CSI 4139

Secure Computer Systems

Fall 2024

Study Guide

Computer Security Concepts

- Computer Security: Generic name for collection of tools designed to protect data and to thwart hackers
- Internet security: consist of measures to deter, prevent, detect, and correct security violations that involve the transmission of information

CIA Triad

- Confidentiality: Covers 2 related concepts
  - Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals
  - Privacy: Assures individual's control or influence on what information related to them may be collected and stored and by whom and to whom that information may be disclosed
- Integrity: Covers 2 related concepts
  - Data integrity: Assures that information and programs are changed only in a specified and authorized manner
  - System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
- Availability: Assures that systems work promptly, service is not denied to authorized users

Additional Concepts

- Authenticity: Verifying that users are who they say they are and that each input arriving at the system came from a trusted source
- Accountability: Security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

Threats

- Computer security is concerned with safeguarding assets, which include information, software, hardware, and services provided by computing and communication systems
- A threat refers to any situation or entity that could potentially harm these assets or lead to security breaches

Risks

- Potential loss that may occur due to future harmful events
- Depends on several factors:
  - Threat agent
  - Likelihood of an attack
  - Potential losses

Risk Assessment

- Quantitative: calculating numerical estimates of risk
- Qualitative: comparing and ranking risks relative to each other

Security Policies

- Policy typically includes:
  - assets that need protection
  - specific users authorized to access assets
  - means of access allowed
  - Security services
  - controls

Security Mechanisms

- Tools used to enforce security policies and services
- Ensure protection of assets and prevent unauthorized access by implementing measures

Passive Attacks

- Eavesdropping of information
- Goal is to obtain information being transmitted
- Two types:
  - Release of message contents
  - Traffic analysis

Active Attacks

- Involve some modification of the data stream or creation of a false stream
- Difficult to prevent because of wide variety of vulnerabilities

Types of Threats

- Internal Threats
  - Insider Threats: Malicious actions by authorized individuals
  - Accidental Errors: Human mistakes leading to security breaches
- External Threats
  - Hackers: individuals or groups with malicious intent
  - National-State Actors: Governments targeting critical infrastructure
  - Organized crime: Criminal groups seeking financial gain
- Natural Threats
  - Disasters: natural events that can disrupt operations
- Technological Threats
  - Internet of Things: Vulnerabilities in connected devices
  - Cloud Security: Threats specific to cloud-based environments
  - Supply Chain Attacks

Threat Modelling

- Identify Assets
- Identify Threats
- Analyze Vulnerabilities
- Prioritize Risks
- Develop Mitigation Strategies

STRIDE

- Spoofing: False identity
- Tampering: Unauthorized modification of data
- Repudiation: Denying involvement in an action
- Information Disclosure: Unauthorized access to sensitive information
- Denial of Service: Preventing legitimate use of a system
- Elevation of Privilege: Gaining unauthorized access to resources

DREAD

- Damage: Potential harm caused by the threat
- Reproducibility: How easily can the threat be repeated
- Exploitability: The ease of exploiting the vulnerability
- Affected users: The number of people impacted by the threat
- Discoverability: How likely is the threat to be discovered

Controls

- The ways to address committed, or possible attacks
- The ways to protect systems
- Actions, devices, procedures, or techniques that reduce or remove vulnerabilities

Vulnerabilities

- A weakness or flaw in a system, application, or network that can be exploited by a malicious actor to gain unauthorized access or control
- Technical Vulnerabilities:
  - Software vulnerabilities
  - Hardware vulnerabilities
  - Configuration vulnerabilities
- Operational Vulnerabilities: Arising from poor security management, such as improper credential management, lack of patches, or weak encryption protocols
- Human Vulnerabilities: Resulting from social engineering, such as phishing or insider threats

Vulnerability Lifecycle

- Discovery: Vulnerabilities can be discovered by researchers, threat actors, or through routine testing
- Disclosure: Once a vulnerability is found, it is typically reported to the responsible vendor or organization
- Patching: A fix or patch is developed and applied to mitigate the vulnerability
- Code Reviews: Regular analysis of software code to identify and fix vulnerabilities before deployment

Security Testing: Conducting penetration tests and vulnerability assessments to identify weaknesses

Exploiting

- Zero-Day Exploits: Exploits that take advantage of vulnerabilities unknown to the software vendor, meaning no patch or fix is available at the time of the attack
- Remote Exploits: Designed to attack vulnerabilities over a network without physical access to the system
- Local Exploits: Require the attacker to have some form of access to the system. Once they gain access, they can use exploits to gain control over higher-level functions

Mitigation Strategies

- Intrusion Detection and Prevention Systems: Systems designed to detect malicious traffic associated with exploits and prevent them from compromising systems
- Zero-Day Protection: Using machine learning and anomaly detection to identify potential zero-day exploits
- Regular Updates and Patch Management: Patching known vulnerabilities to prevent exploits from being effective

