: If a user encrypts something with his private key, he proves that he has his private key, without showing others the private key itself.

Message authentication code (MAC): Provides *data-origin authentication*, or *system authentication*:

- **Hash MAC (HMAC):** append secret key with message when produce the hash.
- **CBC-MAC:**
  - message is encrypted with symmetric block cipher in CBC mode, and the output of the final block of ciphertext us used as the MAC.
- **Cipher-based MAC (CMAC):** same as CBC-MAC but *more secure* mathematically.

CCM block mode combines CTR mode and CBC-MAC.

Cyclic redundancy check (CRC) is used to identify data modifications (e.g. corruption) and used mostly in lower layers of network stack.

Hash function characteristics:

- Hash should be computed for the entire message
- Hash should be a one-way function
- Given a message and its hash value, computing another message with the same hash value should be impossible
- Should be resistant to birthday attack

MD4:

- Produces a 128-bit message digest value
- No longer secure

MD5:

- Produces a 128-bit message digest value
- Subject to collision attacks.

Secure Hash Algorithm (SHA):

- Produces a 160-bit message digest value
- Used with the Digital Signature Standard (DSS)
- Vulnerable to collisions and no longer secure (SHA-1)
- SHA-2 and SHA-3 are secure

- Family: SHA-256, SHA-384, SHA-512

HAVAL: creates a variable-length message digest.

The output of the hashing algorithm is n. To find two messages that hash to the same value would require only 2^(n/2) message.

Digital signature standard (DSS):

- Uses Digital Signature Algorithm (DSA)
- Used only for digital signatures
- DSA is slower than RSA in signature verification

PKI: uses public key cryptography and X.509 standard.

Certificate authority (CA) maintains and issues the digital certificate.

Registration authority (RA) collects user/organization information and acts as a broker between end-user and CA.

Cross certification is the process undertaken by CAs to establish a trust relationship in which they rely upon each other's digital certificates and public keys as if they had issues them themselves.

Certificate revocation list (CRL) is where revoked certificate information is stored.

Online certificate status protocol (OCSP):

- Used more rather than CRL approach
- Work automatically in the background
- It checks CRL that is maintained by CA
- Carries out real-time validation of a certificate and reports back to the user (e.g. valid, invalid, unknown).

By default, web browsers do not check a CRL to ensure that a certificate is not revoked.

Certificate is the mechanism used to associate a public key with a collection of components (e.g. serial number, version number, identify information, algorithm information, lifetime date, signature of the issuing authority).

Multiparty key recover more than one person/entity are needed for this process (dual control).

Key escrow is a process or entity that can recover lost or corrupted cryptographic keys.

Trusted platform module (TPM) is a microchip installed on the motherboard and dedicated for carrying out security functions that involves the storage and processing of secret keys, hashes, and digital certificates:

- **Binds** the hard disk drive: the content of the disk is encrypted and the decryption key is stored in the TPM chip.
- **Seals** system's configuration: TPM stores the hash of the configuration files and validates their integrity.

TPM internal memory is divided into 2 different segments:

- **Persistent (static):**
  - **Endorsement key (EK):** a public-private key pair that is installed in the TPM at the time of manufacturing and cannot be modified. Private key is always inside TPM. Public key is used to verify authenticity of the TPM itself.
  - **Storage Root Key (SRK):** master wrapping key used to secure the keys stored in the TPM.
- **Versatile (dynamic):**
  - **Attestation Identity Key (AIK):** used for the attestation of the TPM chip itself to service providers (AIK ensures the integrity of EK).
  - **Platform Configuration Registers:** used to store cryptographic hashes of data used for "sealing" functionality.
  - **Storage Keys:** used to encrypt the storage media of the computer system.

Ciphertext-only attack: the attacker has the ciphertext of several messages.

Known-plaintext attack: the attacker has the plaintext and corresponding ciphertext of one or more messages.

Chosen-plaintext attack: the attacker has the plaintext and the ciphertext, but can choose the plaintext that gets encrypted to see the corresponding ciphertext.

Chosen-ciphertext attack: the attacker can choose the ciphertext to be decrypted and has access to the resulting decrypted plaintext.

Differential cryptanalysis: the attacker takes two messages of plaintext and follows the changes that take place to the blocks as they go through S-boxes. The difference identified in the resulting ciphertext values are used to find the key.

Linear cryptanalysis: the attacker carries out a known-plaintext attack on several different messages encrypted with the same key.

Algebraic attack: analyze the vulnerabilities in the mathematics used within the algorithm.

Analytic attack: identify algorithms structural weaknesses or flaw.

Statistical attack: identify statistical weaknesses in algorithms design (e.g. number of zeros compared to number of ones, biased PRNG).

Meet-in-the-Middle attack: mathematical analysis used to try and break a math problem from both ends (encrypting from one end and decrypt from the other end).

Facility threats:

- Natural environmental threats (e.g. floods, earthquakes)
- Supply system threats (e.g. power, communication)
- Manmade threats (e.g. unauthorized access, employee error)
- Politically motivated threats (e.g. strike, riot, terrorist attack)

Crime Prevention Through Environmental Design (CPTED):

- Natural access control (landscaping, fences, doors)
- Natural surveillance (straight line of sights, raised entrances).
- Natural territorial reinforcement (employees feel a sense of ownership to the space).

Target hardening focuses on denying access through physical and artificial barriers by applying more granular protection mechanisms. (alarms, locks, fences). Whereas, CPTED mainly deals with the construction, internal/external design and landscaping.

Compliance requirement:

- Occupational Safety and Health Administration (OSHA)
- Environmental Protection Agency (EPA)

Frame construction material has a **30 minutes** fire-rating.

Heavy timber construction material has **1 hour** fire-rating.

Fail-safe (doors default to being unlocked)

Fail-secure (doors default to being locked)

Fire code requires 2 doors for data center: 1 door is only used and the other is for emergency use (locked and exit only with panic bar).

Positive pressurization let the air goes out when the door is open (smoke goes out in case of fire).

Window types:

- **Standard:** no extra protection
- **Tempered:** glass is heated and then cooled to increase its integrity
- **Acrylic:** plastic instead of glass. Polycarbonate acrylic is stronger than regular ones
- **Wired:** a mesh of wire is embedded between two sheets of glass (prevent shattering)
- **Laminated:** plastic layer between two outer glass layers.
- **Solar window film:** provide extra security by being tinted, also this film increases its strength
- **Security film:** transparent film is applied to the glass to increase its strength

Leak detectors should be under raiser floors and on the dropped ceilings.

High humidity: corrosion can take place.
Low humidity: static electricity can be introduced.

Online UPS system have the normal primary power passing though them and able to *quickly* detect if power failure takes place and picks up the load faster.

Standby UPS devices stays inactive until a power line fail. The system has sensors that detect power failure, and the load is switched to the battery pack with small delay.

Power excess:

- **Spike:** momentary high voltage
- **Surge:** prolonged high voltage

Power loss:

- **Fault:** momentary power outage
- **Blackout:** prolonged, completed loss of electric power

Power degradation:

- **Sag/dip:** momentary low-voltage condition, from one cycle to few seconds
- **Brownout:** prolonged power supply that is below normal voltage
- **In-rush current:** initial surge of current required to start a load

Possible types of interference on power (noise):

- Electromagnetic interference (EMI)
- Radio interference (RFI)

Positive drain means that current flow out instead of in.

Hygrometer is used to monitor humidity.

Fire needs fuel, oxygen, and high temperature.

Fire Class	Type of Fire	Elements of Fire	Suppression Method
A	Common combustibles	Wood products, paper, and laminates	Water, foam
B	Liquid	Petroleum products and coolants	Gas, CO_2, foam, dry powders
C	Electrical	Electrical equipment and wires	Gas, CO_2, dry powders
D	Combustible metals	Magnesium, sodium, potassium	Dry powder

Table 3-5 Four Types of Fires and Their Suppression Methods

Fire detectors:

- **Smoke activated:** *photoelectric devices (optical detectors detects variation in light intensity)*.
- **Head activated:** *fixed* temperature or *rate-of-rise*.

The most effective replacement of Halon is FM200 (doesn't damage the ozone).

Replacement of Halon: FM200, NAS-S-III, CEA-410, FE-13, Water, Intergen, Argon, Argonite.

Fire extinguishers should be place **50 feet** away from electrical equipment (viewable and reachable).

Plenum Area:

- wiring and cables are strung through plenum area (dropped ceilings, spaces in walls, under raise flooring)
- It should have fire detectors
- Only plenum-rated cabling should be used (doesn't let off hazardous gasses if it burns)

Water sprinklers:

- Sensors should be used to shut down the electric power before water sprinklers activate.
- **Wet pipe:** pipes always contain water. **Disadvantage** is that water may *freeze* in colder climate or *leak*.
- **Dry pipe:** water is contained in a *holding tank*.
- **Preaction:** similar to dry pipe, but have a thermal-fusible link on the sprinklers head to be melted before water is released.
- **Deluge:** wide open sprinkler heads to allow a larger volume of water to be released in a shorted period.

Seismic detects sound though the change in vibration.

Proximity detector uses *electromagnetic field*.

MIME specifies how multimedia data and email attachment are transferred over the network. **S/MIME** extended that to provide standard email *encryption* and *digital signature*.

Lattice is an *access control model* that provides bounds outlining what a subject can do pertaining to individual objects.

Wassenaar Arrangement: agreement to not export cryptographic products to certain countries.

Clipper Chip is a hardware encryption chip made for all US communication devices in the 90s. It has 80-bit key and 16-bit checksum. It uses SkipJack as a private algorithm.

Phase Alternative Line (PAL): Video recording and transmission standards for CCTV (in Europe). NTSC is used in US and Japan.

CHAPTER 4: Communication and Network Security

Federal Communications Commission (FCC) regulates telecommunications systems, which includes voice and data transmissions.

Open Systems Interconnection (OSI) model:

- **Application:**
  - SMTP, HTTP, DNS, IRC, LDP.
- **Presentation:**
  - It works as a translator, translating the format an application is using to a standard format used for passing a message over a network (e.g. encode the application message and adds a descriptive header: Content-Type: application/pdf).
  - Handles data compression and encryption.
  - No protocol works on this layer, just services.
- **Session:**
  - Establishing a connection between the two applications, maintaining it during the transfer of data, and controlling the release of this connection.
  - **3 phases (dialog management):** connection establishment, data transfer, connection release.
  - 3 different modes: simplex, half-duplex, full-duplex.
  - Controls application-to-application communications.
  - PAP, PPTP, NetBIOS, RPC.
- **Transport:**
  - Controls computer-to-computer communications.
  - Provides end-to-end data transport services and establishes the logical connection between two communicating computers.
  - TCP, UDP, SPX.
- **Network:**
  - IP, ICMP, RIP, OSPF, BGP, IGMP.
- **Data Link:**
  - Divided into two functional sub-layers:
    - Logical Link Control (LLC) – **IEEE 802.2**:
      - Communicates with the protocol immediately above it, the network layer.
      - Takes care of flow control and error checking.
    - Media Access Control (MAC) – **IEEE 802.3, 802.5, 802.11, 802.16**:
      - Have appropriately loaded protocols to interface with the protocol requirement of the physical layer (Ethernet, Token Ring, WLAN, WiMax, etc.).
  - PPP, ATM, L2TP, FDDI, Ethernet, Token Ring.
- **Physical:**
  - 10Base-T, RS/EIA/TIA-422

TCP/IP model:

- Application (Application + Presentation + Session)
- Host-to-host (Transport)
- Internet (Network)
- Network access (Data link + Physical)

A network can be used as:

- Channel of attack
- Target of attack

RPC has lack of, or weak, authentication. **SRPC** is more secure as it needs two computers to be authenticated before communicating with each other.

Distributed Network Protocol 3 (DNP3):

- A multilayer protocol.
- Designed for use in SCADA systems.
- Control instructions and configurations changes are send from the SCADA master to the RTUs and then on to the sensors and actuators.

Controller Area Network Bus (CAN) – *It is different that Campus Area Network*:

- Runs most of automobiles worldwide.
- Designed to allow microcontrollers and other embedded devices to communicate with each other on a shared bus.

Socket: protocol (UDP/TCP) + port + IP address

Ports:

- **Well-known:** 0 – 1023 (can be used only by privileged system or root processes).
- **Registered:** 1024 – 49151 (can be registered with the ICANN).
- **Dynamic:** 49152 – 65535 (as needed basis).

TCP handshake: SYN – SYN/ACK – ACK.

SYN flood:

- An attacker floods the victim system with SYN packets.
- **Mitigations:** use of *SYN cache*, which delays the allocation of a socket until the handshake is completed.

TCP session hijacking: an attacker can correctly predict the TCP sequence numbers that two systems will use.

TCP packet referred to as *segment* and UDP packet referred to as *datagram*.

IPv4: 32-bits address
IPv6: 128-bits address

Class	Address Range	Description
A	0.0.0.0 to 127.255.255.255	The first byte is the network portion, and the remaining 3 bytes are the host portion.
B	128.0.0.0 to 191.255.255.255	The first 2 bytes are the network portion, and the remaining 2 bytes are the host portion.
C	192.0.0.0 to 223.255.255.255	The first 3 bytes are the network portion, and the remaining 1 byte is the host portion.
D	224.0.0.0 to 239.255.255.255	Used for multicast addresses.
E	240.0.0.0 to 255.255.255.255	Reserved for research.

Table 4-2 IPv4 Addressing

Subnetting:

- Allows larger IP ranges to be divided into smaller, logical, and more tangible network segments.
- Reduces the traffic load across the network, reduce network congestion, smaller broadcast domain.
- Easier to implement network security policies more effectively.
- Keep down routing table sizes because external routers can directly send data to the actual network segment.

Classful/Classical IP addresses: traditional subnets are used.

Classless IP addresses: creation of subnets that do not follow traditional sizes.

Classless interdomain routing (CIDR) (supernetting): specify more flexible IP address classes.

Time to live (TTL) value decremented every time the packet passes through a router, so packet do not continually traverse a network forever.

Type of Service (ToS) that means it can prioritize different packets for time-sensitive functions.

IPv6 (IPng):

- ***IPSec*** integrated into the protocol stack (end-to-end secure transmission and authentication).
- Allows for QoS value to be assigned for time-sensitive transmissions.
- Offers auto-configuration, which makes administration much easier.
- Does not require NAT to extend its address space.

- **Anycast address** is defined, which is used to send a packet to any one of a group of nodes (scalability of multicast routing is improved by adding a "scope" field to multicast addresses).
- Some IPv4 header fields have been dropped or made optional.
- Extension to support authentication, data integrity and (optional) data confidentiality.
- Extends the size of the packet's payload (*jumbograms*) and improve performance over high-*maximum transmission units (MTU)* links.

Automatic tunneling: A technique where the routing infrastructure automatically determines the tunnel endpoints so that protocol tunneling can take place without pre-configuration.

- **6to4 tunneling:** the tunnel endpoints are determined by using a well-known IPv4 anycast address on the remote side and embedding IPv4 address data within IPv6 addresses on the local side.
- **Teredo:** uses UDP encapsulation so that NAT address translations are not affected.
- **Intra-Site Automatic Tunnel Addressing Protocol (ISATAP):** treats the IPv4 network as a virtual IPv4 local link, with mappings from each IPv4 address to a link-local IPv6 address.

6to4 and Teredo are ***intersite*** tunneling mechanisms (connectivity between different network).
ISATAP is an ***intrasite*** mechanism (connectivity between systems within a specific network).

NAT: caused a lot of overhead and transmission problems because it breaks the client/server model that many applications use today.

IEEE 802.1AE:

- IEEE MAC Security standard (MACSec).
- Provides hop-to-hop protection at layer 2.
- Only authenticated and trusted devices on the network can communicate with each other.
- When a frame arrives at a device that is configured with MACSec, the MACSec Security Entity (SecY) decrypts the frame if necessary and computes an integrity check value (ICV) on the frame and compares it with the ICV that was sent with the frame.
- If ICV match, the device processes the frame. If not, the device handles the frame according to a preconfigured policy (e.g. discarding it).
- Provides data encryption, integrity, and data origin authentication.

IEEE 802.1AR:

- Specifies unique per-device identifiers (DevID) and the management and cryptographic binding of a device to its identifiers.
- A verifiable unique identity allows establishment of the trustworthiness of devices.
- Each device comes with single built-in initial secure device identity (***iDevID***).
- iDevID is used with authentication protocols such as EAP; which is supported by IEEE8.2.1X.

IEEE 802.1AF:

- carries out key agreement functions for the session keys for data encryption.

802.1X:

- device cannot carry out any network activity until it is authenticated to so do.
- Port authentication kicks-in, which means that only authentication data is allowed to travel from the new device to the authentication server.
- The authentication data is the digital certificate and hardware identity associated with that device (IEEE 802.1AR), which is processed by EAP-TLS.
- Once authenticated by authentication server (e.g. RADIUS), encryption keying materials is negotiated and agreed upon between surrounding network devices.

Converged protocols: protocols start started off independent and distinct from one another but over time converged to become one (or one protocol started being encapsulated/tunneled within the other one).

- **Fiber Channel over Ethernet (FCoE):**
  - Protocol encapsulation that allows Fiber Channel (FC) frames to ride over Ethernet networks.
- **Multiprotocol Label Switching (MPLS):**
  - Was originally developed to improve network performance.
  - But frequently used for its ability to create VPNs over a variety of layer 2 protocols.
  - It has elements in both layer 2 and layer 3 (referred to as 2.5 protocol).
  - Considered converged protocol because it can encapsulate any higher-layer protocol and tunnel it over a variety of links.
- **Internet Small Computer System Interface (iSCSI):**
  - Encapsulate SCSO data in TCP segments.

IP convergence is the transition of services from disparate transport media and protocols to IP (e.g. VoIP).

Analog signals are measured in amplitude and frequency.
Digital signals represent binary digits as electrical pulses (*more reliable*).

Modem (modulator/demodulator) modulates the digital data into an analog signal.

Bandwidth: the number of electrical pulses that can be transmitted over a link within a second, and these pulses carry individual bits of information.

Data throughput: the actual amount of data that can be carried over a connection.

Data throughput values can be higher than *bandwidth* values if compression mechanisms are implemented. But if links are highly congested or there are interference issues, the *data throughput* values can be lower.

Synchronous vs. Asynchronous transmission: communicated systems do not use start and stop bits, but the synchronization of the transfer of data take place through a timing sequence, which is initiated by a clock pulse.
Data link protocol has the synchronization rules:

- High-level Data Link Control - HDLC (synchronous)
- Asynchronous Transfer Mode - ATM (asynchronous)

Baseband: uses the entire communication channel for its transmission.

Broadband: divides the communication channel into individual and independent sub-channels so that different types of data can be transmitted simultaneously (*e.g. CATV: multiple channels over the same cable*).

Digital subscriber line (DSL) uses one single phone line and constructs a set of high-frequency channels for Internet data transmissions.

Coaxial cables:

- Copper core that is surrounded by a shielding layer.
- Compared to twisted-pair cable is more resistant to electromagnetic interference (EMI) and supports longer cable lengths, but more expensive and harder to work with.

Twisted-paid cable:

- Shielded twisted pair (STP) have an outer foil shielding.
- Unshielded twister pair (UTP) does not have this extra shielding.
- Resists the flow of electrons, which causes a signal to degrade after travelling a distance.
- Radiates energy, which means information can be monitored and captured.

Fiber-optic cable:

- Not affected by attenuation and EMI.
- Does not radiate signals and difficult to eavesdrop on.
- **Light sources:**
  - Light-emitting diodes (LEDs)
  - Diode lasers
- **Modes:**
  - **Single-mode:** high-speed data transmission over long distances.
  - **Multi-mode:** able to carry more data than single-mode and best for shorted distances because of their higher attenuation levels.

Crosstalk occurs when electrical signals of one wire spill over to the signals of another wire.

Plenum-rated cables have jackets covers made of fluoropolymers, whereas non-plenum cables usually have a polyvinyl chloride (PVC) jacket.
For better security, wires can be encapsulated into ***pressurized conduits***.

Topology	Characteristics	Problems
Bus	Uses a linear, single cable for all computers attached. All traffic travels the full cable and can be viewed by all other computers.	If one station experiences a problem, it can negatively affect surrounding computers on the same cable.
Ring	All computers are connected by a unidirectional transmission link, and the cable is in a closed loop.	If one station experiences a problem, it can negatively affect surrounding computers on the same ring.
Star	All computers are connected to a central device, which provides more resilience for the network.	The central device is a single point of failure.
Tree	A bus topology with branches off of the main cable.	Multiple single points of failure.
Mesh	Computers are connected to each other, which provides redundancy.	Requires more expense in cabling and extra effort to track down cable faults.

Table 4-4 Summary of Network Topologies

Media access technologies

- **Token Passing:**
  - A token is a 24-bit control frame.
  - The token contains the data to be transmitted and source and destination address information.
  - The token is passed from computer to computer, and only the computer than has the token can actually put frames onto the wire.
  - Each computer checks the message to determine if it is addressed to it, which continues until the destination computer receives it.
  - The destination computer makes a copy of the message and flips a bit to tell the source computer it did indeed get its message.
  - Used in **Token Ring** and **FDDI** technologies.
- **Carrier sense multiple access (CSMA):**
  - Ethernet uses CSMA to provide media-sharing capabilities.
  - **CSMA/CD:**
    - If a computer puts frames on the wire and its frames collide with another computer's frame, it will abort its transmission and alert all other stations that a collision just took place.
    - ***back-off algorithm:*** all stations will wait a random time before attempting to transmit again.
    - Used in **Ethernet** technology.
  - **CSMA/CA:**
    - Each computer signals its intent to transmit data.
    - Once the medium is clear, a computer sends a broadcast stating that it is looking to transmit data.
    - Used in **WLAN 802.11** technology.
  - **Polling:**

- Some systems are configured as primary stations and others are secondary stations.
- At predefined internals, the primary station asks the secondary station if it has anything to transmit.
- Used in **mainframe** media access technology.

Carrier sensing access methods are faster than token-passing methods, but the former do have the problem of collisions.

Contention-based environment is where each system has to "compete" to use the transmission lines, which can cause contention.

Bridges allow broadcast traffic to pass between different parts of a subnet, but not the collisions.

If two LANs are connected by a router, the result is an **internetwork**.

If two LANs are connected by different data layer technology, they are considered a **WAN**.

Ethernet 802.3:

- Usually uses a **bus** or **star** topology
- Contention-based technology (CSMA/CD)
- User broadcast and collision domains
- Uses CSMA/CD
- Supports full-duplex communication
- Can use coaxial, twisted-pair, or fiber-optic cabling

10Base-T (10Mbps): Twisted-pair wiring uses one wire to transmit data and the other to receive data.

10Base2 (Thin Net): uses thin, flexible coaxial cable that is easy to work with. (185 meters).

100Base-TX (100Mbps)

1000Base-R (1,000Mbps): all four pairs of twisted unshielded cable pairs are used for simultaneous transmission in both directions for a maximum distance of **100m**.

10GBase-T (10,000Mbps)

Token Ring IEEE 802.5:

- First, it has ability to transmit data at 4Mbps, and later improved to reach **16Mbps**.
- Each computer is connected to a central hub, called a ***Multi-station Access Unit (MAU).***
- **Physical star** topology, but signals passes in **logical ring**.
- **Active monitor** removes frames that are continuously circulating on the network.

- **Beaconing:** if a computer detects a problem with the network, it sends a beacon frame. This frame generates a failure domain, which is between the computer that issues the beacon and its neighbor downstream.

Fiber distributed data interface (FDDI IEEE 802.4):

- High-speed, token-passing, media access technology.
- Transmission speed up to 100Mbps.
- Usually used as a back-bone network using fiber-optic cabling.
- It provides **fault tolerance** by offering a second counter-rotating fiber ring.
- The primary ring has data travelling clockwise and it used for regular data transmission.
- The second ring transmits data in a counter-clockwise fashion and is involved only if the primary ring goes down.
- It enables several tokens to be present on the ring at the same time, causing more communication to take place simultaneously.
- A version of FDDI is **CDDI** that works over UTP cabling.
- **FDDI-2** allows for fixed bandwidth to be assigned (good for QoS).
- Devices that connect to FDDI rings falls into one of the following categories:
    - **Single-attachment station (SAS):** attaches to only one ring (primary) through a concentrator.
    - **Dual-attachment station (DAS):** has two ports and each port provides a connection for both the primary and secondary rings.
    - **Single-attached concentrator (SAC):** concentrator that connects an SAS device to the primary ring.
    - **Dual-attached concentrator (DAC):** concentrator that connects DAS, SAS, and SAC devices to both rings.

Unicast transmission: a packet needs to go from the source computer to one particular system.

Multicast transmission: a packet needs to go to a specific group of systems.

Broadcast transmission: a system wants all computers on its subnet to receive a message.

IPv4 multicast protocols uses a Class D address (224.0.0.0 to 239.255.255.255).
IPv6 multicast addresses start with eight 1's (1111 1111).

Address resolution protocol (ARP) translates IP address to MAC address.

ARP table cache poisoning: the attacker goal is to receive packets intended for another computer (*masquerading attack*).

Dynamic host configuration protocol (DHCP):

- UDP-based protocol.
- Eliminates the possibility of IP address conflicts.

- **DORA (Discover-Offer-Request-Acknowledge):**
  - The client computer broadcasts a **DHCPDISCOVER** message on the network in search for the DHCP server.
  - The server responds with a **DHCPOFFER** packet, offering the client and IP address and other configuration settings.
  - The client responds to the server with a **DHCPREQUEST** packet confirming its acceptance of the allotted settings.
  - The server responds with a **DHCPACK** packet, which includes the validity period (lease) for the allocated parameters.

Both the client and server segments of the DHCP are vulnerable to **falsified identity**.

Attacker can implement a rouge DHCP server:

- Compromising client system configurations.
- Carry out man-in-the-middle attacks.
- Route traffic to unauthorized networks.

DHCP snooping: implemented on network switches to ensures that DHCP servers can assign IP addresses to only selected systems, identified by their MAC addresses.

RARP frames go to all systems on the subnet, but only RARP server responds. Once the RARP server receives this request, it looks in its table to see which IP address matches the broadcast hardware address (e.g. *used by diskless workstations*).

Bootstrap protocol (BOOTP) was created after RARP to enhance its functionality.

Internet control message protocol (ICMP):

- IP's "messenger boy".
- Delivers status messages, reports errors, replies to certain requests, reports routing information, used to test connectivity and troubleshooting problems.
- ***ping*** utility: ICMP Echo Request frame & ICMP Echo Reply frame.
- Routers use ICMP to send messages in response to packets that could not be delivered.
- ICMP is used by other connectionless protocols, not just IP.

Attacks using ICMP:

- ***ICMP tunneling:***
  - Insertion of data inside an ICMP packet.
  - The attacker would target a computer and install the server portion of the tunneling software. This server portion would "listen" on a port, which is the back door an attacker can use to access the system.
- ***Traffic redirection:***
  - Routers uses ICMP to update status about network links.

- Attacker can send bogus information to direct to his machine, or it can be redirected into a "black hole".

Countermeasures:

- Use firewall rules that only allow the necessary ICMP packets into the network.
- Use of IDS and IPS to watch for suspicious activities.
- Host-based protection (host firewall and host IDS) can also be installed.

Simple network management protocol (SNMP):

- Uses UPD port 161 (SNMP) and 162 (SNMPTRAP).
- 2 main components: manager and agent.
- **Manager** is the server portion, which polls different devices to check status information. It also receives trap messages from agents and provides a centralized place to hold all network-wide information.
- **Agent** has a list of objects that it is to keep track of, which is held in a database-like structure called the ***Management Information Base (MIB)***.
- **Trap** operation allows the agent to inform the manager of an event, instead of having to wait to be polled (e.g. *interface on a router goes down*).
- **Community string** is basically a password a manager uses to request data from the agent. The string can have different levels of access: *read-only* and *read-write*.
- If an attacker can uncover the read-write string, she could change values held within the MIB (e.g. *reconfigure the device*).
- The default read-only community string is "*public*" and the read-write is "*private*".
- SNMPv1 and SNMPv2 community string is sent as ***cleartext***.
- SNMPv3 has ***cryptographic*** functionality.

Domain name service (DNS):

- Converts name to IP address
- Within DNS servers, DNS namespaces are split up administratively into **zones**. One zone may contain all hostnames for the marketing and account departments.
- DNS server that holds the files for one of these zones is said to be the ***authoritative name server*** for that particular zone.
- **Resource record:** a record contained in the SN server that map hostname to an IP address.
- It is recommended that a primary and secondary DNS server cover each zone. The primary server contains the actual resource records for a zone, and the secondary server contains copies of those records. Synchronization happens though ***zone transfer***.
- An unauthorized zone transfer provides an attacker with information on almost every system within the network, if the DNS servers are not properly configured (e.g. attacker can map the network).
- If one DNS server does not know which DNS server holds the necessary resource record to resolve a hostname, it can pass the request up to a DNS server above it.
- Top-level domains: com, net, org, edu, mil, int, gov.
- ***DNS resolver***:

  - In your computer, which is responsible for sending out requests to DNS servers for host IP address information.
  - Resolver can send a **non-recursive query** or a **recursive query**.
- **HOST file**:
  - Resides on the local computer and can contain static hostname-to-IP address mapping information.
  - Malicious manipulation can happen to the HOSTS file involves blocking users from visiting antivirus update websites, which is usually done by mapping target hostnames to the *loopback interface IP address 127.0.0.1*.

DNS poisoning:

- An attacker sees the DNS Server A and querying DNS server B for a resource record, here the attacker replies back to DNS server A with incorrect record, which poisons the DNS cache table. This happens because DNS server doesn't authenticate the sender/responder.
- **Countermeasure:**
  - Usage of **DNSSEC** (DNS Security), which implements KPI and digital signatures, which allows DNS server to validates the origin of a message to ensure that it is not spoofed.

DNS splitting:

- Internal SNS server should only contain resource records for the internal computer systems.
- External DNS server should only contain recourse records for the systems that organization wants the outside world to be able to connect to (information of systems within the DMZ).

URL hiding: embeds hyperlinks in any given text (e.g. Click Here).

Domain grabbing & Cyber squatting: individuals who register prominent or established names, hoping to sell these later to real-world businesses.

SMTP:

- Uses TCP port 25.
- Works as a message transfer agent.
- Works as a message transfer protocol between email servers.
- Is a message-exchange addressing standard: xxx@xxx.xxx
- Most commonly SMTP servers: *Sendmail* (Unix) & Microsoft Exchange (Windows).

Post office protocol (POP):

- Internet mail server protocol.
- A mail server that uses POP, apart from storing and forwarding email messages, works with SMTP to move messages between mail servers.

- Messages are held on the mail server until users are ready to download their messages, instead of trying to push messages right to a person's computer, which may be down or offline.

Internet mail access protocol (IMAP):

- Provides all the functionalities of POP, but has more capabilities.
- Once the messages are downloaded from the POP server, they are usually deleted from that server, depending upon the configuration. In IMAP, user can leave emails on the mail server within her remote message folder (***mailbox***).
- IMAP is a *store-and-forward* mail server protocol.

Simple Authentication and Security Layer (SASL):

- POP3 has the capability to a protocol-independent framework for performing authentication. It means that any protocol can use SASL for authentication without the need to embed the authentication mechanism within its code.
- Data security layer can provide data confidentiality, integrity, and other services.
- IMAP, IRC, LDAP and SMTP use SASL.

Email relaying:

- Public mail server in the DMZ and one or more mail servers within the internal LAN.
- Mail servers use a ***relay agent*** to send a message from one mail server to another.
- Relay agent should be properly configured, so attacker cannot use it for spamming activities.
- **"wide open"** configuration means that a mail server can be used to receive any mail message and send it to any intended recipients.

Email threats:

- ***Email spoofing*** is a technique by malicious users to forge an email to make it appear to be from a legitimate source.
- ***SMTP authentication (SMTP-AUTH)*** is an extension that comprises an authentication feature that allows clients to authenticate to the mail server before an email is sent.
- To deal with forged email messages, ***Sender Policy Framework*** can be used. It is an email validation system designed to prevent email span by detecting email spoofing by verifying the sender's IP address.

Network address translation (NAT):

- Private IP address ranges:
  - 10.0.0.0 – 10.255.255.255 (Class A)
  - 172.16.0.0 – 172.31.255.255 (Class B)
  - 192.168.0.0 – 192.168.255.255 (Class C)
- NAT implementations:
  - **Static mapping:** private address mapped to public address

- **Dynamic mapping:** dynamically mapping a private address to one available public address.
- **Port address translation (PAT):** can use single public IP address with many ports

Routing protocols:

- Individual networks on the Internet is referred to as ***autonomous system (AS)***, which are independently controlled by different service providers and organizations.
- AS is made up of routers that are administered by a single entity and use a common Interior Gateway Protocol (IGP) within the boundaries of the AS.

Dynamic vs. Static:

- **Dynamic routing protocol** can discover routes and build a routing table.
- **Static routing protocol** requires the administrator to manually configure the router's routing protocol.

Distance-Vector vs. Link-State:

- **Distance-vector routing protocol** make their routing decisions based on the distance (or number of hops) and a vector (a direction).
- **Link-state routing protocol** build a more accurate routing table because they build a topology database of the network (metrics: packet size, link speed, delay, network load, reliability).

Interior routing protocols:

- **Routing Information Protocol (RIP):** distance-vector protocol.
- **Open Shortest Path First (OSPF):** uses link-state algorithms.
- **Interior Gateway Routing Protocol (IGRP):** distance-vector routing protocol (*proprietary to Cisco*).
- **Enhanced Interior Gateway Routing Protocol (EIGRP):** advanced distance-vector routing protocol (*proprietary to Cisco*).
- **Virtual Router Redundancy Protocol (VRRP):** two physical routers (primary and secondary) are mapped to one virtual router. If one fails, the other takes over the load.
- **Intermediate System to Intermediate System (IS-IS):** link-state protocol. Doesn't use IP addresses. Instead, it uses ISO addressed, which means that the protocol didn't have to be redesigned to support IPv6.

Exterior routing protocols (exterior gateway protocols, EGPs):

- **Boarder Gateway Protocol (BGP):**
  - Uses a combination of link-state and distance-vector routing algorithms.
  - Creates network topology by using its link-state functionality.
  - Transmits updates on a periodic basis instead of continuously, which is how distance-vector protocols work.

Route flapping refers to the constant changes in the availability of routes.

If a router does not receive an update that a link has gone down, the router will continue to forward packets to that route, which is referred to as a ***black hole***.

Wormhole attack:

- An attacker can capture a packet at one location in the network and tunnel it to another location in the network (two attackers, one at each end of the tunnel).
- **Countermeasure:** use of ***leash***, which is just data that is put into a header of the individual packets. This leash restricts the packet's maximum allowed transmission distance. It can be either ***geographical*** or ***temporal***.

Repeaters:

- Works as line conditioners by actually cleaning up the signals.
- A ***hub*** is a multiport repeater and is often referred to as a ***concentrator***.

Bridges:

- Connect LAN segments.
- Works at data link layer and therefore work with MAC addresses.
- Used to divide overburdened networks into smaller segments to ensure better use of bandwidth and traffic control.
- Used to extend a LAN and enable the administrator to filter frames.
- Isolates collision domains within the same broadcast domain.
- Forward broadcast frames. So, you have you have to watch carefully for ***broadcast storms***.
- Uses ***transparent bridging***, where a bridge starts to learn routes by examining frames and making entries in its forwarding table.
- Uses **Spanning Tree Algorithm (STA)**:
  - Ensures that frames do not circle networks forever
  - Provides redundant paths in case a bridge goes down.
  - Enables an administrator to indicate weather he wants traffic to travel certain paths instead of others.
- 3 main types of bridges:
  - **Local:** connects two or more LAN segments within a local area (e.g. building).
  - **Remote:** can connects two or more LAN segments over a MAN by using telecommunication links.
  - **Translation:** need if two LANs being connected are different types and use different standards and protocols.

Routers:

- Connect similar or different networks (e.g. two Ethernet LANs or an Ethernet LAN and Token Ring LAN).

- It can filter traffic based on access control lists (ACLs) and fragments packets when necessary.
- In ACL, access decisions are based on source and destination IP addresses, protocol type, and source and destination ports.
- If router does not have information in its routing table about the destination address, it sends out an ICMP error message to the sending computer indicating that the message could not reach its destination.
- If the destination network requires a smaller MTU, the router fragments the datagram.

Switches:

- High level switches offer routing functionality, packet inspection, traffic prioritization, and QoS functionality. It creates a lot of overhead, but multilayered switches perform these activities using an ASIC chips.

Layer 3 and 4 Switches:

- A layer 3 switch is basically ***a router on steroids***, because it moves the route lookup functionality to the more efficient switching hardware level.
- It can use ***tags***, which are assigned to each destination network or subnet.
- The switch appends the tag to the packet and sends it to the next switch. All the switches in between this first switch and the destination host just review the tag information to determine which router it needs to take, instead of analyzing the full header. (***Multiprotocol Label Switching, MPLS***).
- When MPLS is used, different priority information is placed into the tags to help ensure that time-sensitive traffic has a higher priority than less sensitive traffic.

VLAN (IEEE 802.1Q):

- Enable administrators to logically separate computers based on resource requirement, security, or business needs.
- **Attacks:**
  - VLAN hopping: attacker manage to move from VLAN to another.
  - Switch spoofing: attacker have a system acts as a switch to gain access to traffic.
  - Double tagging: an attacker insert VLAN tags to manipulate the control of traffic at the data link layer.

Gateways:

- A general term for software running on a device that connects two different environments and that many times acts as a translator for them.
- A popular type is an ***electronic mail gateway*** (translate email send from one mail server to another to a standard format, X.400, that both will understand).
- ***Voice and media gateway*** is another example.

Private Branch Exchange (PBX):

- A private telephone switch that is located on a company's property.
- Performs same switching tasks that take place at the telephone company's central office.
- The voice data is multiplexed onto a dedicated line connected to the telephone company's central office.
- Many companies have modems hanging off their PBX to enable vendor to dial in and perform maintenance to the system (usually unprotected).
- PBX is *vulnerable to brute-force* (preacher uses scripts and dictionaries to gain access to the system).

Source routing:

- Packets contain the necessary information within them to tell the bridge or router where they should go. It doesn't require the bridge or router to dictate their paths.
- External and boarder devices should not accept packets with source routing information within their headers.

Phreaker:

- is a phone hacker who knows knows the default password of modems can perform malicious activities (e.g. *toll fraud*).
- In some cases, he changes people's voice messages (e.g. someone screams).

Firewalls:

- Supports and enforce the company's network policy.
- Considered as a "choke point" in the network because all communication should flow through it, and this is where traffic is inspected and restricted.
- Can discard packets, repackage them, or redirect them.
- **Packets are filtered based on their** source and destination addresses, and ports by service, packet type, protocol type, header information, sequence bits, and must more.
- Used to construct a demilitarized zone (DMZ), which is a segment between protected and unprotected networks.

Packet-filtering firewall:

- 1st generation of firewalls.
- Packet-filtering processes is configured with ACLs.
- The ACL filtering rules are enforced at the network interface of the device.
- Have capability of reviewing protocol header information at the network and transport layers.
- Access decisions based upon the following basic criteria:
    - Source and destination IP addresses
    - Source and destination port numbers
    - Protocol types
    - Inbound and outbound traffic direction (*ingress* and *egress*)
- Packet filtering is also known as *stateless inspection*

- **Weaknesses:**
  - Cannot prevent attacks that employs application-specific vulnerabilities.
  - Limited logging functionality.
  - Most packet-filtering firewalls do not support advanced user authentication schemes.
  - Many packet-filtering firewalls cannot detect spoofed addresses.
  - They may not be able to detect packet fragmentation attacks.

Stateful firewalls:

- maintains a *state table* to keep track of each and every communication session.
- Can detect out of order TCP handshake.
- Can detect malicious activity if all TCP flag values are set.
- Can track connectionless protocols (UDP) by keeping track of source and destination addresses, UDP header, and some ACL rules. It'll time-out the connection after a period of inactivated as there is not tear-down stage.
- Provides a high degree of security and does not introduce the performance hit introduced by *application proxy firewall*.
- ***Weakness:*** can be victim of many types of DoS attacks.

Proxy firewalls:

- Stands between a trusted and untrusted network (e.g. HTTP proxy).
- Breaks the communication channel. There is not direct connection between the two communicating devices.
- ***circuit-level proxy:***
  - Proxy-based firewall that works at the lower layers
  - Creates a connection (circuit) between the two communicating systems.
  - Works at the *session layer*.
  - Monitors traffic from a network-view.
  - Similar to packet-filtering firewall as it makes it decision based on address, port, and protocol type header values.
  - **SOCKS** is an example of a circuit-level proxy gateway that provides a secure channel between two computers.
- ***application-level proxy***:
  - Proxy-based firewall that works at the application layer**.**
  - Inspects the packet up through the application layer.
  - Can distinguish between an FTP GET command and FTP PUT command.
  - Extensive logging capabilities (as it can inspect more information).
  - Capable of authenticating users directly.
  - Can address spoofing and other sophisticated attacks.
  - ***Disadvantages:***
    - Create performance issues.
    - Not suited to high-bandwidth or real-time applications.
    - Limited in terms of support for new network applications/protocols.

- One proxy per protocol that understands how a specific protocol works.

Dynamic packet-filtering firewalls:

- The sending system must choose a dynamic port, when it sets up a connection with another entity. The dynamic packet-filtering firewall then creates an ACL that allows the external entity to communicate with the internal system via this port.
- If this was not an available option in the firewall, you would have to allow "punch holes" in your firewall for all ports above 1023, because the client side chooses these ports dynamically.
- Once communication finishes, the ACL is removed from the list.
- Allowing any type of traffic outbound and permitting only response traffic inbound.

Kernal proxy firewalls:

- 5th generation firewall.
- Creates dynamic, customized network stacks when a packet needs to be evaluated.
- When a packet arrives, a new virtual network stack is created (e.g. if it is an FTP packet, then the FTP proxy is loaded in the stack).
- Faster than application/level proxy firewall, because all the inspection and processing takes place in the kernel and does not need to be passed up to a higher software layer in the OS.
- It is still proxy-base system where communication between communicating entities is broken.

Next generation firewalls (NGFWs):

- In incorporates a signature-based IPS.
- Ability to connect to external data sources such as AD, whitelists, blacklists, and policy servers.

- **Dual-homed firewall:**
  - a device that has two interfaces: one connected to one network and the other connected to a different network.
  - If firewall software is installed in a device, the device must have the routing and forwarding disabled (to ensure ACL is applied as expected).
  - **Multi-homed:** they have several NICs that are used to connect several different networks (e.g. a company can have several DMZs).
  - Different DMZs are used for 2 reasons:
    - Control the different traffic types (makes HTTP traffic only goes toward web servers and DNS requests towards DNS server).
    - If one system on one DMZ is compromised, the other systems in the rest of the DMZs are not accessible to this attacker.

- **Screened host (single-tiered configuration):**
  - a firewall that communicates directly with a perimeter router and the internal network.
  - The *screened host* (the *firewall*) is the only device that receive traffic directly from the router.
  - For any attacker to be successful, they should compromise the router and the firewall.
  - The *router* is the *screening device*, which gets rid of a lot of the "junk" before it is directed toward the firewall.

- **Screened subnet (two-tiered configuration):**
  - Adds another layer of security to the screened-host architecture.
  - The use of two physical firewalls creates a DMZ.
  - The attacker needs to hack two firewalls to gain access.

Virtual firewalls can be used to control and monitor traffic between virtual machines within a host. Also, it can be embedded within the hypervisor, which allow it to monitor all activities taking place within the system.

Usage of **appliances** is usually **more secure** as it uses a **stripped-down OS**.

The **default** action of firewall should be ***implicit deny***.

Any packet entering the network that has a source of an internal host should be denied (*masquerading* or *spoofing*).

No packets allowed from to go outbound if it does not have internal source address (indication of *DDoS zombie activity*).

Firewalls should reassemble fragmented packets before sending them on to their destination. Because firewall cannot make decision based on partial packets (*traffic delay and more overhead*).

Fragmentation attacks: attackers have constructed several exploits that take advantage of some of the packet fragmentation steps within networking protocols:

- **IP fragmentation:** exploits fragmentation flaws within IP, which causes DoS.
- **Teardrop attack:** malformed fragments are created and once they are assembled, they could cause the victim system to become unstable.
- **Overlapping fragment attack:** used to subvert packet filters that do not reassemble packet fragments before inspection. A malicious fragment overwrites a previously approved fragment and executes an attack on the victim's system.

Common firewall rules:

- ***Silent rule:*** drops "noisy" traffic without logging.
- ***Stealth rule:*** disallow 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 primitive "any rules", provides tighter permission rights by specifying what system can be accessed and how.

Bastion host is a highly exposed device that is more likely to be targeted by attackers (in the public side of a DMZ or it directly connected to an untrusted network).

Forwarding proxy is one that allows the client to specify the server it wants to communicate with.

Open proxy is a forwarding proxy that is open for anyone to use.

Reverse proxy appears to the client as the original server. The client sends a request to what it thinks is the original server, but in reality this reverse proxy makes a request to the actual server and provides the client with the response.

Web proxy servers:

- carries out content filtering, block unacceptable web traffic, and logging.
- It can act as caching server.

Honeypot:

- A computer that is intended to be exploited by attackers (*usually in screened subnet or DMZ*).
- Some ***emulates*** services, where the actual services are not running but software that acts like those services is available.
- Should not be connected to production systems.
- On a small scale, companies may choose to implement ***tarpits***. Tarpit can be configured to appear as a vulnerable service that attackers will commonly attempt to exploit. Once the attacker establishes a connection to the victim system, everything seems to be live, but the response from the victim system is slow and the connection may time out.
- Due to slow or no reply by tarpits, automated tools may not be successful.

Unified threat management (UTM):

- Appliance products that provides all (or many) of functionalities in a single network appliance.
- The goal of UTM are simplicity, streamlined installation and maintenance and centralized control.
- ***Drawbacks:***
  - Single point of failure for traffic

- Single point of compromise
- Performance issues

Content distribution networks (CDNs):

- Consists of multiple servers distributed across a large region, each of which provides content that is optimized for users closet to it.
- Makes your internet presence more resistant to DDoS attacks.

Software defined networking (SDN):

- Much easier to dynamically route traffic to/from newly provisioned services and platforms.
- Centralizes the configuration and control of devices
- Control plane is implemented in a central node. Other network devices are left to do the forwarding.
- All changes are pushed out to the devices either reactively (e.g. in response to request from the devices) or proactively (e.g. admin know a change is being made).
- Abstraction of control and forwarding planes.
- **Control plane:**
  - is where internetwork routing decisions are being made.
  - Responsible of discovering the topology of neighboring networks.
  - Maintaining a table of routes for outbound packets.
- **Forwarding plane:**
  - Decision of forwarding happen based on the product of the control plane.
  - Typically implemented in hardware (ASIC).
- **Approaches of SDN:**
  - **Open:**
    - It relies on open-source code. The most common.
    - The controller communicates with the switches using OpenFlow.
    - Allows devices implementing the forwarding plane to provide information (e.g. data utilization) to the controller, while allowing the controller to update the flow tables once the devices.
    - Applications communicate with the controller using the RESTful or Java APIS.
  - **API:**
    - Championed by Cisco.
    - In addition to OpenFlow, this approach leverages a rich API on proprietary switches that allows greater control over traffic in an SDN.
    - Covers the shortage of OpenFlow inability to do deep packet inspection and manipulation (enriching SDNs' Open approach, rather than replacing).
  - **Overlays:**
    - Virtualize all network nodes, including switches, routers, and servers, and treat them independently of the physical networks upon which this virtualized infrastructure exists.

- The SDN simply exists simply as a virtual overlay on top of a physical (underlay) network.

Web-based clients:

- Limit a user's ability to access the computer's system files, resources, and hard drive space; access back-end systems; and perform other tasks.
- Can be configured to provide a GUI with only the buttons, fields, and pages necessary for the users to perform tasks.

Intranet: web-based technologies only available inside the company's network.

Extranet:

- Extends outside the bounds of the company's network to enable two or more companies to share common information and resources.
- Used to be based mainly on dedicated transmission lines which are more difficult to attackers to infiltrate.
- Can be set over internet, which requires properly configured VPNs and security policies.

Trading partners often use ***electronic data interchange (EDI)***, which provides structure and organization to electronic documents, orders, etc.

Value-added network (VAN) is an EDI infrastructure developed and maintained by a service bureau (uses XML, SOAP, web services).

Metropolitan Area Networks (MAN):

- The backbone that connects LANs to each other and LANs to WANs, the internet, and telecommunications and cable networks.
- The majority of today's MANs are:
  - Synchronous Optical Networks (SONET):
  - FDDI rings
  - Metro Ethernet
- SONET and FDDI rings cover large area, and businesses can connect to the rings via T1, fractional T1, and T3 lines.
- MANs can be made up of wireless infrastructures, optical fiber, or Ethernet connections.
- A service provider commonly uses layer 2 and 3 switches to connect optical fibers.
- VLANs are used to allow isolation of different customer's traffic and the core network internal signaling traffic.
- MAN architectures are commonly built on such layers: access, aggregation/distribution, metro and core.

SONET:

- A standard for telecommunications transmissions over fiber-optic cables.

- *Self-healing:* if a break in the lines occurs, it can use a backup redundant ring to ensure transmission continues. All SONET lines and rings are fully redundant.
- Can transmit voice, video, and data over optical networks.

Metro Ethernet:

- Ethernet can connect to previously mentioned MAN technologies, or they can be extended to cover a metropolitan area, which is called Metro Ethernet.
- Can be used as *pure Ethernet* (less expensive and less scalable), or *integrated with other technologies, as in MPLS*, (more expensive and more scalable).

Virtual Private LAN Service (VPLS): is a multipoint, layer 2 VPN that connects two or more customer devices using Ethernet bridging techniques, in other words, VPLS emulates LAN over a managed IP/MPLS network.

Wide Area Networks (WANs):

Telecommunication Evolution:

- Copper lines carry purely analog signals.
- Digital phone systems emerged with ***T1*** trunks, which carried *24 voice communication* calls over two pair of copper wires (*1.544 Mbps* transmission rate).
- Trunk can be implemented on ***T3*** lines, which can carry up to *28 T1 lines* (*44.736 Mbps* transmission rate).
- Then ***SONET*** came, an optical-fiber technology for telecommunications transmission over fiber-optic cables.
- The next step was ***Asynchronous Transfer Mode (ATM)***. ATM encapsulates data in fixed cells and can be used to deliver data over a SONET network. Fixed cells provides better performance and a reduced overhead for error handling.
- **Europe** uses **Synchronous Digital Hierarchy (SDH).** SHD and SONET are similar but *incompatible*.

Dedicated links: also called leased lines or point-to-point link. It is dedicated and expensive.

T-Carriers:

- Dedicated lines that carry voice and data information over trunk lines. (e.g. Fractional T1, T1, T2, T3, T4).
- It offers multiplexing functionality through **time-division multiplexing (TDM**).
- **Fractional T lines:** T1 channels are split up between companies who do not really need the full bandwidth (1.544 Mbps).

E-Carriers:

- Similar to T-carriers and uses TDM for multiplexing.
- **30 channels** interleave 8 bits of data in a frame.

Optical Carrier:

- High-speed fiber-optic connection measured in optical carrier (OC) transmission rates.
- Referred to as **OCx**, where the "x" represents a multiplier of the basic OC-1 transmission rate, which is **51.84 Mbps**. (e.g. OC-12: 622.08 Mbps).

Statistical time-division multiplexing (STDM): analyzes statistics related to the typical workload of each input device, and allocate the required time for data transmission.

Frequency-division multiplexing (FDM): available frequency band is divided into narrow frequency bands and used to have multiple parallel channels for data transfer.

Wave-division multiplexing (WDM): used in fiber-optic communication, which multiplexes a number of optical carrier signals onto a single optical fiber.

CSU/DSU (channel service unit/data service unit):

- Required when digital equipment will be used to connect a LAN to a WAN. This connection take place with T1 and T3 lines.
- Signals and frames can vary between the LAN equipment and the WAN equipment used by service providers.
- DSU device converts digital signals from routers, switches, and multiplexers into signals that can be transmitted over the service provider's digital lines.
- CSU connects the network directly to the service provider's line.
- CSU/DSU provides a digital interface for *data terminal equipment (DTE),* such as terminal or routers, and interface to the *data circuit-terminating equipment (DCE)* device, such as a carrier's switch.

Switching:

- Circuit switching:
  - Sets up a virtual connection that acts like a dedicated link between two systems (e.g. ISDN and telephone calls).
  - Dedicated virtual communication link is set up. Devices do not dynamically move the call through different devices.
- Packet switching:
  - Packets from one connection can pass through a number of different individual devices (e.g. Internet, Frame Relay, X.25).
  - Provide multiple paths to the same destinations, which offers a high degree of redundancy.
  - Data broken into packets and can be travelling into different routes, once received by the receiver, packets must be reassembled in the correct order using *Frame Check Sequence (FCS) numbers*.

Frame Relay:

- It is a WAN technology that operates at the data link layer and uses packet-switching technology.
- To avoid unnecessary cost, companies moved from dedicated lines to frame relay. Cost is based on the amount of bandwidth used.
- Companies that pay more, ensures a higher level of bandwidth will always be available (***committed information rate CIR***).

Virtual Circuits:

- Frame relay (and X.25) forwards frames across virtual circuits.
- Permanent circuit: programmed in advanced (e.g. worked likes a private line with an agreed-upon bandwidth availability).
- Switched circuit: quickly built when it is needed and torn down when it is no longer needed (e.g. used for teleconferencing, establishing temporary connections to remote sites, data replication, voice calls.

X.25:

- An older WAN protocol works in a switching technology.
- Provides any-to-any connection.
- Subscribers are charged based on the amount of bandwidth they use.
- Data is encapsulated in High-level Data Link Control (HDLC) frames.
- Provide many layers of error checking, error correcting, and fault tolerance.

ATM:

- A connection-oriented switching technology. It uses a cell-switching method (e.g. more efficient and faster use of the communication paths).
- Used for LAN, MAN, WAN, and service provider connections.
- ATM set up a virtual circuit that can guarantee bandwidth and QoS (e.g. good carrier for voice and video transmission).
- Used by carriers and service providers, and is the core technology of the Internet.

Quality of Service (QoS):

- Capability that allows a protocol to distinguish between different classes of messages and assign priority levels.
- **Types of QoS:**
    - **Constant bit rate (CBR):** connection-oriented channel that provides a consistent data throughput for time-sensitive applications, such as voice and video applications.
    - **Variable bit rate (VBR):** connection-oriented channel best used for delay-insensitive applications because the data throughput flow in uneven.
    - **Unspecified bit rate (UBR):** connectionless channel the does not promise a specific data throughput rate.

- **Available bit rate (ABR):** connection-oriented channel, where customers are given the bandwidth that remains after a guaranteed service rate has been met.

- **QoS basic levels:**
  - **Best-effort service:** no guarantee of throughput, delay, or delivery.
  - **Differentiated service:** compared to best-effort service, traffic that is assigned this level has more bandwidth, shorted delay, and fewer dropped frames.
  - **Guaranteed service:** ensures specific data throughput at a guaranteed speed.

Traffic shaping: controlling network traffic to allow for optimization or the guarantee of certain performance levels.

SDLC (Synchronous Data Link Control):

- A protocol used in a dedicated, leased lines with permanent physical connections.
- Bit-oriented.
- Developed to enable mainframes to communicate with remote locations (originally IBM proprietary).
- Usually used in an environment that have primary systems that control secondary stations' communication.

HDLC (High-level Data Link Control):

- Bit-oriented.
- Used for serial device-to-device WAN communication (e.g. two routers communicating over WAN link).

PPP (Point-to-Point Protocol):

- Telecommunication devices commonly use PPP as their data link layer.
- It has:
  - Link Control Protocol (LCP): establishes, configures, and maintains the connection.
  - Network Control Protocols (NCPs): used for network layer protocol configuration and provides user authentication capabilities, through Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Extensible Authentication Protocol (EAP).

HSSI (High-Speed Serial Interface):

- Connect multiplexers and routers to high-speed communications services such as ATM and frame relay.
- It supports speed up to *52 Mbps*.
- Works as the physical layer.

Multiservice Access Technologies:

- Combine several types of communication categories (data, voice, and video) over one transmission line.
- Signaling System 7 (SS7) is used to control the PSTN phone call. When VoIP is used, it employees Session Initiation Protocol (SIP).

- SIP is an application layer protocol that ca work over TCP or UDP.
- **Jitter:** experience of lags in VoIP conversation, which means that packets holding the other person's voice message got queued somewhere within the network and are on their way.
- **Isochronous network:** contains the necessary protocols and devices that guarantee continuous bandwidth without interruption (e.g. good for time-sensitive applications).
- Components of VoIP: IP Telephony device, call-processing manager, voice system, and voice gateway.

H.323 Gateways:

- An H.323 environment features terminals, which can be telephones or computers with telephony software, gateways that connect this environment to the PTSN, etc.
- H.323 gateways connect different types of systems and devices and provide the necessary translation functionality.
- H.323 terminals are connected to these gateways, which in turn can be connected to the PSTN.

SIP:

- Two major components: User *Agent Client (UAC)* and *User Agent Server (UAS)*.
- UAC is the application that create the SIP requests for initiating a communication session.
- UAS is the SIP server, which is responsible for handling all routing and signaling involved in VoIP calls.
- Relies on a three-way-handshake process to initiate a session.
- How it works?
    - A starts be sending an **INVITE** packet to B.
    - Since A is unaware of B's location, the **INVITE** packet is sent to the SIP server, which looks up B's address in the SIP *registrar server*.
    - Once location of B has been determined, the **INVITE** packet is forwarded to him.
    - During this entire process the server keeps A updating by sending him **TRYING** packet.
    - Once packet reaches B, it starts ringing. B sends **RINGING** packet to A.
    - Once B answers the call, an **OK** packet is sent to A (through the server).
    - A now issues an **ACK** packet to begin the call setup.
    - RTP is used to to stream media (e.g. voice or video):
        - RTP is a session layer protocol.
        - End-to-end delivery service over the transport layer protocol UDP.
        - RTP Control Protocol (RTCP) is used with RTP and considered session layer also. It provides out-of-band statistics and control information to provide feedback on QoS levels.
    - Once communication is done, a **BYE** message is sent from the system terminating the call. The other system responds with an **OK** message.
- SIP architecture consists of three different types of servers:
    - **Proxy server:** relay packets within a network between the UACs and the UAS.

    - **Registrar server:** keeps a centralized records of the updated locations of all the users on the network.
    - **Redirect server:** allows SIP devices to retain their SIP identities despite changes in their geographic location.
- Intra-organizational routing enables SIP traffic to be routed within a VoIP network without being transmitted over the PSTN or external network.
- Skype uses a *peer-to-peer communication* model rather than the traditional client/server approach of VoIP systems.

IP Telephony issues:

- SIP-based signaling lack of encrypted call channels and authentication of control signals.
- Attackers can tap into the SIP server and client communication to sniff out login ID, passwords/PINs, and phone numbers.
- VoIP-PSTN gateways must be secure from intrusion to avoid toll fraud.
- Attackers can masquerade identities by redirecting SIP control packets from a caller to a forged destination.
- Attacker can impersonate a server and issue commands like **BYE**, **CHECKSYNC**, and **RESET**:
    - The **CHECKSYNC** command can be used to reboot VoIP terminal.
    - The **RESET** command causes the server to reset and reestablish the connection.
- **SPIT (Spam over Internet Telephony):** spamming the voicemail servers.

Dial-up Connections:

- Utilize existing telephone lines.
- A modem (modulator-demodulator) is added that modulates an outgoing digital signal into an analog signal that will be carried over an analog carrier, and demodulates the incoming analog signal into digital signals that can be processed by a computer.
- Most companies did not enforce access control through these modem connections. Thus, **war dialing** can be performed by attackers.
- Dial-up connection take place over PPP.

ISDN (Integrated Services Digital Network):

- Technology provided by telephone companies and ISPs.
- Enables data, voice, and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.
- It provides a point-to-point, circuit-switched medium.
- Can be used for LAN-to-LAN on demand connectivity, instead of the expensive dedicated link.
- If both communicating devices have the necessary equipment to utilize ISDN, this mean a higher bit rate can be achieved.
- Analog telecommunication signals use a full channel for communication, but ISN can break this channel into multiple channels to move various types of data, and provide full-duplex communication.
- ISDN provides two basic services:

- **Basic Rate Interface (BRI):**
  - 2 B channels that enables data to be transferred and 1 D channel that provides for call setup, connection management, error control, caller ID, etc.
  - Channel D is "out-of-band" because the control data is not mixed in with the user communication data.
  - Aimed for small office and home office.
  - Bandwidth available is 144 Kbps.
- **Primary Rate Interface (PRI):**
  - 23 B channels and 1 D channel.
  - Bandwidth is equivalent to T1 (1.544 Mbps).
  - ISDN is used as a backup in case the primary connection of the company goes down.
  - Companies can implement **dial-on-demand routing (DDR)**, which work over ISDN. DDR allows a company to send WAN data over its existing telephone lines and use the PSTN as a temporary type of WAN link.

- **Broadband ISND (BISDN):** Mainly used within telecommunications carrier backbones.

DSL (Digital Subscriber Line):

- 6 to 30 times higher bandwidth speeds than ISDN and analog technologies (**52 Mbps**).
- Limited to 2.5-miles radius of the DSL service provider's equipment.
- In DSL, low and high frequencies is used for data transmission, and not being filtered out by the service providers.
- **Types of DSL:**
  - **Symmetric DSL (SDSL):** data travels upstream and downstream at the same rate.
  - **Asymmetric DSL (ADSL):** data travels downstream faster than upstream.
  - **High-bit-rate DSL (HDSL):** provides T1 speed, and requires two twisted pairs of wires.
  - **Very High-Data-Rate DSL (VDSL):** it is a ADSL at much higher data rate (e.g. for HDTV, VoIP, etc.).
  - **Rate-Adaptive DSL (RADSL):** adjusts the transmission speed to match the quality and the length of the time.

Cable Modems:

- Provide high-speed access to the Internet through existing cable coaxial and fiber lines.
- The bandwidth is shared between users in a local area.
- Most cable provides comply with Data-Over-Cable Service Interface Specifications (DOCSIS), which allow for the addition of high-speed data transfer to an existing cable TV (CATV) system.

Always connected: DSL lines and cable modems are connected to the Internet and "live" all the time. This can cause security issues, as this always online is available for scanning, probing, hacking and attacking at any time.

VPN (Virtual Private Network): secure and private connection through an untrusted network.

PPTP (Point-to-Point Tunneling Protocol):

- For many years, the *de facto standard* for VPN software was PPTP.
- PPTP uses Generic Routing Encapsulation (GRE) and TCP to encapsulate PPP packets and extend a PPP connection through an IP network.
- **Limitations:** cannot support multiple connections over one VPN tunnel, which means that it can be used for system-to-system communication but not gateway-to-gateway connections.

L2TP (Layer 2 Tunneling Protocol):

- L2TP tunnels PPP traffic over various network types (IP, ATM, X.25, etc.). Thus, it is not restricted to IP networks as PPTP is.
- The line between your house and your ISP is a point-to-point telecommunication link. Point-to-point telecommunication devices do not understand IP, so your router has to encapsulate your traffic in a protocol that ISP's device will understand – PPP.

PPP provides *user* authentication through PAP, CHAP, or EAP-TLS, whereas IPSec provides *system* authentication.

IPSec (Internet Protocol Security):

- **IPSec protocols:**
  - Authentication Header (AH): provides data integrity, data-origin authentication, and protection from replay attacks.
  - Encapsulating Security Payload (ESP): provides confidentiality, data-origin authentication, and data integrity.
  - Internet Security Association and Key Management Protocol (ISAKMP): provides a framework for security association creation and key exchange.
  - Internet Key exchange (IKE): provides authentication keying material for use with ISAKMP).
- AH and ESP can be used separately or together in an IPSec VPN configuration.
- IPSec is usually used to protect gateway-to-gateway connections.
- **Transport adjacency** can be configured, which means that more than one security protocol (ESP and AH) is used in a VPN tunnel.
- **Iterated tunneling** can be configured, which means an IPSec tunnel is tunneled through another IPSec tunnel.
- Two modes:
  - **Tunnel mode:**
    - Encrypts IP header and payload.
    - Used for site-to-site VPN.
    - NAT traversal is supported.
  - **Transport mode:**

- Only payload is encrypted.
- Used for client-to-client VPN.
- NAT traversal is not supported.

Transport Layer Security (TLS) VPN:

- TLS works at the session later and used mainly to protect HTTP traffic and its capabilities are already embedded into most web browsers.
- TLS VPN is closer to the application layer, thus, it can provide more granular access control
- TLS VPN types:
  - **TLS Portal VPN:** user access single portal with standard TLS connection and from there, he can access other resources.
  - **TLS tunnel VPN:** user uses a web browser to securely access multiple network services, including applications and protocols that we not web-based. This commonly requires custom programming to allow the services to be accessible through a web-based connection.

PAP (Password Authentication Protocol):

- Used by remote users to authenticate over PPP connections.
- The username and password are sent over the network to the authentication server after a connection has been established via PPP.
- Credentials are sent in a cleartext. Thus, it is vulnerable to sniffing.
- Vulnerable to man-in-the-middle attacks.

CHAP (Challenge Handshake Authentication Protocol):

- It uses challenge/response mechanism.
- The user sends the authentication server a request to login, the sever respond back with a challenge (nonce). The challenge is encrypted with a predefined password (encryption key). The server uses the same password t decrypt the response.
- Not vulnerable to man-in-the-middle attacks, because it continues this challenge/response activity throughout the connection.

EAP (Extensible Authentication Protocol):

- EAP is not a specific authentication protocol as are PAP and CHAP. Instead, it provides a framework to extends the authentication possibilities from the norm (PAP and CHAP) to other methods, such as OTP, token cards, biometrics, Kerberos, digital certificate, and future mechanisms.

Protocol	Description
Lightweight EAP (LEAP)	Wireless LAN authentication method developed by Cisco Systems
EAP-TLS	Digital certificate–based authentication
EAP-MD5	Weak system authentication based upon hash values
EAP-PSK	Provides mutual authentication and session key derivation using a preshared key
EAP-TTLS	Extends TLS functionality
EAP-IKE2	Provides mutual authentication and session key establishment using asymmetric or symmetric keys or passwords
PEAPv0/EAP-MSCHAPv2	Similar in design to EAP-TTLS but only requires a server-side digital certificate
PEAPv1/EAP-GTC	Cisco variant based on Generic Token Card (GTC) authentication
EAP-FAST	Cisco-proprietary replacement for LEAP based on Flexible Authentication via Secure Tunneling (FAST)
EAP-SIM	For Global System for Mobile Communications (GSM), based on Subscriber Identity Module (SIM), a variant of PEAP for GSM
EAP-AKA	For Universal Mobile Telecommunication System (UMTS) Subscriber Identity Module (USIM) and provides Authentication and Key Agreement (AKA)
EAP-GSS	Based on Generic Security Service (GSS), uses Kerberos

Table 4-15 EAP Variants

The higher the frequency, the more data the signal can carry, but the more susceptible the signal is to atmospheric interference.

Ethernet employ the **CSMA/CD**, while Wireless LAN employ **CSMA/CA**.

Spread Spectrum:

- The sender spreads its data across the frequencies over which it has permission to communicate. This allows for more effective use of the available bandwidth, because the sending system can use more than one frequency at at time.
- **FHSS (Frequency Hopping Spread Spectrum):**
  - Takes the total amount of bandwidth (spectrum) and splits it into smaller sub-channels.
  - The FHSS algorithm determines the individual frequencies that will be used and in what order, and this is referred to as the sender and receiver's *hop sequence*.
  - Difficult for eavesdroppers to listen. But in today's WLAN devices, the hopping sequence is known and does not provide any security.
  - If the signal is corrupted, it must be re-sent.
- **DSSS (Direct Sequence Spread Spectrum):**

- Apply sub-bites to a message. The sub-bites are used by the sending system to generate a different format of the data. The receiving end uses these sub-bits to reassemble the signal into the original data format.
- These sub-bits called *chips*. The sequence of how the sub-bits are applied is called the *chipping code* (it is sometimes called a *pseudo-noise sequence*).
- When message is combined with the chip, the signal appears as random noise to anyone does not know the chipping sequence.
- Synchronization between both parties is required.
- It does provide error recovery instructions.

- **FHSS vs. DSSS:**
  - FHSS uses only a portion of the total bandwidth available at any one time. While, DSSS uses all of the available bandwidth continuously.
  - DSSS spreads the signals over a wider frequency band, whereas FHSS uses a narrow band.
  - DSSS sends data across all frequencies at once, it has a higher data throughput than FHSS.

OFDM (Orthogonal Frequency-Division Multiplexing):

- The modulated signals are orthogonal (perpendicular) and do not interfere with each other.
- Uses a composite of narrow channel bands.
- It is officially a multiplexing technology and not a spread spectrum technology.
- Used for wideband digital communication (e.g. digital TV, audio broadcasting, DSL broadband Internet access, wireless networks, 4G mobile communications).

Infrastructure WLAN: when AP is used to connect wireless and wired networks.

Standalone mode: when there is just one AP and it is not connected to a wired network.

Ad hoc WLAN: has no APs. The wireless devices communicate with each other through their wireless NICs instead of going through a centralized device (peer-to-peer operation mode).

A **channel** is a certain frequency within a given frequency band.

When wireless devices work in infrastructure mode, the AP and the wireless clients form a **Basic Service Set (BSS).** This group is assigned a name, which is the SSID value. **SSID** is a Service Set ID.

Gap in the WAP: wireless device encrypts packets using WTLS and sends it to WAP. WAP performs translation from WTLS to TLS. Here WAP is decrypts the WLTS protected packets and encrypts it using TLS standard.

Evolution of WLAN Security:

- **IEEE 802.11 (WEP):**
  - It uses **Wired Equivalent Privacy (WEP)**.
  - WEP uses RC4 algorithm, which is a stream-symmetric cipher.
  - **The 3 core deficiencies with WEP:**
    1. Use of static encryption keys
    2. Ineffective use of IV: In most WEP implementation, the same IV values are used over and over again.
    3. Lack of packet integrity assurance: An attacker can actually change date within the wireless packet by flipping specific bits and altering the ICV.
  - The key and IV value are inserted into the RC4 algorithm to generate key stream. The values of the key stream are XORed with the binary values of the individual packets.
  - The wireless device using this protocol can authenticate to the AP in two main ways: *open system authentication (OSA)* and *shared key authentication (SKA)*.
  - **OSA:**
    - Does not require the wireless device to prove to the AP it has a specific cryptographic key to allow for authentication purposes.
    - The wireless device needs to provide only the correct SSID value.
    - All transactions are in cleartext.
  - **SKA:**
    - The AP sends a random value to the wireless device. The device encrypts it with its cryptographic key and returns it. The AP decrypts and extracts the response.
  - AirSnort and WEPCrack are tools to easily crack WEP.
- **IEEE 802.11i (WPA2):**
  - **WiFi Protected Access II (WPA2)**
  - Temporal Key Integrity Protocol (TKIP):
    - Backward-compatible. The goal was to increase the strength of WEP or replace it fully without the need for hardware replacement.
    - Works with WEP by feeding it keying materials, which is data to be used for generating new dynamic keys.
    - It generates a new key for every frame that is transmitted.
    - It provides a sequence counter to protect against replay attacks.
    - The protocol increases the length of IV and ensure every frame has a different IV value.
    - TKIP deals with integrity issues by using MIC instead of ICV.
  - The use of 802.1X provides access control by restricting the network access until full authentication and authorization have been completed. It also provides an authentication framework that allows for different EAP modules to be plugged in (using EAP allows for mutual authentication with flexibility: passwords, tokens, OTP, certificates, smart cards, Kerberos).

- The full WPA2 has a major advantage over WPA by providing encryption protection with the use of the AES algorithm in counter mode with CBC-MAC (CCM).

- **IEEE 802.1X:**
  - Port-based network access control.
  - It is a network access protocol that can be implemented on both wired and wireless networks.
  - The 3 main entities in this framework are:
    - Supplicant (wireless device)
    - Authenticator (AP)
    - Authentication server (e.g. RADIUS server).
  - The wireless device cannot send or receive HTTP, DHCP, SMTP, or any other type of traffic until the user is properly authorized.
  - Disadvantage of the original 802.11 is that mutual authentication is not possible (e.g. A rouge AP can be set up to capture user's credentials).

Wireless Standards:

Standard	Speed	Frequency Range	Notes
802.11	1-2 Mbps	2.4GHz (unlicensed range by FCC, dirty and crowded)	
802.11b	11 Mbps	2.4 GHz	First extension as 802.11a was not released due to complexity involved. It uses DSSS Backward-compatible with 802.11.
802.11a	54 Mbps	5 GHz (some countries have not allocated this band for use of WLAN transmissions).	It uses OFDM Not backward compatible with 802.11 or 802.11b.
802.11e	-	-	Provides QoS and support for multimedia traffic (time-sensitive applications).
802.11f	-	-	Conveying of required information between different APs during roaming
802.11g	54 Mbps	2.5 GHz	A speed extension for 802.11b.
802.11h	54 Mbps	5 GHz	Builds upon the 802.11a specs to meet the requirements of European wireless so products working on 5 GHz can be implemented there.

802.11j	-	-	It aims on bringing together many of the different standards and streamlining their development to allow for better interoperability across borders.
802.11n	100 Mbps	5 GHz	Uses MIMO to increase the throughput.
802.11ac	1.3 Gbps	5 GHz	Extension of 802.11n Backward-compatible with 802.11a, 802.11b, 802.11g, 802.11n It supports *beamforming*, which is the shaping of radio signals to improve their performance in specific directions.

- **802.16 (MAN wireless standard):** It is referred to as *broadband wireless access* or *WiMAX*.
- **802.15.4 (wireless personal area network -WPAN):**
  - A computer communicating with a wireless keyboard.
  - It operates in the 2.4 GHz band.
  - Devices that conform to this standard typically low-cost, low-bandwidth and ubiquitous.
- **Bluetooth – IEEE 802.15.1:**
  - 1-3 Mbps.
  - 2.4 GHz
  - Works approximately within 1, 10, 100 meters.
  - **Bluejacking:** Someone sends an unsolicited message to a device that is Bluetooth-enabled. The hacker is trying to send someone else their business card, which will be added to the victim's contact list in their address boos. **Countermeasure:** put the device into non-discoverable mode.
  - **Bluesnarfing:** Unauthorized access from a wireless device through a Bluetooth connection. This allows access to a calendar, contact list, emails, text messages, photos and videos.

Best Practices for Securing WLANs

There is no silver bullet to protect any of our devices or networks. That being said, there are a number of things we can do that will increase the cost of the attack for the adversary. Some of the best practices pertaining to WLAN implementations are as follows:

- Change the default SSID. Each AP comes with a preconfigured default SSID value.
- Implement WPA2 and 802.1X to provide centralized user authentication (e.g., RADIUS, Kerberos). Before users can access the network, require them to authenticate.
- Use separate VLANs for each class of users, just as you would on a wired LAN.
- If you must support unauthenticated users (e.g., visitors), ensure they are connected to an untrusted VLAN that remains outside your network's perimeter.
- Deploy a wireless intrusion detection system (WIDS).
- Physically put the AP at the center of the building. The AP has a specific zone of coverage it can provide.
- Logically put the AP in a DMZ with a firewall between the DMZ and internal network. Allow the firewall to investigate the traffic before it gets to the wired network.
- Implement VPN for wireless devices to use. This adds another layer of protection for data being transmitted.
- Configure the AP to allow only known MAC addresses into the network. Allow only known devices to authenticate. But remember that these MAC addresses are sent in cleartext, so an attacker could capture them and masquerade himself as an authenticated device.
- Carry out penetration tests on the WLAN. Use the tools described in this section to identify APs and attempt to break the current encryption scheme being used.

Satellites:

- For two locations to communicate via satellite links, they must be within the satellite's line of sight and footprint (area covered by the satellite).
- On top of building, we see antennas contains one or more microwave receivers, depending upon how many satellites it is accepting data from.
- It commonly provides broadband transmission (e.g. TV, PC Internet access,).
- One way for TV data, and two-ways transmission for Internet connectivity.
- Low Earth Orbit: there is not as much distance between the ground stations and the satellites as in other types of satellites (e.g. smaller receivers can be used).
- 2 main microwave wireless technologies are:
  - Satellite (ground to orbiter to ground)
  - Terrestrial (ground to ground)
- **Very small aperture terminal (VSAT):** links a remote site to the Internet through a satellite gateway facility run by a service provider (cost are affordable now).

Mobile Wireless Communication:

- Mobile device is a device that can send voice and data over wireless radio links. It connects to a cellular network, which is connected to the PSTN.
- Radio stations use broadcast networks, which provide **one-way transmission**.
- A cellular network distributes radio signals over dedicated areas, called **cells**.
- Each cell has at least one fixed-location transceiver (base station) and is joined to other cells to provide connections over large geographic areas.
- Individual cells can use the same frequency range, as long as they are not right next to each other.
- Many multiple access technologies highlighted below.

Frequency division multiple access (FDMA) – 1G:

- The available frequency range is divided into sub-bands (channels), and one channel is assigned to each subscriber (cell phone).
- Multiple users can share the frequency range without the risk of interference between simultaneous calls.

Time division multiple access (TDMA) – 2G (GSM):

- Takes the radio-frequency spectrum channels and dividing them into time slots.
- Increase speeds and service quality.
- Requires that each slot's start and end time are known to both the source and destination.

Code division multiple access (CDMA) – 3G:

- Assigns a unique code to each voice call or data transmission to uniquely identify it from all other transmissions sent over the cellular networks.
- Calls are spread throughout the entire radio-frequency spectrum band.
- Permits every user of the network to simultaneously use every channel in the network.

Orthogonal frequency division multiple access (OFDMA) – 4G:

- Derived from the combination of FDMA and TDMA.
- Each of the channels is subdivided into a set of closely spaced orthogonal frequencies with narrow bandwidth (sub-channels).

Hacking mobile phones:

- 2G networks lack the ability to authenticate towers to phones (e.g. attacker can implement a rouge tower with more power than the nearby legitimate ones).
- Even though 3G and 4G corrected this, but it is possible to force most 3G and 4G phones to switch down to 2G mode by jamming 3G and 4G towers.
- Devices designed to perform this type of attack are called **International Mobile Subscriber Identity (IMSI)** catchers.

1G:

- Analog services
- Voice service only

2G:

- Primarily voice, some low-speed data (circuit switched).
- Phones were smaller in size.
- Added functionality of email, paging and caller ID.

2.5G:

- Higher bandwidth than 2G.
- "Always on" technology for email and pages.

3G:

- Integration of voice and data.
- Packet-switched technology.

3.5G (3GPP):

- Higher data rates.
- Use of OFDMA technology.
- Has number of new or enhanced technologies: EDGE, HSPDA, CDMA2000, WiMAX.

4G:

- Based on an all-IP packet-switched network (LTE – Long Term Evolution).
- Data exchange at 100Mbps – 1Gbps.

Link encryption:

- Encrypts all the data along a specific communication path.
- Not only is the user information encrypted, but the headers, trailers, addresses, and routing data that are part of the packets are also encrypted.
- The only traffic not encrypted in this technology is the data link control messaging information.
- Packets must be decrypted at each hop so the router knows where to send the packet next.
- It works at lower layer, so user do not need to do anything to initiate it.
- Provides protection against packet sniffers and eavesdroppers.
- Sometimes called *online encryption*. Also referred to as *traffic-flow security*.
- Disadvantages:
  - Key distribution and management (key change, key update).
  - More points of vulnerability (each hop decrypts the packet).

End-to-end encryption:

- Headers, trailers, addresses and routing information are not encrypted.
- Flexible to the user in choosing what gets encrypted and how.
- Higher granularity of functionality as each application or user can choose specific configuration.
- Each hop device on the network does not need to have a key to decrypt each packet.

- **Disadvantages:** headers, addresses, and routing information are not encrypted, and therefore not protected.

Multipurpose Internet Mail Extensions (MIME):

- Technical specifications indicating how multimedia data and email binary attachments are to be transferred.
- If a message or document contains a binary attachment, MIME dictates how that portion of the message should be handled.
- Secure MIME (S/MIME) is a standard for encrypting and digitally signing email, with its attachments, and for providing secure data transmissions.
- S/MIME follows the Public Key Cryptography Standards (PKCS).
- S/MIME provides confidentiality through encryption, integrity through hashing, authentication through the use of X.509 certificates, and nonrepudiation through cryptographically signed digests.

Pretty Good Privacy (PGP):

- A freeware email security program.
- It can use RSA public key encryption for key management and use IDEA algorithm for bulk encryption of data.
- PGP can provide confidentiality by using the IDEA algorithm, integrity by using MD5 hashing, authentication by using public key certificates, and nonrepudiation by using cryptographically signed messages.
- PGP uses its own type of digital certificates rather than what is used in PKI.
- User's private key is generated and encrypted when the application asks the user to randomly type on her keyboard for a specific amount of time.
- Instead of using passwords, PGP uses passphrases. The passphrase is used to encrypt the user's private key that is stored on her hard drive.
- PGP relies on "web of trust" and do not use a hierarchy of CAs: each user generates and distributes his public key, and users sign each other's public keys, which creates a community of users who trust each other.
- Each user keeps in a file, called ***key ring***, which includes a collection of public keys he has received from other users. Each key in that ring has a parameter that indicates the level of trust assigned to that user and the validity of that particular key.

Internet security:

- The Web is the collection of HTTP servers that holds and processes websites we see.
- Web browsers enable users to read pages by enabling them to request and accept web pages via HTTP.
- User's browsers convert the language (HTML, DHTML, and XML) into a format that can be viewed on the monitor.
- HTTP is a stateless protocol, which means the client and web server make and break the connection for each operation. The web server never "remembers" the users that ask for different web pages.

- **HTTP Secure (HTTPS)** is HTTP running over Secure Socket Layer (SSL) or Transport Layer Security (TLS). Nowadays, SSL considered insecure and obsolete and TLS should be used in its place.
- **S-HTTP** protects individual message between two computers instead of all communications.
- **Secure Socket Layer (SSL):**
  - Uses public key encryption and provides data encryption, server authentication, message integrity, and optional client authentication.
  - The web server will start the necessary tasks and invoke SSL and protect this type of communication.
  - The server sends a message back to the client, indicating a secure session should be established, and the client in response sends its security parameters. This is the handshaking phase.
  - The server authenticates to the client by sending over its certificate. If mutual authentication is required, the client sends back its certificate.
  - The client generates a session key and encrypts it with the server's public key, so they both use this symmetric key for encryption.
  - SSL session keeps open until one of the parties ends it (usually a client sends a FIN packet).
  - SSL requires an SSL-enables server and browser.
  - SSL lies beneath the application layer and above the network layer (so SSL is not limited to specific application protocols). *For the purpose of CISSP exam, SSL protocol works at the transport layer*.
  - The final version of SSL was 3.0 (considered insecure today).
- **Transport Layer Security (TLS):**
  - TLS is the open community and standardized version of SSL.
  - TLS is currently in version 1.2.
  - Passing Oracle On Downgraded Legacy Encryption (POODLE) attack was the death of SSL and demonstrated that TLS was superior security-wise. The key to POODLE attack was to force SSL to downgrade its security.
- **Cookies:**
  - Text files that a browser maintains on a user's hard drive or memory segments.
  - In most cases, cookies contain sensitive information should stay in the memory and not to be stored in the hard drive.
  - Some 3rd parties are used to limit the type of cookies downloaded, hides user's identity as he travels from one site to another.
- **Secure Shell (SSH):**
  - A type of tunneling mechanism that provides terminal-like access to remote computers.
  - SSH provides authentication and secure transmission over vulnerable channels like the Internet.
  - SSH should be used instead of Telnet, FTP, rlogin, rexec, or rsh.
  - SSH is a program and a set of protocols.

- Two computers go through a handshaking process and exchange (via Diffie-Hellman) a session key.

Network Attacks:

- **Denial of service (DoS):** compromise to the availability.
- **Malformed packets:**
  - *Ping of Death*. This attack sent a single ICMP Echo Request to a computer, which resulted in the "death" of its network stack until it was restarted. This attack exploited the fact that many early networking stacks did not enforce the maximum length of ICMP packet, which is 65,536 bytes.
  - The single most important countermeasure here is to keep your system patched.
- **Flooding:**
  - Overwhelming the target computer with packets until it is unable to process legitimate user requests (e.g. *SYN flooding*).
- **Distributed denial of service:**
  - A network of compromised computers. Each of these computers are called a ***bot*** or a ***zombie***, and the network they form called a ***botnet***.
  - A countermeasure is to leverage a content distribution network (CDN).
  - Most modern switches and routers have rate-limiting features that can throttle or block the traffic from particularly noisy sources such as these attackers.
  - If the attack happens to be a SYN flood, you can configure your servers to use a technique known as delayed binding in which the half-open connection is not allowed to tie up a socket until the three-way handshake is completed.
- **DNS hijacking:**
  - an attack that forces the victim to use a malicious DNS server instead of the legitimate one.
  - **Host based:** adversary changes the IP settings of the victim's computer to point to the rouge DNS server.
  - **Network based:** adversary in a network use a technique such as ARP table cache poisoning to redirect DNS traffic to his own server. **Countermeasure:** NIDS.
  - **Server based:** if DNS server is not configured properly, the attacker can tell the server that is own rouge server is the authorities one for whatever domain he wants to hijack. **Countermeasure:** DNSSEC.
- **Drive-by download:**
  - Occurs when a user visits a website that is hosting malicious code and automatically gets infected.
  - This type of attack exploits vulnerabilities in the user's web browsers (e.g. a browser plug-in such as video player).

Loki attack:

- Loki is a client/server program used by attacker to create backdoor.
- The attacker installs the server potion on the compromised machine and communicates with it by embedding data into ICMP packets.

HAIPE (High Assurance Internet Protocol Encryptor):

- A type 1 encryption device developed by U.S. NSA.
- Based on IPSec with additional enhancements.
- HAIPE is typically a secure gateway that allows two enclaves to exchange data overran untrusted network.

CHAPTER 5: Identity and Access Management

Subject is an active entity that requests access to an object or the data within an object (e.g. user, program, process).

Object is a passive entity that contains information or needed functionality (e.g. computer, database, file, directory, field or table in a database).

Steps in order: Identification – Authentication – Authorization – Accountability

Race condition: an attacker can force the authorization step to take place before the authentication step.

Authentication usually involves two-step process: entering public information (username, employee number), and them entering private information (password, PIN).

Authentication factors:

- *Something you know* (authentication by knowledge): password, PIN, mother's name
- *Something you have* (authentication by ownership): key, swipe card, access card, badge
- *Something you are* (authentication by characteristic): biometrics

Strong authentication (multi-factor authentication) contains ***2 or all*** of these three methods.

Three-factor authentication is also possible.

Creating/issuing secure identities must have 3 aspects:

- **Uniqueness:** every use must have a unique ID for accountability.
- **Non-descriptive:** neither piece of the credential set should indicate the propose of that account.
- **Issuance:** elements that have been provided by another authority as a means of proving identity (e.g. ID cards).

System-based authentication: computers and devices can be identified, authenticated, monitored, and controlled based upon their hardware addresses and or IP addresses. (e.g. NAC technology authenticates systems before they are allowed to access to the network).

Directories:

- Most directories follow a hierarchical database format, based on the X.500 standard, and a type of protocol (e.g. Lightweight Directory Access Protocol, **LDAP**).

- Applications can request information about a particular user by making an LDAP request to the directory.
- ***Directory service*** allows an administrator to configure and manage how identification, authentication, authorization, and access control for individual systems.
- Directory service keeps everything organized by using *namespaces*. Databases based on X.500 that are accessed by LDAP uses ***distinguished names (DNs)*** to each object.
- ***DN*** is a collection of attributes (common name, domain components).
- Many **legacy** devices and applications **cannot be managed by the directory service**.
- **Meta-directory** gathers the necessary information from multiple sources and stores it on one central directory. It synchronizes itself with all of the identify stores periodically.
- **Virtual directory** does not have the information stored physically, but points to where the actual data resides.

Web access management (WAM):

- A software controls what users can access using a web browser to interact with web-based enterprise assets.
- It is the main gateway between users and the corporate web-based resources.
- Usually provides a single sign-on (SSO) capability.

Cookies can be in a format stored on the user's hard drive (**permeant**), or only held in memory (**session**).

Password management:

- **Password synchronization:** reduce the complexity of keeping up with multiple passwords.
- **Self-service password reset:** reduces help-desk calls.
- **Assisted password reset:** reduces the resolution process for password issues for the help desk (may include other types of authentication mechanisms: biometrics or tokens).

SSO is different than password synchronization:

- In SSO, a user doesn't need to enter his credentials on each system, but the SSO software will provide the system with the credentials.
- SSO is may be seen as a bottleneck and single point of failure.

Usually users' data is being pulled from ***authoritative source*** (e.g. HR database) into a directory.

Authoritative system of record (ASOR) is a hierarchical tree-like structure system that tracks subjects and their authorization chains.

The centralized directory can be called an ***identity repository***.

User provisioning refers to the creation, maintenance, and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications, in response to business process.

Biometrics:

- Analyzes a unique personal attribute or behavior.
- Very sophisticated technology and expensive.
- **Challenges:** user acceptance, enrollment timeframe, throughput.
- 2 different categories:
  - Physiological (e.g. fingerprints) – ***What you are***
  - Behavioral (e.g. signature dynamics) – ***What you do***
- Type of errors:
  - **Type I error (false rejection rate FRR):** rejects authorized individual
  - **Type II error (false acceptance rate FAR):** accepts impostors who should be rejected
- **Crossover error rate (CER) (Equal error rate EER)** is a percentage that represents the point at which FRR equals FAR (CER of 3 is more accurate that CER 4).

Fingerprint:

- Detailed characteristics of fingerprint called **minutiae**.
- This technology extracts specific features from the fingerprint and stores it in the hard drive to allow smaller space and to allow quicker database lookup.

Palm scan can include fingerprints of each finger in addition to a wealth of other information.

Hand geometry relies on the shape of a person's hand.

Retina scan:

- Scans the blood-vessel pattern of the retina on the backside of the eyeball.
- A camera is used to project a beam inside the eye and capture the pattern.
- Involves number of privacy issues (e.g. collected information can be used in the diagnosis of medical conditions).

Iris scan is one of the most accurate biometric technologies. Iris remains constant through adulthood.

Signature dynamics relies on the physical motions performed when someone is signing a document, which create electrical signals. It provides more information than a static signature.

Keystroke dynamics captures the speed and motions of keyboard stokes.

Voice print:

- It records words from a user during enrollment process.
- During authentication, the system jumbles the words in different sequence to overcome an attacker replays a recorded audio file.

Facial scan scans the face and geometry of the face.
Hand topography:

- A camera snaps wide-view picture of the hand from different view and angle than that of systems that target hand geometry.
- Collected attributes are not unique enough, so it is commonly used in conjunction with hand geometry.

If an attacker is looking to get a user's password, he'll try different techniques:

- **Electronic monitoring:** sniffing packets (e.g. replay attack).
- **Access the password file:** password file usually located in authentication server.
- **Brute-force attacks**
- **Dictionary attacks**
- **Social engineering**
- **Rainbow table**

Password checkers (called *password cracker* by *hackers*) are tools that perform dictionary and/or brute-force attacks to detect the weak password.

In **Windows**, passwords are located in **SAM database**.

In **Linux**, passwords are located in a file called "**shadow**", which store hash values of passwords.

Salts are random values added to the encryption process to add more complexity and randomness.

Password aging is used to set expiration date for passwords. Also the system can keep history of most recently used passwords to prevent users from using them.

Cognitive password:

- It is a fact or opinion-based information used to verify an individual's identity. A user is enrolled by answering several questions based on her life experience (e.g. first person he kissed, name of friend in 8th grade).
- Best for services that are not used in daily basis because it takes longer that other authentication techniques.

One-time password:

- A dynamically generated password.
- **2 types:**
    - **Synchronous token device:**
        - The token device synchronizes with the authentication server by using time or a counter.

        - ***If it is a time-based***, both the token device and the server much hold the same time in their internal clocks.
        - ***If it is a counter-based (a.k.a event-based)***, the user needs to create an OPT by pushing a button on the token device. This let authentication server to advance to the next counter value.
        - The server and the token device must share the same secret base key.
    - **Asynchronous token device:**
        - A challenge/response scheme to authenticate the user.
        - The server sends a challenge (random value called *nonce*).
        - The user enters the nonce into the token device, which encrypts it and returns a value the user uses as OTP.
    - Not vulnerable to electronic eavesdropping, sniffing, or password guessing.
    - If OTP is generated in software, it called **soft token**.
- implemented in 3 formats:
    - Dedicated physical device with a small screen that displays the OTP.
    - Smartphone application
    - A service that sends an SMS message.

SecureID:

- A well-known time-based token from RSA Security Inc.
- One version of the product generates the OPT by using a mathematical function on the time, date and ID of the token card. Another version of the product requires a PIN to be entered into the token device.

Cryptographic key can be used to prove one's identity by using a private key to generate a digital signature.

Passphrase:

- A sequence of characters that is longer than a password.
- The user enters the passphrase into the application, and the application transforms the value into ***virtual password.***
- More secure than password because it is longer, thus, harder to guess.
- The user more likely to remember a passphrase than a password.

Memory cards holds information but cannot process information. It contains authentication information (e.g. swipe card, ATM card).

Smart cards can hold and process information:

- ***Contact smart card:*** has a gold seal on the face of the card and needs to be fully inserted into the reader. This will supply power and data I/O to the chip.
- ***Contactless smart card:*** has an antenna wire that surrounds the perimeter of the card. When the card comes within an electromagnetic field of the reader, the antenna generates enough energy to power the internal chip.

2 types of contactless smart cards are available:

- **Hybrid:** has two chips, with the capability of utilizing both contact and contactless formats.
- **Combi:** has one microprocessor chip that can communicate to contact or contactless readers.

Contactless smart cards have extra cost for readers and overhead of card generation.

Smart card attacks:

- **Fault-generation:** attackers tries to introduce computational errors into the smart cards (e.g. changing input voltage, clock rate, temperature fluctuations).
- **Side-channel:** differential power analysis, electromagnetic analysis, timing.
- **Software attacks:** input instructions into the card that allow the attacker to extract account information.
- **Microprobing:** uses needleless and ultrasonic vibration to remove the outer protective material on the card's circuits. Then, manipulate data by directly tapping into the card's ROM chip.

ISO/IEC 14443 smart card standard.

RFID:

- An electronic tag that has an integrated circuit for storing and processing data.
- **A common security issue** that that data can be captured as it moves from the tag to the reader.

Authorization creep is when an employee is working in a company for a long time and moves from one department to another and get assigned more and more access rights and permissions.

Kerberos:

- Works in a client/server model.
- Open protocol (vendors can manipulate it).
- Based on symmetric key cryptography.
- Example of an SSO system for distributed environment (de-facto for heterogeneous networks).
- Provides end-to-end security.
- **Key Distribution Center (KDC):**
  - Holds all users' and services' secret keys.
  - Provides an **authentication service (AS)**.
  - Offers key distribution functionality.
  - Provides security services to *principals* (e.g. users, applications, network services).
  - Shares secret key for each principal.

- **Ticket granting service** on the KDC generates **ticket** and give it to the principal when he needs to authenticate to another principal (e.g. print server).
- **Realms** are used to allow an administrator to logically group resources and users.

- **How does it work?**
  - Username of user sends to AS within KDC.
  - KDC sends TGT encrypted with user's symmetric key.
  - User then decrypts the TGT using his password and access his machine.
  - When user wants to access print server, he sends his TGT to TGS within KDC.
  - TGS creates another ticket to user. It contains a 2 instances of the session key, once encrypted with the user's key and the other with the print server's key. It also contains an *authenticator* (user ID, IP address, sequence number, timestamp).
  - User sends the generated ticket to the print server, which decrypts the session key.
  - **Timestamp** is used to fight **against replay attack**.
- **Weaknesses:**
  - KDC can be single point of failure.
  - KDC must be able to handle the number of requests.
  - Secret keys are temporarily stored on the users' workstations.
  - Session keys are decrypted and resides on the users' workstations.
  - Vulnerable to password guessing (don't know if dictionary attack is taking place).
  - Needs all client and server clocks to be synchronized.

SEASME extends Kerberos and offers symmetric and asymmetric keys for encryption and uses Privileged Attribute Certificates (PACs) instead of tickets.

Security domains:

- Set of resources available to a subject.
- Network administrator can put similar users in same domain as they use the same resources.
- Different domains are separated by logical boundaries (e.g. firewalls with ACL, directory services making access decisions, ACL on objects).
- Subjects can access resources in domains of equal or lower trust levels.
- Domain can contain network devices, users, processes.

Single Sign-On technologies:

- **Kerberos**
- **Security domains**
- **Directory services (provides SSO):** LSAP, NetIQ eDirectory, Microsoft Active Directory.
- **Thin clients (provides SSO):** a diskless computer than cannot do anything until it authenticates to a centralized server to get its OS, profile and functionality.

Federated identity:

- A portable identity, and its associated entitlements, that be used across business boundaries.
- Doesn't need to synchronize or consolidate directory information.

Digital identity:

- A collection of **attributes** (user, department, role, shift time, clearance), **entitlement** (resources available, authoritative rights), **traits** (biometrics, height, sex).

Web portal:

- A part of a website that act as a point of access to information.
- Presents information from diverse resources in a unified manner.
- Made up of ***portlets***, which are pluggable user-interface software components that present information from other system.

XML is a universal and foundational standard that provides a structure for other independent markup languages to be built from and still allow for interoperability.

Service provisioning markup language (SPML):

- Allows for the exchange of provisioning data between applications, which could reside in one organization or many.
- Allows for automation of user management (account creation, amendments, revocation) and access entitlement configuration.
- Made up of 3 main entities:
  - **Requesting Authority (RA):** requests account creation or changes to an existing account.
  - **Provisioning Service Provider (PSP):** the software that responds to the account requests.
  - **Provisioning Service Target (PST):** carries out the provisioning activities on the requested system).

Security assertion markup language (SAML):

- Allows the exchange of authentication and authorization data to be shared between security domains (e.g. Oracle ERP is *service provider*, AD is *identity provider*).
- Transmission of SAML data can take place over different protocol types (common one is **Simple Object Access Protocol SOAP**). **SOAP** is a specification that outlines how information pertaining to web services is exchanges in a structured manner.
- HTTP encapsulates SOAP. SOAL encapsulates SAML.

Extensible access control markup language (XACML):

- Used to express security policies and access rights to assets provided through web services and other enterprise applications.
- Used a Subject element (requesting entity), a Resource element (requested entity), and an Action element (type of access).

OpenID:

- open standard for user authentication by 3rd parties.
- Similar to SAML, but information is handled by 3rd party and not user's organization.
- It defines 3 roles:
  - **End user:** user who wants to be authenticated.
  - **Resource party:** server that owns the resource required by the user
  - **OpenID provider:** system that an end user already has an account on.

OAuth:

- Open standard for authorization (not authentication) to 3rd parties.
- Authorizes a website to use something you control at a different website.

Identity as a service (IDaaS): A type of SaaS that is normally configured to provide SSO, federated IdM, and password management services.

Access control models:

- **Discretionary access control (DAC):**
  - enables the owner of the resource to specify which subjects can access the resource (based on the discretion of owner).
  - Most commonly implemented through ACL.
  - Change permission (read, write, execute, delete) but not change (ACL, owner).
  - Full Control permission allows changing ACL and owner of a resource.
- **Mandatory access control (MAC):**
  - In most systems based on MAC model, user cannot install software, etc. User only uses the system for specific purposes (e.g. used by government-oriented agencies).
  - Users are given a security clearance and data is classified in the same way.
  - ***Security labels*** (also called *sensitivity label*) are attached to all objects:
    - **Classifications:** one level more trusted than another.
    - **Categories (enforces need-to-know):** e.g. department, project.
  - Organization must purchase OS that work on MAC model (e.g. SE Linux).
  - Limited functionality to the user and not user friendly.
  - Requires a lot of administrative overhead and very expensive.
  - Considered ***nondiscretionary*** access control model.
  - **Software guard** is a front-end product that allows interconnectivity between systems working at different security levels.
  - **Hardware guard** is a system with 2 NICs connecting the two systems that need to communicate with one another.
- **Role-based access control (RBAC):**

- Centrally administered set of controls to determine how subjects and objects interact.
- Access to resources based on the role the user holds.
- Best model for organization with high employee turnover.
- RBAC can be managed in the following ways:
  - **Non-RBAC:** users mapped directly to applications and no roles are used.
  - **Limited RBAC:** users mapped to multiple roles and mapped directly to other types of applications that do not have role-based functionality.
  - **Hybrid RBAC:** users mapped to multiapplication roles with only selected rights assigned to those roles.
  - **Full FBAC:** users mapped to enterprise roles.
- **Core RBAC:**
  - Integrated in every RBAC implementations because it is the foundation of the model.
  - RBAC can be configured to include time of day, location of role, day of week to make access decisions.
- **Hierarchical RBAC:**
  - The component allows an administrator to map the RBAC model to the organizational structures.
  - 2 types:
    - **Limited hierarchies:** only one level of hierarchy is allowed (Role 1 inherits from Rom 2 and no other role).
    - **General hierarchies:** allows for many level of hierarchies (Role 1 inherits Role 2's and Role 3's permissions).
  - Different separation of duties are provided under this model:
    - **Static separation of Duty (SSD) Relations through RBAC:** user cannot be a member of both the Cashier and Accounts groups.
    - **Dynamic separation of Duty (DSD) Relations through RBAC:** constraining combination of privileges that van be activated in one session (user cannot be in both the Cahier and Cashier Supervisor roles at the same time, but user can be a member of both).
- **Privacy-aware RBAC** (e.g. manager can access employee details, but don't see his social security number).
- RBAC can be used in combination with DAC and MAC systems.

- **Rule-based access control (RB-RBAC):**
  - uses specific rules that indicates what can and cannot happen between a subject and object (e.g. If X then Y).
  - Built on top of traditional RBAC.

Constrained user interfaces:

- **Menus and shells:** specific items in the menu and specific commands in the sell.
- **Database views:** restrict user access to data contained in databases.

- **Physically constrained interfaces:** provide only certain keys on a keypad or certain touch buttons on a screen.

Access control matrix:

- A table of subjects and objects indicating what actions subjects can take upon objects.
- Subjects in rows and objects in columns.
- Usually an attribute of DAC models.

Capability table:

- Access rights a certain subject pertaining to specific objects.
- Corresponds to the subject's row in the access control matrix.
- A capability can be in the form of a token, ticket, or key. (e.g. Kerberos ticket).

Access control list (ACL):

- List of subjects that are authorized to access a specific object.
- Defines what level of authorization is granted.
- Corresponds to the object's column in the access control matrix.

Capability-based access control means that the subject has to presenting something, which outlines what is can access (e.g. ticket, token, key, password).

Lattice-based access control provides upper and lower bounds of access for a subject pertaining to a specific object.

Access control administration comes in two basic flavors: ***centralized*** and ***decentralized***.

AAA protocol: authentication, authorization, auditing (some call it accounting).

Traditional authentication protocols:

- Password Authentication Protocol (PAP)
- Challenge Response Authentication Protocol (CHAP)
- Extensible Authentication Protocol (EAP)

Remote Authentication Dial-In User Service (RADIUS):

- RADIUS is an open protocol.
- Network protocol that provides client/server authentication, authorization, and auditing to remote users.
- Access server requests the remote user's login credentials and passes them to a RADIUS server.

- Remote user is a client to the access server, and the access server is a client to the RADIUS server.
- Most ISPs authenticate customers to RADIUS server before allowed access to the Internet.
- Client and access server agree upon an authentication protocol (PAP, CHAP, EAP).
- Access server and RADIUS server communicate over the RADIUS protocol.
- RADIUS protocol is set of fields referred to as **attribute-value pairs (AVPs)** (2^8).
- Appropriate for simplistic username/password authentication with accept/deny response.

Diameter:

- A protocol that have been developed to build upon the functionality of RADIUS and overcome many of its limitation.
- **Peer-based protocol** that allows either end to initiate communication.
- Uses TCP and AVPs (2^32).
- Better error detection and correction than RADIUS.
- Consists on 2 portions:
    - **Base protocol:** provides the secure communication among entities, feature discovery, and version negotiation.
    - **Extensions:** built on top of the base protocol to allow various technologies to use Diameter for authentication (e.g. VoIP, FoIP, Mobile IP, wireless, and cell phone authentication).

Terminal Access Controller Access Control System (TACACS):

- Has gone 3 generations: TACACS, Extended TACACS (XTACACS), TACACS+.
- Cisco-proprietary.
- **TACACS**:
    - combines authentication and authorization processes.
    - Uses fixed passwords for authentications.
- **XTACACS**:
    - separates authentication, authorization and auditing processes.
- **TACACS+**:
    - XTACACS with extended two-factor user authentication.
    - Distinct and totally different protocol and not backward-compatible.
    - Allows users to employ dynamic (one-time) password.
    - Provides same functionality as RADIUS with few differences:
        - Uses TCP and RADIUS uses UDP.
        - RADIUS must have the necessary code to detect packet corruption long timeouts, dropped packets.
        - RADIUS encrypts user's password only (from client to RADIUS server), while TACACS+ encrypts all data.
    - Enables network administrator to define more granular user profiles (what commands users can carry out).
    - Have more AVPs than RADIUS do.

Mobile IP:

- Allows a user to move from one network to another and still use the same IP address.
- Allows a user to have a ***home IP address*** (associated with his home network) and a ***care-of address*** (changes as he moves from one network to another).
- All traffic addressed to home IP address is forwarded to care-of address.

Decentralized access control administration:

- Gives control of access to the people closer to the resources, who better understand who should have access to a certain resource (e.g. functional manager).
- Increase the possibility of conflict of interest.
- Does not provide uniformity and fairness across organization.

Personnel controls indicates what security actions should be taken when an employee is hired, terminated, suspended, moved into another department, or promoted (HR and legal departments are involved).

Each employee has a **supervisor** to report to, and that supervisor is responsible for that employee's actions.

All security controls, mechanisms, and procedures must be **tested** on a periodic basis to ensure they properly support the security policy (management responsibility).

Computer can have physical controls (e.g. locks).

Cables need to be routed throughout the facility and not exposed to any dangers like being cut, burnt, crimpled, or eavesdropped upon.

Zone control: the company facility should be split up into zones based on the sensitivity of the activity taking place per zone.

The following should be audited and logged:

- **System-level events** (e.g. system performance, date/time of logon attempt).
- **Application-level events** (e.g. error messages, files opened/closed).
- **User-level events** (e.g. identification and authentication attempts, commands initiated).

Audit reduction tool reduces the amount of information within an audit log.

SIEM attempts to correlate the log data and provide analysis capabilities (standardization and normalization of data).

Situational awareness means that you understand the current environment even though it is complex and dynamic, to make best possible decisions.

Scrubbing is the act of a hacker where he deletes his track (e.g. from audit logs).

Audit logs can be *stored in a remote host* or on a *write-once media (e.g. CD-ROMs)* to prevent loss of modification of the data.

Keyboard dongle (hardware key logger) can be placed between the keyboard and the computer and can captures even the power-on passwords.

Object reuse: an object must be cleared from sensitive data before being used by another subject (e.g. memory locations, variables, registers, USB drive).

TEMPEST:

- A standard that outlines how to develop countermeasures to electrical signals emitted by electrical equipment.
- Devices have an outer metal coating, referred to as **Faraday cage**, that allows only certain amount of radiation is released.
- TEMPEST rated devices might need modification to other components like power supply.
- 2 alternatives to TEMPEST:
    - **White noise:** uniform spectrum of random electrical signals, It is distributed over the full spectrum so the bandwidth is constant.
    - **Control zone:** some facilities use material in their walls to contain electrical signals, which acts like a large Faraday cage.

IDS have 3 common components: sensors, analyzers, administrative interfaces.

Network-based IDS: has its interface card (NIC) in ***promiscuous*** mode.

Host-based IDS: used to make sure users do not delete system files, reconfigure important setting.

Knowledge/Signature-based IDS:

- **Pattern matching:**
    - Most popular IDS product.
    - Weak against new types of attacks.
- **Stateful matching:**
    - Has rules that outline which state transition sequences should sound an alarm.
    - Only identify know attacks.

Anomaly-based IDS:

- **Statistical anomaly-based:**
    - Put in a learning mode to build a profile of an environment's normal activities.

  - Packets are given an anomaly scope. If it is higher than the predefined threshold, alarm is triggered.
  - Capable of detecting "low and slow" and new attacks.
  - It sends generic alerts, compared to other types of IDSs (team should be experienced to analyze).
- **Protocol anomaly-based:**
  - Has specific knowledge of each protocol they monitor.
  - Builds a model (or profile) of each protocol's normal usage (official and real-world usage).
- **Traffic anomaly-based:**
  - Detects changes in traffic patterns, as in DoS or a new service that appears on the network.

Rule-based (heuristic-based):

  - Use of if/then rule-based programming within expert systems.
  - Use of expert system allows for AI usage (inference engine).
  - More complex rule requires extra processing.
  - Cannot detect new attacks.

Application-based: Very focused in one application and gathers fine-grained and detailed activities.

IDS sensors:

- Placed in network segments the IDS is responsible to monitor.
- Filter out irrelevant information and detect suspicious activity.
- A **monitoring console** monitors all sensors.
- Different placements are possible (outside firewall detects attacks, inside firewall detects intrusions).
- IDS can be centralized (integrated with the firewall) or distributed (multiple sensors throughout the network).
- In very high-traffic network, multiple sensors are preferred to insure all packets are investigated.
- Different sensors can be set to analyze each packet for different signatures (load is broken up over different points).

In **switched environment**, we have to take all the data on each individual connection, make a copy of it, and put the copies on one port (**spanning port**) where the sensor is located.

IPS:

- Detects malicious activity and not allow the traffic to gain access to the target in the first place.
- Preventive and proactive technology.
- Can be content-based (signature-based and protocol analysis) or rate-based metrics which focuses on the volume of traffic (flood attack, excessive scans).

Land attack: a hacker modifies the packet header so that when a receiving system responds to the sender, it is responding to its own address.

Loki attack: usage of ICMP to move data between networks.

Xmas attack: sends a specifically crafted TCP where some of its flags are set to 1.

Attacks or viruses discovered in production environments are referred to as being "**in the wild**".

Attacker can establish a DoS attack on IDS to take it offline. Also, he can send IDS incorrect data to let administrator busy with the wrong part.

Sniffer is a tool that can capture network traffic. If it has the capability of understanding and interpreting individual protocols, it can be referred as a **protocol analyzer**.

Hybrid attack can combine both dictionary attack and a brute-force attack.

War-dialing attack: an attacker inserts a long list of phone numbers into a program in hopes of finding a modem that can be exploited to gain unauthorized access.

Phishing is a type of social engineering with the goal of obtaining personal information credentials, credit cards number, or financial data (**spear-phishing attack** is crafted to trick a specific target). When senior executives are the target, it is called **whaling**.

Pharming redirects a victim to a seemingly legitimate, yet fake, website. In this type of attack, the attacker carries out something called **DNS poisoning**, in which a DNS server resolves a hostname into an incorrect IP address.

Syskey is a 128-bit RC4 encryption key used in Microsoft Windows to encrypt the SAM database.

Password advisor is a tool that helps a user to create passwords that are easy to remember and difficult to break.

CHAPTER 6: Security Assessment and Testing

Audit:

- A systematic assessment of the security controls of an information system.
- Could be driven by regulatory or compliance requirement, by a significant change to the architecture of the information system, or by new developments in the threat facing the organization.
- The scope of the audit should be determined in coordination with business unit managers.
- Information systems security audit process:
    - Determine the goals
    - Involve the right business unit leaders
    - Determine the scope
    - Choose the audit team
    - Plan the audit:
        - To understand any risk introduced to the business processes.
        - Make sure we meet each of the audit goals.
        - Ensure that the audit process is repeatable (reproduce the results).
        - Documentation starts and continue all the way through to the results.
    - Conduct the audit
    - Document the results
    - Communicate the results

Internal audits:

- Familiarity with the inner working of your organization.
- More agile in its assessment efforts.
- **Disadvantages:**
    - The team will probably have a lot of depth in the techniques they know, but not a lot of breadth.
    - Potential conflicts of interests.
    - They may be overstate/fabricate security false to secure better funding.

Third party audits:

- External auditors probably have seen and tested many information systems in different organization.
- Unaware of the internal dynamics and politics.
- ***Compliance audits*** must be performed by external parties.
- **Disadvantages:**
    - Cost.
    - Level of supervision is required even if NDA is signed.
    - Auditors taking a longer time to get oriented and be able to perform the test.

Service organizations are organizations that provide outsourcing services that can directly impact the control environment of a company's customers (e.g. insurance and medical claim processors, hosted data centers, application service providers (ASPs), managed security providers).

Statement of Auditing Standards (SAS 70) audit carried out a way to ensure that a company you work with and depend upon was really protecting your company's assets as they claimed to be.

Other evaluation types have existed: **WebTrust (e-commerce controls)** and **SysTrust (operational controls)**.

Service Organization Controls (SOC):

- A new framework of auditing standards on service organization controls released by AICPA.
- **3 kinds of SOC reports:**
  - **SOC 1:** pertains to financial controls.
  - **SOC 2:** pertains to trust services (security, availability, confidentiality, process integrity, privacy):
    - produces very detailed data which is not for the general public.
    - Includes description of the tests performed by the auditor and the results of those tests and the auditor's opinion of the effectiveness of the individual controls/systems.
  - **SOC 3:** similar to SOC 2:
    - less detailed and can be used for general purposes.
    - Just reports whether the system meet the requirements of the criteria for the specific trust service.
    - Used as "seal for approval" and placed on the service provider's websites and marketing collateral.

Vulnerability testing:

- Before carrying out vulnerability testing, a written agreement from management is required.
- The goals are:
  - Evaluate the security posture
  - Identify as many vulnerabilities as possible.
- Tester must explain the testing ramifications before starting the test.
- **Personnel testing:**
  - Reviewing employee tasks and identifying vulnerabilities in the standards practices and procedures.
  - Social engineering attacks.
- **Physical security:**
  - Reviewing facility and perimeters protection mechanisms.
  - Is there a file suppression system?
- **System and networking testing:**

- Automated scanning products identified known system vulnerabilities and some may attempt to exploit it (always update the vulnerability database of the product before the product is used).

Because security assessment is a point-in-time snapshot, it should be performed regularly.

Vulnerability testing and penetration testing comes in boxes with different colors:

- **Black box testing:**
  - The tester has no *a priori* knowledge of the internal design or features of the system.
  - Simulates an external attacker.
  - **Disadvantages:**
    - May not cover all the internal parts.
    - May by targeting a subsystem which is critical for the daily operations.
- **White box testing:**
  - Auditor has complete knowledge of the inner workings of the system before the first scan.
  - Achieve more complete testing.
  - **Disadvantages:**
    - May not be representative of the behaviors of an external attacker.
- **Gray box testing:**
  - Meets somewhere between the other two approaches.
  - Some, but not all, information on the internal workings is provided to the test team.

Penetration testing:

- The process of simulating attacks on a network and its system at the request of the owner, senior management.
- Measures an organization's level of resistance to an attack and to uncover any weaknesses within the environment.
- Timeframe for the tests should be agreed upon so productivity is not affected.
- It may include physical security, as well as, personnel security.
- The final result of a penetration testing is a report given to management.
- **Steps the team go through:**
  - **Discovery:** foot-printing and information gathering
  - **Enumeration:** performing port scans and resource identification methods
  - **Vulnerability mapping:** identify vulnerabilities in the identified resources
  - **Exploitation:** attempting to gain unauthorized access by exploiting vulnerabilities
  - **Report to management:** deliver a report with all findings to the management.
- **The penetration testing team can have varying degree of knowledge about the target:**
  - Zero knowledge
  - Partial knowledge
  - Full knowledge

"Get Out of Hail Free Card" is an authorization letter authorizing the extent of the penetration testing and should be always available with the testing team members.

Blind test: the assessors only have publicly available data to work with and the network security staff is aware that this type of test will take place.

Double-blind test (stealth assessment): is a blind test to assessors, and security staff is not notified about the test.

Targeted tests can involve external consultants and internal staff carrying out focused tests on specific areas of interest (e.g. before a new application is rolled out).

Commonly exploited vulnerabilities:

- **Kernel flaws:** countermeasure is to ensure that security patches to OS are promptly deployed.
- **Buffer overflows:** countermeasure is to adopt good programming practices and the usage of strongly typed language that disallow buffer overflows.
- **Symbolic links (used in Unix and Linux):** a symbolic link is a stub file that redirects the access to another place. When compromised, an attacker can gain unauthorized access. Countermeasure is programs and scripts must be written to ensure that the full path to the file cannot be circumvented.
- **File descriptor attacks:** file descriptors are numbers that represents open files in a process. If a program makes unsafe use of a file descriptor, an attacker may be able to cause unexpected input or cause output to go to unexpected place. Countermeasure is good programming practices and automated source code scanners.
- **Race conditions:** example is TOC/TOU. Countermeasure is good programming practices.
- **File and directory permissions:** countermeasure is file integrity checkers.

Postmortem: after tests are over and the interpretation and prioritization are done, management have in its hands a compilation of many of the ways the company could be successfully attacked. This is the input to the next cycle in the remediation strategy.

War driving is the act of checking for wireless access points while roaming around the facility.

Log reviews:

- The examination of system log files to detect security events or to verify the effectiveness of security controls.
- Time standardization across all networked devices is very critical in logs (NTPv4).
- By default, logs are stored locally on the corresponding devices.
- Centralization of logs makes it easy to correlate events and archive the logs for long-term retention and automated alerts generation (SEIM).

Preventing log tempering:

- Remote logging
- Simplex communication
- Replication
- Write-once media
- Cryptographic hash chaining

Network Time Protocol (NTP):

- Time is sent in **UDP** datagram that carries 64-bit timestamp on **port 123**.
- Hierarchy of time sources organized into ***strata***:
    - Stratum 0 being the most authoritative (GPS, government standard) and have high accuracy.
    - Network device on a lower stratum acts as a client to a server on a higher stratum, but could be a server to a node in the lower stratum.
    - Nodes in the same stratum level can communicate with each other to improve the accuracy of their times.
    - The standard allows for a hierarchy of *up to 16 strata*.

Synthetic transactions:

- A transaction that is generated by a script and not a person.
- Allows us to systematically test the behavior and performance of critical services (e.g. periodic visit to a website, measure performance, response time)
- Also, can be written to behave as malicious users (e.g. attempting to XSS attacks).

Real user monitoring (RUM) vs. synthetic transactions:

- RUM is a passive way to monitor the interaction of real users with a web application or system.
- RUM uses real people instead of scripted commands.
- RUM is more accurate in capturing actual user experience.
- RUM produces noisy data (e.g. user change their minds in the middle of an operation, losing mobile connectivity).
- Synthetic transactions are predictable and regular and can detect rate occurrences most reliably than waiting for a user to actually trigger that behavior (more proactive).

Misuse case testing:

- Use case that includes threat actor and the tasks they want to perform on the system.
- Threat actors (stick figures with shaded head) and their actions (shaded ovals) in UML.
- Shaded ovals connected to unshaded ones to denote the threat relationship. These create unshaded ovals connected to shaded ones with a narrow labeled “mitigate”.

Code review:

- Performed by someone other than the author of the code.
- Ensure that author follows the team's style guide and standards.
- Looks for uncalled or unneeded functions or procedures (called ***code bloat***).
- looks for modules that are complex and should be restructured or split into multiple modules.
- Looks for blocks of repeated code that could be refactored.
- Meeting can be held to review the code:
    - Obvious errors can be sent offline (not in a meeting).
    - Team leader displays the code and everyone discuss it.
    - At the end of the meeting. A decision made:
        - Passed
        - Passed with rework (only team leader checks the corrections).
        - Re-inspect (another meeting is held).

Defensive programming means that as you develop or view the code, you constantly looking for things to go badly.

Interface testing:

- A systematic evaluation of a given set of exchange points.
- An interface is an exchange point for data between systems and/or users (e.g. NIC, API, GUI).
- A special case of *integration testing* (assessment of how different parts of a system interact with each other).
- **Boundary conditions:** testing in the boundary that separates the good from bad (e.g. a packet that should contain a payload of no more than 1024 bytes. You can check 1024-1, 1024, 1024+1).

Testing data backups:

- Develop scenarios
- Develop a plan
- Leverage automation
- Minimize impact on business
- Ensure coverage
- Document the results
- Fix or improve

Business continuity looks holistically at the entire organization. A subset of this effort, called **disaster recovery**, focuses on restoring the information systems after a disastrous event.

Many people are moving away from BCP/DR ***testing*** (only pass/fail) into performing ***exercises***.

Tests and DR drills and exercises should be performed **at least once a year**.

Specific parameters and scope of the exercise must be worked out before sounding the alarms. The team must agree on what exactly is getting tested, timing and duration of the exercise.

Types of drills:

- **Checklist test (desk check test):** copies of the DRP or BCP are distributed to the different departments and functional areas for review.
- **Structured walk-through test:** representative from each department or functional area come together and go over the plan to ensure its accuracy. The group walks through different scenarios of the plan from beginning to end to make sure noting was left out.
- **Simulation test:** all employees who participates in the operational and support functions come together to practice executing the disaster recovery plan base on specific scenario (used to test reaction of each team member). This test can continue up to the point of actual relocation to an offsite facility.
- **Parallel test:** some systems are moved to the alternate site and processing takes place. This results are compared with the regular processing that is done at the original site.
- **Full-interruption test:** the most intrusive to regular operations. The original site is actually shut down, and processing take place at the alternate site. This time of test only performed after all other types of tests are successful and it needs senior management approval.

After a disaster, **telephone service may not be available**: *mobile phones* or *walkie-talkies* may be used.

Security training is the processing of teaching a skill or set of skills that will allow people to perform specific functions better.

Security awareness training is the process of exposing people to security issues so that they may be able to recognize them and better respond to them. The key measure of the effectiveness of the awareness program is the degree to which people change their behaviors when presented with certain situations.

Pretexting is usually practiced in person or over the phone, in which the attacker invents a believable scenario in an effort to persuade the target to violate a security policy (*it was legal in the US, as long as it doesn't used to obtain financial records*).

Key performance indicators (KPIs) measures how well things are going now.

ISO 27004 Information Security Metrics Implementation, outlines a process by which to measure the performance of security controls and processes.

Factor: an attribute of the ISMS that can be described as a value that can change over time (*e.g. number of alerts generated by an IDS).*

Measurement: the value of the factor at a particular point in time (*e.g. 356 IDS alerts in the last 24 hours*).

Baseline: an arbitrary value for a factor that provides a point of reference (*e.g. historic trend in the number of IDS alerts over the past 12 months*).

Metric: a derived value that is generated by comparing multiple measurements against each other or against a baseline (*e.g. the ratio of verified incidents to IDS alerts during a 30-day period*).

Indictor: an interpretation of one or more metrics that describes an element of the effectiveness of the ISMS (*indicators are meaningful to management*).

Key risk indicators (KRIs) measures how badly things could go in the future.

It is useful to relate KRIs to **SLE equations**.

Technical report:

- Should show that it is a tailored audit (not an output of an automated tool).
- Must document the methodology used.
- Written in the context of ***system under study (SUS)***.
- Highlights the findings and recommended controls or changes.
- Raw data and automated reports can be in the *appendix*.
- **Important key elements:**
    - The treats (*should consider threats as per the risk management process (RMP)*)
    - The vulnerabilities
    - The probability of exploitation
    - The impact of exploitation (*often expressed in monetary terms*)
    - Recommended actions

Executive summaries:

- Technical report includes an executive summary of no more than **1-2 pages**.
- Can show ROI.

Way to express risk in monetary term:

- **Cost approach** simply looks at the cost of acquiring or replacing the asset.
- **Income approach** considers the expected contribution of the asset to the firm's revenue stream.
- **Market approach** is based on determining how much other firms are paying for a similar asset in the marketplace.

Management review:

- A formal meeting of senior organizational leaders to determine whether the management systems are effectively accomplishing their goals (e.g. *performance of the ISMS*).

- Cycle of continuous improvement **Plan-Do-Check-Act** loop.
- The input to the management review comes from **variety of sources** (e.g. results of relevant audits, executive summaries, impact to the organization, recommended changes, list of open issues and action items from the previous meeting, customer feedback).

CHAPTER 7: Security Operations

Operational security: the practice of operational maintenance to keep an environment running at a necessary level, liability, and legal responsibilities.

Administrative management is dealing with personnel issues:

- **Separation of duties:** ensure that one person acting alone cannot compromise the company's security (high-risk activities should be broken up) (preventive).
- **Job rotation:** more than one person fulfills the tasks of one position within the company (helps identify fraudulent activities) (detective).
- **Least privilege:** an individual should have just enough permissions and rights only to fulfill his role. Each user should have a **need to know** about the resources that she is allowed to access.
- **Mandatory vacations:** best for auditing to take 2 contiguous weeks off (detective).

Operations departments often focuses on the hardware and software aspects. **Management** is responsible for employees' behavior and responsibilities.

Security administrators **should not report** to IT administrators (conflict of interests).

Security administrator tasks:

- Implements as maintains security devices and software
- Carries out security assessments
- Create and maintain user profiles and implements and maintains access control mechanisms
- Configures and maintains security labels in mandatory access control (MAC) environment
- Manage password policies
- Review audit logs

Users' access attempts and activities need to be properly monitored, audited and logged (accountability).

Products are available to parse logs to a readable format.

Clipping level is a threshold/baseline number of certain type of errors that will be allowed before the activity is considered suspicious (Mostly IDS is used to track these).

Inconspicuousness prevents the user from knowing too much about security controls.

Operational assurance: concentrates on the product's architecture, embedded features, and functionality that enable a customer to continually obtain the necessary level of protection when using the product.

Life-cycle assurance: how the product was developed and maintained (design specifications, clipping-level configurations, unit and integration testing).

Investigation of the:

- **unusual or unexplained occurrence**
- **deviation from standards:** device accepts 300 requests per minute but now accepts 3 only
- **Unscheduled initial program loads (IPL) (rebooting):** on servers and appliances, rebooting is always scheduled, or intentionally triggered by an authorized person or process.

IPL is a mainframe term for loading the OS's kernel into the main memory.

Central monitoring and event management solutions can save time.

Configuration management is the process of establishing and maintaining effective system control (maintaining consistent baselines on all of our systems).

System crashes (freeze, or shutdown) if it encounters:

- Something insecure
- Did not understand something

An OS response to this type of failure can be (trusted recovery):

- **System reboot:**
  - Takes place after the system shuts itself down in a controlled manner in response to a kernel failure (no enough space in some critical table, OS finds inconsistent data structures).
  - This releases the resources and return the system to a more sable and safe state.
- **Emergency system restart:**
  - after a system failure happens in an uncontrolled manner (kernel or media failure caused by lower-privileged user processes attempting to access a restricted memory segment).
  - System sees it as insecure activity that it cannot properly recover from without rebooting.
  - The system goes into a maintenance mode and recovers from the actions taken.
- **System cold start:**
  - Unexpected kernel of media failure happens and the regular recovery procedure cannot recover the system to a more consistent state.
  - While system attempts to recover itself, intervention from the user or administrator may be required.

Troubleshoot and fix system after crash:

- enter into single user mode or safe mode (when system cold start happens). "single user" mode will not start services for users or the network and only local console is accessible.
- Fix issue and recover files
- Validate critical files and operation

Security issues that should be addressed in a trusted recovery process:

- **Protect the bootup sequence (C:, A:, D:):**
  - The design of the system must prevent an attacker from changing the bootup sequence of the system.
- **Do not allow bypassing of writing actions to system log**
- **Do not allow system forces shutdowns (only administrator can perform shutdowns)**
- **Do not allow outputs to be rerouted**
  - Unauthorized users must not be able to redirect the destination of diagnostic logs and console output.

Applications must perform input checking and logical input.

If a report has no information (nothing to report), it should contain "no output".

Code signing is supported in most OSs: software, device driver, etc.

Gold master (GM) is a standard hardened image for workstations:

- Have all required software
- All proper configuration
- Went through vulnerability scanning and penetration testing.

Unneeded software must be removed; unneeded services must be disabled. Components that can be neither left off not disabled, must be configured to the most conservative practical settings.

Locked-down systems are referred to as **bastion hosts**.

Companies are responsible for ensuring software in their environment is **not pirated**, and that the **licenses are not exceeded**.

AUP must indicate what software users can install and inform user that regular survey will happened to verify compliance.

For secure remote systems administration:

- Use of VPN connection protected by MFA.
- Data should not be in cleartext (SSH should be used)

- Strong authentication should be there
- Truly critical system should be administered locally only
- Small number of administrators should be able to carry out this remote functionality.

Physical security modes:

- During normal facility operations
- During the time the facility is closed

Review should happen to identify which individuals should be allowed into what area and deploy access control points accordingly.

Locks consider a *delaying* devices to intruders.

The delay time provided by the lock should match the penetration resistance of the surrounding components (e.g. door, door frame, hinges).

Keys can be easily *lost* or *duplicated*.

Locks can be *picked* or *broken*.

Padlocks can be used on chained fences

Preset locks can be used on doors

Combination locks have internal wheels that have to line up properly before being unlocked.

Electronic combination locks use keypad that allows a person to type in the combination.

Cipher locks (programmable locks):

- use keypad to control access. Sometimes they require swipe card.
- Provides much higher level of security.
- Unique access code per user (accountability) (referred to as smart locks: e.g. hotel key).
- Functionalities:
    - **Door delay:** alarm is triggered in door is kept open.
    - **Key override:** master combination can be programmed for emergency use to override normal operation or for supervisory operations.
    - **Master keying:** supervisory usage to change access codes or other features.
    - **Hostage alarm:** if user is held hostage, a combination he enters can communicate this situation to the guards or police station.

Mechanical locks:

- **Warded lock (padlock):**
    - It has a spring-loaded bolt with a notch cut on it

  - Cheapest locks
  - Easiest to pick
- **Tumbler lock:**
  - Has more pieces and parts that warded lock
  - The key fits into a cylinder, which raises the lock metal pieces to the correct height. Once all the pieces are in the correct level, the internal bolt can be turned
  - **3 types:**
    - **pin tumbler:**
      - most commonly used
    - **wafer tumbler (disc tumbler):**
      - small round locks used for file cabinets
      - can be easily circumvented
    - **lever tumbler**

Device locks:

- **Switch controls:** covers on/off power switches.
- **Slot locks:** tie bracket mounted in a spare expansion slot to a stationary component using a steel cable.
- **Port controls:** block access to disk drives or unused serial or parallel ports.
- **Peripheral switch control:** secure a keyboard by inserting an on/off button switch between the system unit and they keyboard input slot.
- **Cable trap:** prevent removal of input-output devices by passing their cables through a lockable unit.

Locks should be assigned by facility management and assignment must be documented.

Tension wrench:

- is a tool shaped like an L and is used to apply tension to the internal cylinder of a lock.
- the lock picker uses a lock pick to manipulate the individual pins to their proper placement. Once picked, a tension wrench holds these down while the lock picker figures out the correct settings of the other pins.

Raking:

- to circumvent a tumbler lock, a lock pick is pushed to the back of the lock and quickly slid out while providing upward pressure.

Lock bumping:

- force the pins in tumbler lock to their open position by using a special key called *bump key*.
- The stronger the material of the lock, the smaller the change for this way to success.

Locks strengths:

- **Grade 1:** commercial and industrial use

- **Grade 2:** heavy-duty residential/light-duty commercial
- **Grade 3:** residential/consumer

Cylinders within a lock:

- **Low security:** no pick or drill resistance
- **Medium security:** medium pick or drill resistance
- **High security:** high pick or drill resistance

Preventive measure against **piggybacking**:

- security guards
- educate employees
- mantrap

Cards types:

- **memory card:** the reader pulls information from it and makes an access decision
- **smart card:** individual may be required to enter a PIN or password

Proximity identification devices:

- **user-activated readers:** user actually has to do something (swipe card or enter a PIN)
- **system-sensing readers (transponders):**
  - recognize the presence of an approaching object within a specific area
  - The reader sends an interrogating signals and obtain the access code from the card without the user having to do anything

Electronic access control (EAC) tokens is a generic term used to describe proximity authentication devices: proximity readers, programmable locks, biometric systems.

Perimeter security controls can be:

- **Natural** (hills, rivers)
- **Manmade** (fencing, lighting, gates)

Fencing is a psychological deterrent control (first line of defense).

Barbed wire on top of the fences can be tilted in or out.

Perimeter Intrusion Detection and Assessment System (PIDAS):

- A type of fencing that has sensors located on the wire and at the base of the fence
- Detects if someone attempts to cut or climb the fence
- It has passive cable vibration sensor
- Very sensitive and can cause false alarms

Fence height:

- **3-4 feet** (deter casual trespassers)

- **6-7 feet** (too high to climb easily)
- **8 feet** (deter more determined intruder)

Gates strengths:

- **Class I:** residential usage
- **Class II:** commercial usage (public access)
- **Class III:** industrial usage (limited access)
- **Class IV:** restricted access (prison)

Underwriters Laboratory (UL) classifies electronic devices, fire protection equipment, and specific construction materials.

Bollards placed to limit the treat of someone driving a vehicle through the exterior wall

Lighting is used to eliminate dead spots (unlit areas) should exist between the lights

If the light is going to bounce off of dark, dirty, or darkly painted surface, then more illumination is required for contrast between people and environment.

Guards to be more in the shadows (lower amount of illumination) (***glare protection***)

Continuous lighting is an array of lights that provides an even amount of illumination across area.

Lighting gadgets are used as **standby lighting**.

Security guards can switch lights on and off, so potential intruder thinks that people are inside.

CCTV system: cameras, transmitters, receivers, recording system, monitors.

Attack on CCTV is to replay previous recording without security guards knowing it.

Digital recorders save images to hard drives and allow advanced search techniques that are not possible with videotape recorders. It also used advanced compression techniques.

Charged-coupled devices (CCD):

- an electrical circuit that receive input light from the lens and converts it into an electronic signal, which is then displayed on the monitor.
- Allows capture of extraordinary details of objects and precise representation.
- It has sensors in the infrared range, which extends beyond human perception.

Type of lens:

- Fixed focal length: wide, medium, narrow (normal view is like human eye)
- Zoom (varifocal)

Focal length:

- Effectiveness in viewing objects from a horizontal and vertical views
- Its value relates to the angle of view that can be achieved
- **Short** focal length lenses provide **wider-angle** view.
- **Long** focal length lenses provide a **narrower** view.

Fixed focal length lenses doesn't allow **optical** change of the area that fills the monitor. Though, it achieved data **digitally** (decrease the image quality) (***digital zoom***).

Depth of field:

- the portion of the environment that is in focus when shown in the monitor
- to take photo of a person, use **shallow depth of focus**
- to take photo of the background, use **greater depth of focus**
- the depth of field increases as the size of the length opening decrease.

CCTV lenses have ***irises***, which control the amount of light that enters the lengths:

- **manual iris** lens must adjust manually by rotating a ring around the lens.
- **Auto iris** should be used in environment where the light changes (outdoor).

Illumination requirements are represented by ***lux*** value.

Cameras can be **fixed mounted** or **PTZ**.

Annunciator system: listen for noise, or detect movement, and activate electrical devices (e.g. lights, sirens). No need for security guards to keep staring at a CCTV monitor.

IDSs can be used to detect changes in:

- Beam of light
- Sounds and vibrations
- Motion
- Different types of fields (microwave, ultrasonic, electrostatic)
- Electrical circuits

IDSs can detect intruders by employing:

- electromechanical systems (magnetic, switches, metallic foil, pressure mats)
- volumetric systems (vibration, microwave, infrared, photoelectric) – *more sensitive*

Electromechanical systems: detecting a change or break in a circuit (e.g. strip of foil embedded in window)

Vibration detectors can detect movement on walls, screens, ceilings, floors by fine wires embedded into the structure.

Photoelectric systems (photometric) detects the change in light beam (used only in windowless rooms):

- cross-sectional means that one area can have several different light beams extending across it (e.g. using hidden mirrors to bounce back until it hits the receiver).

Passive infrared (PIR) system identifies the changes of heat waves.

Acoustical detection system uses microphones installed on floors, walls, ceilings:

- Very sensitive and cannot be used in areas open to sounds.

Vibration sensors used to detect forced entry (used in walls of vaults in banks).

Wave-pattern motion detectors differ in the frequency of the waves they monitor:

- It sends patterns and receive it back. If pattern is distributed, it means something in the room moves.

Proximity detector (capacitance detector) emits a measureable magnetic field. An alarm is sound if field is disrupted (e.g. artworks, cabinets, safe).

Electrostatic IDS:

- Creates and electrostatic magnetic field made up of subatomic particles.
- Creates a balanced electrostatic field between itself and the object.
- If intruder comes within a certain range of the monitored object, there is a capacitance change.

IDSs are:

- Expensive and require human intervention
- Require redundant and emergency power supplies
- Can be linked to a centralized security system
- Should have a **fail-safe** configuration (**default is "activated")**
- Should detect, and be resistant to, tempering

Patrol force to monitor the facility's grounds (deterrence)

Dogs used to detect intruders (in CISSP dogs might not be the correct choice due to human safety).

Provisioning is the set of activities required to provide one or more new information services to a user or group of users.

PAS 28000:2007 means to use a consistent approach to securing supply chain.

Back-doors installed in hardware by **manufacturers (pirated hardware)** or 3rd parties (**government**).

Pirated software might include back-doors and impossible to patch/update.
Change control process:

1. Request for a change to take place
2. Approval of the change
3. Documentation of the change: should be entered into a change log
4. Tested and presented: rollback plan in this phase
5. Implementation
6. Report change to management

Network and resources availability:

- **Redundant hardware** (ready to for hot swapping by replacing the failed component while the system is running. Usually degraded performance but avoid downtime)
- **Fault-tolerant technologies:** survive single component failure (expensive)
- **Service level agreements (SLA):** from service providers
- **Solid operational procedures**

Mean Time Between Failures (MTBF): rely on vendor to calculate this value as they have information on many devices than we do (it means device is repairable, if not, it'll be called mean time to failure MTTF).

Mean Time To Repair (MTTR): how much time is required to repair.

Single point of failure. **Countermeasures**: backups, maintenance, redundancy, fault tolerance, multiple paths, dynamic routing protocol, ISDN backup line.

Redundant array of independent disks (RAID):

- a technology used for redundancy and/or performance improvement that combines several physical disks into one logical array.
- Have *hot-swapping* disks (they can replace drives while the system is running).
- **RAID 10** (combination of level 1 and 0: **RAID 1+0** or **RAID 0+1**)

Stripping:

- divides the data and writes it across multiple drives.
- Write is not affected. Read is improved as multiple disks being read at the same time.

RAID Level	Activity	Name
0	Data striped over several drives. No redundancy or parity is involved. If one volume fails, the entire volume can be unusable. It is used for performance only.	Striping
1	Mirroring of drives. Data is written to two drives at once. If one drive fails, the other drive has the exact same data available.	Mirroring
2	Data striping over all drives at the bit level. Parity data is created with a hamming code, which identifies any errors. This level specifies that up to 39 disks can be used: 32 for storage and 7 for error recovery data. This is not used in production today.	Hamming code parity
3	Data striping over all drives and parity data held on one drive. If a drive fails, it can be reconstructed from the parity drive.	Byte-level parity
4	Same as level 3, except parity is created at the block level instead of the byte level.	Block-level parity
5	Data is written in disk sector units to all drives. Parity is written to all drives also, which ensures there is no single point of failure.	Interleave parity
6	Similar to level 5 but with added fault tolerance, which is a second set of parity data written to all drives.	Second parity data (or double parity)
10	Data is simultaneously mirrored and striped across several drives and can support multiple drive failures.	Striping and mirroring

Table 7-2 Different RAID Levels

Direct access storage device (DASD):

- a general term of magnetic disk storage devices which has been in mainframes and mini computers (mid-range computers).

DASD vs. SASD (Sequential):

- DASD: any point may be promptly reached (e.g. RAID).
- SASD: every point in between the current position and the desired position must be traversed in order to reach the desired position (e.g. tape drives).

Some tape drives have minimal DASD intelligence (include multitrack tape devices that stored specific points on the tape).

Massive array of inactive disks (MAID):

- Carries out mostly *write* operations
- Intended to not have active drives
- All inactive disks powered down, with only the controller alive
- When application asks for data, the controller powers up the appropriate disk(s), reads the data, and powered it down again

- Increase power saving and disk lifetime

Redundant array of independent tapes (RAIT):

- Similar to RAID but uses tapes
- Lower in cost
- Very slow
- For very-large writes (where MAID is not economical) and higher performance than typical tape store is desired, RAIT may fit.

Storage area network (SAN):

- Numerous storage devices linked together by a high-speed private network and a storage-specific switches.
- Provide redundancy, fault tolerance, reliability, backups.

Clustering (server farm):

- Fault tolerance server technology.
- Each server takes part in processing services.
- Viewed logically as one server.
- Immunity to fault.
- Improved performance.

Grid computing:

- Load-balanced parallel mean of massive computation.
- Nodes may join or leave randomly (loosely coupled systems).
- Most computers have extra CPU processing power that is not being used and can be utilized in grid computing.
- Nodes do not trust each other and have no central control.
- Should not process sensitive data or time-sensitive applications.

Backup policy implements and indicates: what gets backed up, how often it gets backup up, and how these processes should occur.

Hierarchical storage management (HSM):

- Provides continuous online backup functionality.
- Combines hard disk technology with the cheaper and slower optical or tape.
- The faster media holds the files that are accessed more often.
- "stub" is used as pointer to where the information is actually located/stored.
- Focused on a balance between cost and performance.

Contingency planning:

- Defines what should take place during and after an incident.
- Must be documented and readily available. At least 3 documents:
    - Original on site

    - Copy on site but in protective, fireproof safe.
    - Copy in an offsite location.
- It should be tested (organizations must carry out exercises).

BCP vs. Contingency planning:

- BCP addresses how to keep the organization in business after a disaster takes place.
- Contingency planning address how to deal with small incidents that do not qualify as disasters.

Preventive measures:

- Understand the risk
- Use the right tools
- Use the controls correctly
- Manage your configuration
- Assess your operation

IDS can be HIDS, NIDS or WIDS.

IDS can be rule-based or anomaly-based.

False positive is detecting intrusions when none happened.

False negative is when system incorrectly classifies as benign.

Base-lining is the process of establishing the normal patterns of behavior (even used in rule-based should be configured with what is normal for an organization).

Fine-tuning IDS is essential to reduce false positives.

Antimalware is a signature-based and cost effective protection.

Patch management is the process of identifying, acquiring, installing, and verifying patches for products and systems.

Patches are software updates intended to remove vulnerability or provide new feature.

Unmanaged patches (decentralized): each software periodically checks for updates and automatically applies them. **Disadvantages:**

- Requires credentials
- Difficult configuration management
- Bandwidth utilization
- Affects service availability

Centralized patch management:

- Best practice
- Comes in different flavors:
  - **Agent based:** an update agent is installed on each device.
  - **Agentless:** use some hosts to remotely connect to each device using admin credentials and check for updates (usually uses AD objects in domain controllers to manage patch levels).
  - **Passive:** passively monitor the network traffic to infer the patch levels (least effective).

Attackers are reverse engineer recent release patches to understand the vulnerability and exploit still unpatched systems:

- Some vendors use *code obfuscation* to eliminate this threat.

Sandbox is an application execution environment that isolates the executing code from the operating system to prevent security violations.

Honeynet is an entire network that is meant to be compromised (2 or more honeypots).

Organization can dynamically spawn honeypots to appeal attacker (adaptive).

Honeyclients are synthetic applications meant to allow an attacker to conduct a client-side attack (can be human interactive or highly automated):

- If you suspect a phishing attack, you can let a honeyclient to visit the link in the email and pretend it is a real user.

Black holes typically are routers with rules that silently drop specific (malicious) packets without notifying the source (render botnet useless).

Incident management process:

- **Detect:** realize that there is a problem.
- **Respond:** determine what the appropriate response might be.
- **Mitigate:** mitigate or contain the damage.
- **Report:** starting of a continuous process of documentation.
- **Recover:** return all systems and information to a known-good state.
- **Remediate:** need to ensure that the attack is never again successful. Identification of IOA and IOC (share them with community).
- **Learn:** have team briefing that includes all groups affected to answer their questions.

Organization should develop incident response team (from various department):

- **Virtual team** (made up of experts who have other assignment within organization).
- **Permanent team** (dedicated strictly to incident response).

- **Hybrid team** (part is dedicated and part is called upon when required).

Incident response policy should be managed by the legal department and security department.

CERT is an organization that is responsible for monitoring and advising users and companies about security perpetration and security breaches.

The cyber kill chain:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation: executing on the malware on a CPU
5. Installation
6. Command and Control (C&C)
7. Actions on the objective

If you can thwart the attack before stage four (exploitation), you stand better change of wining.

MTD (maximum tolerable downtime):

- Company will not be able to recover if this time exceeds.

RTO (recovery time objective):

- Maximum time period within which a business process must be restored to avoid breaking the business continuity (acceptable downtime).
- Deals with getting the infrastructure and systems up and running.

WRT (work recovery time):

- Remainder of the overall MTD value after the RTO has passed.
- Deals with restoring data, testing processes, and making everything live for production.

RPO (recovery point objective):

- Acceptable amount of data loss measured in time.

All these values are derived from from **BIA** process.

Disruption in BCP terms:

- **Non-disasters:** disruption in service with limited impact on business at a facility.
- **Disasters:** event that causes the entire facility to be unusable for a day or longer.
- **Catastrophes:** a major disruption that destroys the facility altogether.

In case facility got affected, the organization should decide on:

- dedicated site that the organization operate itself.
- Lease a commercial facility such as “hot site”.

- Enter into a formal agreement with another facility.

3 main types of leased or rented offsite facilities:

- **Hot site:**
  - Fully configured and ready to operate within few hours
  - Only missing items usually data only
  - Equipment and system software must absolutely be compatible
  - Most of the time, it supports *annual tests*
  - Most expensive
- **Warm site:**
  - Partially configured with some equipment (HVAC, wiring)
  - No actual components
  - Practical for proprietary hardware or software
  - Most widely used model
- **Cold site:**
  - An empty data center
  - Need weeks to get the site activated
  - Could have racks and dark fiber
  - Least expensive

Service bureau is a company that has additional space and capacity to provide applications and services such as call centers.

Contingency company supplies services and materials temporarily to an organization that is experiencing an emergency.

Tertiary site is a *secondary* backup site, just in case the primary backup site is not available (backup to the backup).

Reciprocal agreement:

- can be established with another company (usually in similar field).
- If company A have a disaster, company B offers the usage of its facility (and vice versa).
- Difficult for two companies to work in the same shared facility.
- NOT enforceable agreement.

Consortium (mutual aid agreement) is similar to reciprocal agreement but *more than two organizations* agree to help one another.

Hot site is a *subscription* service. **Redundant site** is a site *owned* and maintained by the company.

Rolling hot site (mobile hot site) is a site on the back of a large truck (can be data center or working area).

Multiple processing centers is when organization may have 10 different facilities throughout the world, where data can be moved between them in a mater of seconds when an interruption is detected.

Even if the company **outsource** a service, the **organization is ultimately responsible** for the continuity of a product or service that is outsourced.

Hardware backups:

- Estimated of the hardware availability and delivery time.
- Depends on vendors SLA or purchase redundant hardware?
- Replacement of legacy systems?

Software backups:

- 2 copies: 1 (on-site) + 1 (offsite).

Software escrow:

- Where a 3rd party holds the source code, backup of the compiled code, manuals, and others.
- Customer can have an access to the source code only if and when the vendor goes out of business.

Executive succession planning is if someone in a senior executive position retires, leave the company, or is killed, the organization has predetermined steps to carry out to protect the company (e.g. deputy role).

Online backup technologies usually record the changes to a file in a *transaction log*, which is *separate from the original file*.

Full backup:

- all data is backed up.
- Archive bit is cleared (0).
- Restoration is one step.
- Backup/restore could take along time.

Differential backup:

- Bucks up the files that have been modified *since the last full backup*.
- Archive bit does not change.
- Full backup restored first, followed by the most recent differential backup is put on top.

Incremental backup:

- Backs up all the files that have been changed *since the last full backup or incremental backup*.
- Archive bit is cleared (0).
- Full backup restored first, followed by each incremental backup *in order*.

It is important to **not mix differential and incremental backups**. This overlap causes files to be missed, since the incremental backup change the archive bit and the differential does not.

Software backup technologies

Disk duplexing:

- Means that there is more than once disk controller. If one disk controller fails, the other is ready and available.

Disk shadowing:

- Used to ensure availability of data and to provide fault tolerance.
- Duplicating hardware and maintaining more than one copy of information.
- Provides online backup storage.
- Boost read operation performance (parallel read).

Disk mirroring:

- Each disk would have a corresponding mirrored disk that contains the exact same information.

Electronic vaulting:

- Makes copies of the files as they are modified and periodically transmits them to an offsite backup site.
- Takes place in batches (not real-time) (e.g. hourly, daily, weekly).

Remote journaling:

- Include moving the journal or transaction logs to the offsite facility not the actual files.
- Logs contains the deltas (changes) that have taken place to files.
- Takes place in real-time.
- Efficient for database recovery.

Tape vaulting:

- The data is sent over a serial line to a backup tape system at the offsite backup site.
- Better than manually transfer the tape.

Asynchronous replication:

- means the primary and secondary data volumes are out of sync.
- Synchronization may take place in: seconds, hours, days.

Synchronous replication:

- means the primary and secondary data volumes are always in sync.
- Real-time duplication.

High availability is a combination of technologies and processes that work together to ensure that some specific thing is always up and running.

Fault tolerance is the capability of a technology to continue to operate as expected even if something unexpected takes place (a fault).

Failover means that if there is a failure that connected be handled, then processing is "switched over" to a working system.

Reliability is the probability that a system performs the necessary function for a specified period under defined conditions.

Insurance:

- can be taken to not take the full risk.
- The goal is to make the coverage fills in the gap in what the current preventive controls cannot protect against.

Cyber insurance is a new type of coverage that insures losses caused by a DoD attack, malware damages, hackers, etc.

Business interruption insurance if if the company is out of business for a certain period, the insurance company will pay for specified expenses and lose earnings.

If the company doesn't practice due care, the insurance company may not be legally obliged to pay.

Restoration team is responsible for getting the alternative site into a working and functioning environment

Salvage team is responsible for starting the recovery of the original site.

Reconstitution phase if the time for the company to move back into its original site, or new site.

The least critical function should be moved back first, to uncover any issues in network configurations or connectivity, etc.

Structure of BCP:

- Initiation phase
- Activation phase
- Recovery phase

- Reconstruction phase
- Appendixes

Continuity of operations (COOP):

- A U.S government initiative to ensure that agencies are able to continue operation after a disaster or disruption.
- Similar to BCP, but BCP is more private-sector oriented.
- Focuses on restoring essential functions in the alternative sites and perform these functions for up to 30 days before returning to the normal operation.

Even acts of nature (storms, earthquakes, etc.) allow adversaries to victimize the organization.

Forensics is a science and an art that requires specialized techniques for the recovery, authentication, and analysis of electronic data for the purposes of a digital criminal investigation (digital evidence).

The **most fragile and volatile** evidence should be collected first.

Scientific working group on digital evidence (SWGDE) aims to ensure consistency across the forensics community.

Motive – Opportunity – Means (MOM):

- **Motive:** "who" and "why"
- **Opportunity:** "where" and "when"
- **Means:** abilities a criminal would need to be successful

Modus Operandi (MO) for computer criminals may include the use of specific hacking tools, or targeting specific systems or networks. This method usually involves repetitive signature behaviors.

Locard's exchange principle also applies to *profiling*: criminal leaves something behind at the crime scene and takes something with them.

Forensics process:

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation
- Decision

Exact copy of the hard drive must be taken (e.g. *Forensics Toolkit*, *EnCase*, *dd Unit utility*).

Original media should have 2 copies:

- **Primary image** (a control copy in the media library)
- **Working image** (for analysis and evidence collection)

The **new media** to copy the original image to, must be purged.

Chain of custody is a history that shows how evidence was collected, analyzed, transported, and preserved in order to be presented in court.

Dead forensics in ***labs***. **Live forensics** in ***field***.

Most of the time, computer-related documents are secondhand evidence (**hearsay**).

4 characteristics of evidence:

- **Relevant:** must have a reasonable and sensible relationship to the findings**.**
- **Complete:** must present the whole truth of an issue.
- **Sufficient/believable:** persuasive enough.
- **Reliable:** consistent with facts.

---

2 main types of surveillance:

- Physical surveillance (CCTV)
- Computer surveillance (auditing events, sniffers, keyboard monitors, wiretaps)

Exigent circumstance is when a law enforcement agent collects an evidence that is not included in the warrant.

Enticement is legal.

Entrapment is neither legal or ethical.

Interviewer of a suspect:

- should be in a position that is senior to the employee suspect.
- Held in a private place.
- No need to read person's rights unless law enforcement officers do the interrogation.

Due care means that a company did all it could have reasonably done to prevent security breaches (company practiced common sense and prudent management and acted responsibly).

Due diligence means that the company properly investigated all of its possible weaknesses and vulnerability.

Downstream liability is where a company A sue company B because company B was negligent and affected company A.

To prove negligence in court, the plaintiff must establish that the defendant had a ***legally recognized obligation*** to protect data reasonably.

Proximate cause is an act or omission that naturally and directly produces a consequence (e.g. cause to an injury).

Vendor management governing includes performance, metrics, SLA, scheduled meetings, reporting structure.

Auditor can be internal or external.

Governance, risk and compliance (GRC).

Occupant emergency plan (OEP) describes that actions that facility occupants should take in order to ensure their safety during an emergency situation.

S-RPC uses Diffie-Hellman public key cryptography to to determine a shared key to be used with DES to encrypt remote procedure calls.

65% of businesses would fail if they have downtime for 1 week.

Parallel test ensures that specific systems moved and work at the new location, without interfering with business operation.

Simulation test go through a simulated disaster to identify whether emergency response plans are adequate.

Full-interruption test is a real test to fully mimics real situation.

Walk-through test is walk through plans to identify issues and changes.

Checklist test is a test where all departments are given a copy of the continuity plan. Each department must review and confirm that the information is correct.

Slamming is when a user's telephone service provider has been changed without that user's consent.

Cramming is adding on bogus charges for services that user did not request or receive.

Economic Espionage Act prosecute a theft of trade secrets.

First Amendment protects person's free speech and expression.

Approaches to address privacy:

- **The generic approach is horizontal enactment.** It defines rules that stretches across all industries (including government).

- **Regulation by industry is vertical enactment.** It defines requirements for specific verticals.

Anticybersquatting Consumer Protection Act (ACPA) protects trademarks (domain names).

SATAN (Security Administrator Tool for Analyzing Network) is a scanning tool that can uncover weaknesses within a network.

CHAPTER 8: Software Development Security

Programmers traditionally are not educated to secure coding.

OSs and applications were not build on secure architectures.

Software development procedures have not been security oriented.

Security products can, **to a certain degree**, help mitigating risks rise by bad coding.

Out of the box implementations are not secure. Most security has to be configured and turned on after installation.

Software development life cycle (SDLC):

- **Requirement gathering:**
  - Could include evaluating products currently on the market.
  - Could be direct request for a specific project from a customer.
  - Security topics:
    - *Security requirement*
    - *Security risk assessment*
    - *Privacy risk assessment (privacy impact rating can be assigned)*
    - *Risk-level acceptance*
- **Design:**
  - Information model: type of information to be processed and how it'll be processed
  - Functional model: the tasks and functions the application needs to carry out
  - Behavioral model: states the application will be in during and after specific transition takes place
  - Security topics (e.g. automated tools available):
    - *Attack surface analysis*
    - *Threat modelling*
- **Development:**
  - Security topics:
    - Computer-aided software engineering (CASE) tools: generate code, test, debug.
    - *Static analysis*
- **Testing/validation:**
  - Good developers develop unit tests before start coding, or in parallel (*test-driven approach*).
  - Different team can carry out the formal testing (separation of duties).
  - If system crashes, it should revert to a secure state.
  - Security topics:
    - *Dynamic testing*
    - *Fuzzing*

        - *Manual testing*
        - *Unit, integration, acceptance, regression testing*
- **Release/maintenances:**
    - Security topics:
        - *Final security review*

Privacy impact rating (no standards approach to define these ratings):

- P1, High privacy risk (e.g. PII is stored and processed)
- P2, Moderate privacy risk (e.g. affecting privacy is a one-time and user-initiated)
- P3, Low privacy risk (e.g. no privacy information)

If a software product is developed for a specific customer, it is common for a **Statement of Work (SOW)** to be developed, which describes the product and customer requirement. This help to make sure the requirements are properly understood and assumptions are made.

Scope creep is when the scope is continually extending in an uncontrollable manner.

Work breakdown structure (WBS) is a project management tool which decompose the project into tasks and subtasks.

Buffer overflow can lead to a privilege escalation.

Organizations have secure software development guidelines:

- **OWASP:** issues top 10 web applications security issues.
- **U.S. Department of Homeland Security (DHS):** best practices in all aspects for every phase in building secure software (called *Build Security in, BSI*).
- **MITRE:** have Common Weakness Enumeration (CWE) initiative, which maintain a list of the top most dangerous software errors.

Code review:

- Manual inspection by human.
- Can detect logical and design flaws.

Static analysis:

- Examining the code without executing the program.
- Carried out before the program is complied.
- Usually done by automated tools.
- Cannot reveal logical errors and design flaws (e.g. must be used with code review).

Dynamic analysis:

- Evaluation of a program in real-time, when it is running.
- Effective for compatibility testing, detection memory leakage, identifying dependencies.

Types of Testing:

- **Unit testing:** testing individual component.
- **Integration testing:** verifying that components work together.

- **Acceptance testing:** ensure meeting customer requirements.
- **Regression testing:** happen after a change is introduced to the system.

Manual testing involves auditing by security-centric programmers (simulates live scenarios involved in real-work attacks).

Fuzzers use complex input to impair program execution to discover flaws (e.g. buffer overflows, DoS vulnerabilities, injection weaknesses, validation flaws).

Verification: determines if the product accurately represents and meets the specifications (**did we built the product right?).**

Validation: determines if the product provides the necessary solution for the intended real-world problem (**did we built the right right?).**

OWASP top 10 web application security risks:

- A1: Injection
- A2: Broken authentication and session management
- A3: Cross-site scripting (XSS)
- A4: Insecure direct object references
- A5: security misconfiguration
- A6: Sensitive data exposure
- A7: Missing function level access controls
- A8: Cross-site request forgery (CSRF)
- A9: Using components with known vulnerability
- A10: Un-validated redirects and forwards

Build and Fix model:

- No architecture design is carried out with little or no planning.
- Problems are dealt with as they occur.

Waterfall model:

- Linear-sequential life-cycle approach.
- Each phase must be completed entirely before the next phase can begin.
- At the end of each phase, a review takes place to make sure the project is in the correct path.
- All requirement gathered in the initial phase and they is no formal way to integrate new changes or requirement (e.g. waiting for the entire project to complete).
- Could be useful for small projects that have all requirements fully understood.

V-Shaped model (V-model):

- It follows steps that are laid out in a V format.

- Verification and validation of the product at each phase and provides a formal method of developing testing plans as each coding phase is executed.
- Sequential path of execution processes. Each phase must be completed before the next phase begins.
- Requires testing throughout the development phases and not just waiting until the end of the project.
- Adapting to changes is more difficult and expensive.
- Good if the requirements are understood up front and scope changes are small.

Prototyping:

- ***Prototype*** is a sample of software code or a model that can be developed to explore specific approach to a problem before investing expensive time and resources.
- 3 different main prototype models:
  - **Rapid prototype (throwaway):**
    - Develop a prototype to test the validity of understanding.
    - "quick and dirty".
    - Sample not meant to be built upon, but to be discarded.
  - **Evolutionary prototype:**
    - Build for incremental development until it reaches the final product stage.
    - Feedback obtained through each phase is used to improve the prototype.
  - **Operational prototype:**
    - An extension of the evolutionary prototype method.
    - Designed to be implemented within a production environment as it is being tweaked.

Incremental Model:

- Allows the team to carry out multiple development cycles on a piece of software throughout its development stage.
- Each incremental phase results in a deliverable that is an operation product.
- Product is available at early stages of development (flexibility).
- Allows for changes to take place.
- Testing after each operation allows errors to be identified earlier.
- Good if vendor wants to deliver customer a working product with basic functionality as it works in the development of the product.

Spiral Model:

- An iterative approach.
- Emphasis on risk analysis.
- 4 main phases:
  - Determine objectives
  - Risk Analysis
  - Development and test
  - Plan the next iteration
- Allows new requirement to be addressed as they are uncovered.

- Allows for testing to take place early in the development project.
- Good model for complex projects that have fluid requirements.

Rapid Application Development (RAD):

- Relies more on the use of rapid prototyping than on extensive upfront planning.
- The delivery of a workable product takes **less than half of the time** compared to Waterfall model.
- Combines the use of prototyping and iterative development procedures.
- Allows for the customer to be involved in the development phase (end result maps his expectation).

Agile model:

- An umbrella for several development methodologies.
- Focus on incremental and iterative development methods (not prototype).
- Considered "lightweight".
- Focuses on small increments of functional code that are created based upon business need (not too much upfront design analysis).
- Promotes customer collaboration instead of contract negotiation.
- **User story** is a sentence that describes what a user wants to do and why.
- Development team can take parts of all of the available SDLC methods.

Scrum:

- The **most** widely adopted agile methodology today.
- Good for projects of any size and complexity.
- Vere lean and customer focused (the fact the customer needs cannot be completely understood in the initial phase).
- Focus on team collaboration, customer involvement and continuous delivery.
- Addition, changes, removal can happen at the conclusion of each ***sprint***.
- **Sprint** is a fixed duration development interval that is usually two weeks in length and promises delivery of a very specific set of features.

Extreme programming (XP):

- Takes code review to the extreme by having them take place continuously.
- **Pair programming:** one programmer dictates the code to her partner, who then types it.
- Rely on *test-driven development* (unit tests are written before the code).

Kanban:

- Developed by Toyota.
- Stresses visual tracking of all tasks so that the team knows what to prioritize as what point in time (e.g. sticky notes in a conference room).
- Kanban wall usually divided vertically by production phase (Planned, In Progress, Done).

Exploratory model:

- Clearly defined project objectives have not been presented.

Joint Application Development (JAD):

- Workshop-oriented environment.
- Includes of members other than coders in the team (e.g. executives, experts, end-users).

Reuse model:

- Reusable programs are evolved by gradually modifying pre-existing prototypes to customer specifications.
- Doesn't require programs to be built from scratch.
- Reduces development time and cost.

Cleanroom:

- Attempts to prevent errors by following structured and formal methods of developing and testing.
- Used for high-quality and mission-critical applications.

Integrated product team (IPT):

- A multidisciplinary development team with representative from many or all the stakeholder populations.
- **IPT** focuses on brining in the business stakeholders. **JAD** focuses on involving the end-user community.

DevOps: development team includes software development, operations staff (IT), quality assurance (QA).

Capability Maturity Model Integration (CMMI):

- It addresses the different phases of a software development life cycle.
- It can be used to evaluate security engineering practices and identify ways to improve them.
- 3rd party companies evaluate software development companies to certify their product development processes.
- **5 maturity levels:**
  - **Initial (no plan):**
    - Development process is ad hoc or even chaotic.
    - Company does not use effective management procedures and plans.
    - No assurance in consistency and quality.
  - **Repeatable (structure but no defined processed):**
    - Formal management structure, change control, quality control.
    - The company does not have formal process models defined.
  - **Defined (defined processes and quantifiable results):**
    - Formal procedures are in place that outline and define processes carried out in each project.
    - The company has a way to allow for quantitative process improvement.
  - **Managed (processes to analyze quantitative data):**

        - The company has formal processes in place to collect and analyze quantitative data.
        - Metrics are defined and fed into the process improvement program.
    - **Optimizing (continuous improvement):**
        - The company had budgeted and integrated plans for continuous process improvement.

Change control is the process of controlling the changes that take place during the life cycle of a system and documenting the necessary change control activities.

New code should go to the *librarian*. Production code should come only from the librarian and not from a programmer or directly from a test environment.

Software configuration management (SCM):

- Identifies attributes of software at various points in time.
- Performs methodical control of changes for the purpose of maintaining software integrity and traceability.
- **Versioning** keeps track of file revisions (make it possible to "*rollback*").

Code repositories:

- Encouraged to be implemented in an isolated network (*air-gaped*). This enhance security but makes it hard for external developers to collaborate and for remote access.
- Can be hosted in the internet, with VPN connection with an added SSH security layer.

Programming languages categories:

- **G1: Machine language:**
    - A format that the computer's processor understands and work with directly.
    - Binary format (1 and 0).
- **G2: Assembly language:**
    - Low-level programming language.
    - Symbolic representation (mnemonics) of machine-level instructions.
    - Hardware specific programs (not portable).
- **G3: High-level language:**
    - Processor independent.
    - Can be converted to machine language for different processor architectures using compliers and interpreters.
- **G4: Very High-level language:**
    - Take natural language-based statements one step further.
    - Amount of required code is less compared to previous generation languages.
    - Have been developed to be user by inexpert users.
- **G5: Natural languages:**
    - The goal is to create software the can solve problems by itself instead of programmer having to develop code to deal with individual and specific problems.

- Works like black box.
- Use advanced knowledge-based processing and AI (eliminate the need of the programing expertise).

Assemblers converts assembly language source code into machine code.

Compliers converts high-level language statements into the necessary machine-level format (.exe, .dll) for specific processors to understand (develop once and compile for various platforms).

Interpreters:

- Interprets the application's code into processor-specific code at run-time.
- Improve portability.
- Java source code is compiled into a **bytecode**. Once code wants to run, a JVM started and has an interpreter specific for the platform it is installed on (converts bytecode into a machine-level code).
- **Advantages:** platform independence and memory management functions are part of it.
- **Disadvantage:** cannot run as standalone as it requires the interpreter to be installed on the local machine.

Programs written in the **C language** could be vulnerable to buffer overrun and format string errors.

Java performs automatic garbage collection. **C** requires the developer to perform memory management manually.

Garbage collection:

- Identifies blocks of memory that were used and no longer required and mark them as free.
- Gathers scattered blocks of free memory and combines them into larger blocks.

OOP works with classes and objects.

An **object** is an instance on a class.

Method is the functionality or procedure an object can carry.

Objects **encapsulate** the attributes values.

Object can have a shared portion and private portion.

The shared portion is the *interface (API)*.

The private portion offers *data hiding*.

Objects can be catalogued in a library. The library holds pointers to where the object is living within the system or on another system.

Benefits of OOP:

- **Modularity:** autonomous objects cooperating through **the** exchange of messages.
- **Deferred commitment:** internal components of an object can be redefined without changing other parts of the system.
- **Reusability**
- **Naturalness:** modeling map to business needs.

Polymorphism is where two objects can receive the same input and have different outputs (*overloading* and *overriding*).
Object-oriented analysis (OOA) is the process of classifying objects that will be appropriate for a solution. A problem is analyzed to determine the classes of objects to be used in the application.

Object-oriented design (OOD) creates a representation of a real-world problem and maps it to a software solution using OOP.

Data modelling: OOA and databases are example of data modelling (e.g. attributes and relationships).

Data structure:

- A representation of the logical relationship between elements of data.
- Can be: scalar, array, hierarchical.

Cohesion:

- how many different types of tasks a module can carry out.
- If a module carries out only one task, or very similar tasks, it is having **high cohesion** (*good*)**.**
- The higher the cohesion, the easier to update/modify a module without affecting other modules.
- Easier to reuse and maintain.

Coupling:

- Measurement that indicates how much interaction one module requires to carry out its tasks.
- High (tight) coupling means a module depends upon many other modules to carry its tasks.
- Lowe coupling is **good**.

API specifies how software components interacts with other software components.

Software library is a collection of components that do specific things that are useful to many other components.

Distributed Computing Environment (DCE):

- It is a client/server framework developed by Open Software Foundation (OSF).
- DCE provides a Remote Procedure Call (RPC) service, security service, directory service, time service, distributed file support.
- Set of management services with communication layer based on RPC.
- Uses *universal unique identifier (UUID)*.
- Mainly for Unix-based environmnets.

Distributed Component Object Model (DCOM):

- Same functionalities as DCE.
- Uses *globally unique identifier (GUID)*.
- Developed by Microsoft (more proprietary).
- Evolved into .NET framework.

Common Object Request Broker Architecture (CORBA):

- Open object-oriented standard architecture.
- Defines the APIs, communication protocols, client/server communication methods.
- Enables applications to communicate no matter the location of the application.
- In this model, clients request services from objects. Clients pass a message that includes the name of the object, the requested operation, and parameters.
- It contains 2 parts:
  - *System-oriented components (object request brokers ORB and object services).*
  - *Application-oriented components (application objects and common facilities).*
- ORB is the middleware that allows the client/server communication to take place between objects residing on different systems.
- ORB receive the request from the requested object, locating the necessary object, sends the request with parameters, and return the result to the client.

COM and DCOM:

- COM allows for inter-process communication within one application, or between applications within the same computer system.
- Developed by Microsoft.
- DCOM is for distributed computer systems (access objects that resides in different part of the network).

Object Linking and Embedding (OLE):

- Provides a way for objects to be shared on local personal computer and to use COM as their foundation.
- Enables objects (e.g. graphics, clipart, spreadsheets) to be embedded into documents.
- **Linking** is the capability of one program to call another program.
- **Embedding** is the capability to place a piece of data inside a foreign program/document.

Java Platform, Enterprise Edition (Java EE):

- Client/server model that is object-oriented and platform independent.
- Its inter-process communications are based upon CORBA.
- Java EE application server can handle scalability, concurrency, transactions, security for the client.
- Focus on let developers focus on business logic.
- **Enterprise JavaBeans (EJB)** is a structural design for the implementation of distributed applications written in Java.

Directory service when given a name, it returns the network address of the resource.

Service-Oriented Architecture (SOA):

- Application functionality is separated into different distinct units (services) and offered through well-defined interfaces and data-sharing standardization.
- It is amore *web-based approach*.
- An entity that will provide a service in a SOA environment, sends a service description document to a *service broker*.
- The *service broker* map all the services available.
- When an application needs a specific service, it makes a call to the broker, which points the application to the necessary service provider.
- A ***web service*** allows for web-based communication to happen seamlessly using web-based standards:
    - **Simple Object Access Protocol (SOAP):**
        - an XML-based protocol that is used to exchange messages between a requested and provider of a web service.
        - SOAP sent over HTTP
    - **Web Services Description Language (WSDL):**
        - provides a machine-readable description of the specific operations provided by the service.
    - **Universal Description, Discovery and Integration (UDDI):**
        - an XML-based registry that lists available services.
        - It provides a method for services to be registered by service providers and located by service consumers.
        - Provides mechanisms to allow businesses around the world to publish their services and others to discover and use these services.
    - **HTTP**
    - **Extensible Markup Language (XML)**

Mashup is the combination of functionality, data, and presentation capabilities of two or more sources to provide some type of new service or functionality.

Mobile code: a code that can be transmitted across a network, to be executed by a system or device on the other end (e.g. web browser applets: to watch video or download more contents).

Java applet are small components that run in a user's web browser.

JVM is created to run the Java program or applet in a ***sandbox***. Bad guys figured out how to escape the confines and restrictions of the sandbox.

ActiveX:

- Microsoft technology composed of a set of SOA technologies and tools based on COM and DCOM.
- Programmers can create *ActiveX controls* (similar to Java applets) the can be executed in Windows environment.
- These controls can be *automatically* downloaded from websites to add extra functionality. Also, they are also components of Windows OS itself.
- Allow web browsers to execute other software applications within the browser (e.g. play media files, open PDF).
- The problem lay in the fact that ActiveX controls shared the privilege levels of the current user on a system.
- ActiveX control can download further ActiveX components without user authentication.
- Comes with a *component container* feature that allows multiple applications and networked computers to reuse active components.
- Unlike Java applets, ActiveX components are downloaded to the hard drive when user chooses to add the functionality the component provides.
- Security level of the web browser dictates if the ActiveX component can be downloaded automatically, or the user is first prompted with a warning.
- The main security different between Java applets and ActiveX controls is that Java sets up a sandbox for the applet code to execute in, while, ActiveX uses *Authenticode* technology, which relies on digital certificates and trusting certificate authorities.
- *Authenticode* doesn't necessarily provide security.

Using a **web-based administrative interface** is a **bad idea**.

The most **secure management interface** is **out-of-band**.
Usernames and passwords the the most common access control mechanism to web applications.

Uniform Resource Location (URL): http://www.google.com/?q=cissp

Input validation attacks:

- **Path or directory traversal:** ../../
- **Unicode encoding:** path traversal can happen without the need to enter "/" character, the attacker can use the Unicode representation of that character "%c1%qc").
- **URL encoding:** *space* got represented by "%20" because *space* is not allowed in a URL. Attackers represents characters differently to bypass filtering techniques.

SQL injection: instead of valid input, the attacker puts actual database commands into the input fields.

Cross-site scripting (XSS):

- An attacker discovers and exploits a vulnerability on a website to inject malicious code into a web application.
- Malicious code executes on the victim's browser and my lead to: stolen cookies (session hijack), malware execution, bypass access control.
- **XSS types:**
  - **Non-persistent XSS (reflected vulnerabilities):** Exploits the lack of proper input or output validation on dynamic sites.
  - **Persistent XSS (stored or second order):** Attacker posts some text that contains some malicious JavaScript, and when other users view the posts, their browsers render the page and execute the attacker's JavaScript.
  - **DOM-based XSS (local XSS):** Attacker uses the DOM environment to modify the original client-side JavaScript.

Parameter validation where the values that are being received by the application are validated to be within defined limits before the server application processes them within the system.

Parameter validation vs. Input validation:

- Input validation is validating values received by the user.
- Parameters values is also validating the values defined in the system (beyond user's reach).

Web developers uses cookie to help server remember things of the state of the connection (**session cookie**), or store details of the session locally in a file (**persistent cookie**).

Common Gateway Interface (CGI) is used to respond dynamically to inputted data.

Web proxy:

- A piece of software installed on a system that is designed to intercept all traffic between the local web browser and the web server (e.g. Burp Suite).
- Attacker could monitor and modify information as it travels in either direction.
- Exploits the user of hidden fields in web pages.

Per-validation: input controls verifying data in in appropriate format prior to submission to the application (e.g. form validation).

Post-validation: ensuring an application's output is consistent with expectation.

Session management:

- Most commonly used technique is to assign a unique ID (***session ID***).

- Using sequential session ID for clients is a mistake (attacker can guess and hijack a session).
- Usage of timestamp or time-based validation will combat **replay attacks**.

In event of an error, websites ought to be designed to behave in a predictable and non-comprising manner (**failing securely**), but showing friendly error messages without revealing internal system details.

Database management system (DBMS) is a suite of programs used to manage large sets of structured data with ad hoc query capabilities for many types of users. It can also control the security parameters of the database.

Transaction persistence means the database procedures carrying out transactions are durable and reliable.

Database models:

- **Relational:**
  - Attributes (columns) and Tuples (rows)
  - 2-d tables
  - primary key links all the data within a record to a unique value.
- **Hierarchical:**
  - Combines records and fields that are related in a logical tree structure.
  - The parents can have one child, many children, or no children.
  - Useful to mapping one-to-many relationships.
  - Not as flexible in creating relationships between data elements as in relational database.
  - Employs when building indexes for relational databased. An index can be built on any attribute and allows for very fast searches of the data over that attribute.
  - Most commonly used in **Lightweight Directory Access Protocol (LDAP).**
- **Network:**
  - allows each data elements to have multiple parent and child records.
  - Forms a redundant network-like instead of strict-tree structure.
  - Allows for quick retrieval of data compared to the hierarchical model.
  - Uses a construct of *records* and *sets*:
    - A record contains fields.
    - Sets define the one-to-many relationships between the different records.
- **Object-oriented:**
  - Handles a variety of data types (images, audio, documents, video).
  - More dynamic as objects can be created when needed and the data and methods go with the object when it is requested.
  - Has classes to define the attributes and procedures of its objects.
  - When application queries for some data, data and a code that can carry out procedures on this data are returned
  - Doesn't depend upon SQL for interactions.

- **Object-relational:**
  - A relational database with a software front end that is written in an object-oriented programming language.
  - The front end provides the procedures (methods) that can be carried out on the data, then each and every application that accesses this database doesn't need to have the necessary procedures.

Database programming interfaces:

- **Open Database Connectivity (ODBC):**
  - API that allows an application to communicate with the database (locally or remotely).
  - Application sends requests to the ODBC API, which translates the requests into the database commands that a specific database will understand.
- **Object Linking and Embedding Database (OLE DB):**
  - Separates data into components that run as middleware on a client or server.
  - Replacement for ODBC.
- **ActiveX Data Objects (ADO):**
  - API that allows applications to access back-end database systems.
  - It's a high-level data access programming interface to an underlying data access technology (uses OLE DB).
  - It's a set of COM objects for accessing data sources, not just database access.
  - It allows a developer to write programs that access data without knowing how the database is implemented.
  - SQL commands are not required to access a database when using ADO.
- **Java Database Connectivity (JDBC):**
  - API that allows a Java application to communicate with a database.
  - The application can bridge through ODBC or directly to the database.

Relational database components:

- **Data definition language (DDL):** defines the structure and schema of the database.
- **Data manipulation language (DML):** contains all the commands that enable a user to view, manipulate, a user the database (view, add, modify, sort, delete).
- **Query Language (QL):** enables users to make requests of the database.
- **Report generator:** produces printouts of data in a user-defined manner.

Data dictionary:

- A central collection of data element definitions, schema objects, and reference keys.
- The schema object can contain tables, views, index, procedures, function, triggers.
- A data dictionary can contain default values of columns, integrity information, the name of users, privileges and roles of users, auditing information.
- A tool to manage data about data (e.g. *metadata*).
- Different view settings for each user are held within the data dictionary.

Database can run into **concurrency problems** when there is data that will be accessed and modified at the same time by different applications/users.

To ensure no concurrency problems happen, **software lock** can lock the table within the database until the change happens, then release the lock.

Database software performs 3 main types of integrity services:

- **Semantic integrity:** makes sure structural and semantic rules are enforced. These rules pertain to data types, logical values, uniqueness constraints.
- **Referential integrity:** if all foreign keys reference existing primary keys. The database must not contain unmatched foreign key values.
- **Entity integrity:** guarantees that the tuples are uniquely identified by primary key values.

Operations that help protects the integrity of the data within the database:

- **Rollback:**
  - Operations the ends a current transaction and cancels the current changes to the database.
- **Commit:**
  - Completes a transaction and executes all changes just made by the user.
  - Changes can be made to the data or schema information.
- **Savepoints:**
  - Used to make sure that if a system failure occurs, or if an error is detected, the database can attempt to return to a point before the system crashed or hiccupped.
  - Having too many savepoints can degrade the performance.
  - Can be initiated by:
    - Time intervals
    - Specific action by the user
    - Number of transactions or changes made
- **Checkpoints:**
  - very similar to savepoints.
  - When a database software fills up a certain amount of memory, a checkpoint is initiated, which saves the data from the memory segment to a temporary file.
  - If a glitch experienced, the software will try to use this information to restore the user's working environment to its previous state.
- **Two-phase commit:**
  - Many times a transaction will require more than one database by updated during the process (either each database is properly modified, or no modification takes place).
  - A transaction monitor will send out a "***pre-commit***" command to each database.
  - If all databases respond with an ***acknowledgement***, then the monitor sends out a "**commit**" command to each database.
- **Batch processing**:

- Requests for database changes are put into a queue and activated all at once (not the exact time the user makes the request).

Database views: permit one group, or a specific user, to see certain information while restricting another group from viewing it altogether.

Database can employ **DAC** or **MAC** access controls.

Database Polyinstantiation: enables a table that contains multiple tuples with the same primary keys, with each instance distinguished by a security level (prevents *inference attacks*).

Online Transaction Processing (OLTP):

- Generally used when databases are clustered to provide fault tolerance and higher performance.
- Provides mechanisms to watch for problems and deal with them when they occur.
- Ensure that transactions either happed properly or don't happen at all.
- **ACID** test characteristics:
  - **Atomicity:** ensures that all modifications take effect or none takes effect.
  - **Consistency:** ensures all data is consistent in the different databases.
  - **Isolation:** transactions execute in isolated until completed, without interacting with other transactions.
  - **Durability:** once the transaction is verified, it is committed and the databases cannot be rolled back.

Data warehousing:

- Combines data from multiple databases or data sources into a large database for the purpose of providing more extensive information retrieval and data analysis.
- Data is **normalized** (redundant information is stripped out and data is formatted in the required format).
- Related pieces of data are summarized and correlated before being presented to the user.

Datamart:

- Collection of data from different databases or systems that fulfill a specific need (subset of data warehouse).

Data mining:

- The process of massaging the data held in the data warehouse into more useful information.
- It finds an association and correlation in data to produce *metadata*. Revealing unseen relationships or abnormal patterns (such data must be highly protected).
- Look at complex data and simplify it using fuzzy logic (a set of theory) or expert systems (uses AI).
- Also knows as ***Knowledge Discovery in Database, KDD.*** These approaches are used in KDD systems to uncover patterns:

- **Classification:** group data according shared similarities
- **Probabilistic:** identifies interdependencies and applies probabilities to relationships.
- **Statistical:** identifies relationships between data elements and uses rule discovery.

Expert systems uses:

- Knowledge base filled by experts.
- Inference engine to create metadata of the data in the knowledge base.
- Rule-based programming (e.g. if/then).

Neural network can deal with different situations and data (can learn) (e.g. Artificial Neural Network ANN).

Big data:

- A very large data sets with characteristics that make them unsuitable for traditional analysis techniques.
- Includes heterogeneity, complexity, variability, lack of reliability, and sheer volume.

95% of all compromises use **email** as the principal **attack** vector.

Some **malware stored in the RAM** and not a hard drive (difficult to detect).

Malware can be installed in a "**drive-by download**" process (victim is tricked into clicking something malicious).

Viruses:

- a small application, or string of code, that infects software.
- It reproduces and deliver its payload and require a host application to do this. If is cannot self-replicate they don't fall into the category of viruses.
- It infects a file by inserting or attaching a copy of itself to the file.
- Examples: ILOVEYOU, Melissa, Naked Wife (uses Outlook or Outlook Express as host).
- **Marco virus** is a virus written in one of micro languages (Visual Basic, VBScript) and is platform independent. It is extremely easy to write.
- **Boot sector viruses** infects the boot sector by either move data within the boot sector or overwrite the sector with new information (initiates the virus when a system boots up). The rest of their code in sectors on the hard drive that the virus has marked off as bad (they'll not get overwritten).
- **Stealth virus** is a virus that hides its tracks after infecting a system.
- **Polymorphic virus** produces varied but operational copies of itself (e.g. using different encryption algorithms, different action sequence, include *noise*, use mutation engine and random-number generator for randomization).

- **Multipart virus** has several components to it and can be distributed to different parts of the system (e.g. infects the boot sector and the hard drive).
- **Meme virus** is not a computer virus, but types of email messages that are continually forwarded around the internet (replicated by human and not software).
- **Script viruses** are files that are executed by an interpreter (written in VBScript and Jscript).
- **Tunneling virus** attempts to install itself "under" the antimalware program. When antimalware makes a request to the OS to gather this information, the tunneling virus can intercept this call and reply that everything is fine.

Stealth virus vs. Tunneling virus:

- Stealth virus is a general term of virus that hides its activities. It can uses tunneling technique to perform that.

Malware components:

- **Insertion:** insert itself on the victim's system
- **Avoidance:** avoids detection
- **Eradication:** removes itself after the payload has been executed
- **Replication:** makes copy of itself and spreads to other victims
- **Trigger:** uses an event to initiate its payload execution
- **Payload:** carries out its function

Worms:

- Can reproduce on their own without a host application (self-contained programs).
- Used to transport and deliver malicious payloads.
- **Example:** Stuxnet

Rootkit:

- a bundle of tools that first this usually do is installing a back-door program.
- Other tools within the rootkit used for: credentials capturing, sniffing, covering tracks.
- Replaces itself with default system tools It acts as Trojaned programs, because it carries out the intended functionality and the malicious activities in the background.
- **Log scrubbers:** removes traces of the attacker's activities from the system logs.
- Powerful rootkits update the kernel of the system (very difficult to detect). Re-installation of the OS may be the only solution.

Spyware: gathers sensitive information about the user (e.g. logging keystrokes, taking screenshots).

Adware: a software that automatically generates (renders) advertisements (e.g. through pop-ups, user interface components).

Botnets:

- **Bots** are type of malware and are being installed on thousands of computers. It usually lies dormant (zombie code) and waits for command instructions for activation purposes.
- The owner of the botnet called **bot herder**.

- Usually communicated through Internet Relay Chat (IRC) protocol.
- Can be used for legitimate purposes (e.g. web crawling).
- Command & Control server manages the bots.

Fast flux:

- An evasion technique. Botnets can use fast flux functionality to hide the phishing and malware delivery sites they are using. One common method is to rapidly update DNS information to disguise the hosting location of the malicious websites.

Logic bomb:

- Executes a program, or string of code, when a certain set of conditions is met (e.g. time and date, after a user carries out a specific action, if forensics activities started).

Trojan Horses:

- A program that is disguised as another program (e.g. can be names Notepad.exe).
- When a user executes Notepad.exe, the program deletes system files.
- Perform useful information, as well as, malicious functionality in the background.
- **Remote Access Trojans (RATs)** are malicious programs that run on systems and allow intruders to access and user a system correctly (e.g. Sakula, KjW0rm, Havex, Dark Comet).

Crimeware Toolkits:

- Can be purchased from the black market.
- Allow hackers to create their own tailored malware through a GUI.
- It provides pre-developed malicious code that can be easily customized, deployed, and automated.

Antimalware Software:

- Traditional malware uses *signatures*.
- Scans files, email messages, an other data passing through specific protocols.
- Some antimalware created a virtual machine (sandbox) to assess the code (*emulation buffer*).
- **Signature-based detection** (*fingerprint detection*) is effective way to detect conventional malware, but there is a delayed response time to new threats.
- **Heuristic detection** analyzes the overall structure of the malicious code, evaluate the coded instructions and logic functions. It collects information about the code and assesses the likelihood of it being malicious in nature (e.g. uses *suspiciousness counter*).

Behavior blocking antimalware allows the suspicious code to execute within the OS unprotected and watches its interactions with the OS.

1st generation behavior blockers only looked for individual actions.

Newer generation behavior blockers analyze sequences of these types of operations.

Proactive and can detect new malwares: Heuristic detection and Behavior blocking.

Reputation-based protection: vendor collects data from many customers and mines the data to identify good and bad files. Each file is assigned a **reputation metric value**.

Diskless workstations are still vulnerable as *viruses can resides in memory*.

Immunizer:

- Attaches code to the file or application, which would fool a virus into "thinking" it was already infected (e.g. would make a file or application looks as it has been infected).
- The challenge is that the immunizer is virus specific.

Spam detection:

- **Bayesian filtering** reviews prior events to predict future events, which is basically quantifying uncertainty. It carries out a frequency analysis on each word and then evaluates the message as a whole to determine it is spam or not.
- Spams eats up a lot of network bandwidth.
- Can be the source of spreading malware.

Antimalware files that contain updates (new signatures) are called **DAT files** (.dat).

The scanning software can be integrated into a mail server, proxy server, or firewall (e.g. virus walls). It can scan SMTP, HTTP, FTP, and other protocol types.

EICAR test is a file used to test the configurations of the antivirus software package.

Pseudo-flaw is code inserted into an application or OS with the sole purpose to trap intruders who break into these systems.

Smurf attack is a DDoS in which large number of **ICMP packets** with the intended victim's spoofed source IP are broadcast to a network using an IP broadcast address. Most of devices will respond by reply to the source IP address.

Fraggle attack is similar to Smurf attack but uses spoofed **UDP traffic**.

Teardrop attack is a DoS attack where an attacker is sending fragmented packets to a target machine, and let the victim unable to reassemble the fragmented packets.

Good Luck!