Attack Surface

- Network Attack Surface: Includes all the vulnerable points where attackers can interact with the network
- Software Attack Surface: Includes the code vulnerabilities in the software
- User behaviour: User actions and practices can create additional attack surfaces
- Third-party components: Dependencies on external software or services can introduce vulnerabilities
- Physical attack surface: Refers to the physical locations where an attacker can gain access to infrastructure, including data centres, servers, and workstations

Mitigation Strategies

- Reduce unnecessary features
- Network Segmentation: isolating sensitive parts of network to limit scope of attack
- Minimizing Priveleges: Limiting privileges to minimize potential for exploitation

Layered Security

- Employing various security controls at different levels of the system
- Physical Security: Protecting hardware through locks, surveillance, restricted access
- Network Security: Firewalls, intrusion detection/prevention systems, network segmentation
- Endpoint security: Ensuring devices such as laptops and mobile phones are protected with antivirus software and encryption
- Application Security: Implementing security best practices in coding
- User awareness and policies: Educating users about security risks, enforcing strong password policies, and applying least-privilege principles to minimize access to sensitive systems

Cryptography Terminology

- Encryption: The process of encoding a message so that its meaning is not obvious
- Decryption: The reverse process, transforming an encrypted message back into its original form
- Cryptosystem: System for encryption and decryption

$c = E(p)$, $p = D(c)$

  - c ciphertext
  - p plaintext
  - E encryption algorithm
  - D decryption algorithm
- Want: $P = D(E(P))$
- Encryption and decryption algorithms often use a set of keys, k. Then we have $c = E(k, p)$
- Symmetric encryption: encryption and decryption keys are the same
- Asymmetric encryption: decryption key inverts the encryption of encryption key

$P = D(k_D, E(k_E, P))$

- Cryptanalyst: a person who studies encryption and ciphertexts to figure out the corresponding plaintexts
- Breakable Encryption: given enough time and data, an analyst can determine the algorithm
- Theoretically breakable $\neq$ Practical to break

Substitution Ciphers

- Mono-alphabetic: fixed substitution over the entire message
  - Caesar Cipher (shifting the alphabet)
  - Atbash Cipher (reversing the alphabet)
- Poly-alphabetic: uses a number of substitutions at different positions in the message
  - Vigenere Cipher
  - Enigma machine
- Not secure to use
- Good to know and use as building blocks in other encryption methods
- Main goal: confusion
- Complexity proportional to number of characters

One-Time Pads

- Length of key should be the same as that of the plaintext message
- Issues
  - Synchronization between sender and receiver
  - Unlimited number of keys
- Perfect Secrecy: Ciphertext gives absolutely no additional information about plaintext

Transpositions

- Permutation
  - Reordering of the characters of the plaintext
  - One way is to use a key to control the permutation
- Goal: Diffusion
  - Widely spreading the information from the message or the key across the ciphertext
- Time needed proportional to length of message

Good Ciphers

- Amount of secrecy needed should determine the amount of labor appropriate for encryption and decryption
- Set of keys and enciphering algorithm should be free from complexity
- Implementation should be as simple as possible
- Errors in ciphering should not propagate and cause corruption of further info
- Size of ciphertext should be no larger than text of original message

Trustworthy of Encryption Systems

- Based on sound mathematics
- Been analyzed by competent experts and found to be sound
- Stood the "test of time". Flaws in many algorithms discovered relatively soon after their release
- Three popular cryptosystems:
  1. Data Encryption Standard (DES)
     - Older, symmetric encryption standard, now considered insecure due to short key length
  2. Rivest-Shamir-Adelman (RSA)
     - Widely used and secure symmetric encryption standard with key sizes 128, 192, or 256 bits
  3. Advanced Encryption Standard (AES)
- DES and RSA meets all 3 criteria
- AES meets first 2 criteria

Stream and Block Ciphers

- Stream Cipher: Converts one symbol of plaintext immediately into a symbol of ciphertext
  - Transformation depends only on the symbol, the key, and the control information of the algorithm
  - Skipping a character in the key during encryption affects enoyption of all future characters
- Block cipher: A group of plaintext symbols are encrypted as one block

Confusion and Diffusion

- Confusion: The interceptor should not be able to predict what will happen to the ciphertext by changing one character in the plaintext
- Diffusion: The cipher should also spread the information from the plaintext over the entire ciphertext.

Cryptoanalysis

- Four types of information
  - Ciphertext
  - Full Plaintext
  - Partial Plaintext
  - Algorithm
- Five approaches
  - Ciphertext only
  - Full or partial plaintext
  - Ciphertext of any plaintext
  - Algorithm and Ciphertext
  - Ciphertext and Plaintext

Attacking the Cipher

- Exhaustive Search
  - Try all possible keys
- Statistical Analysis
  - Compare to 1-gram model of English

Encryption Systems

- Symmetric Cryptosystem
  - Two-way channel to their users: A and B share a secret key, and they can both enrypt info to send to the other as well as decrypt information from the other
  - Difficulty: key distribution
- Asymmetric Cryptosystem
  - Two separate keys
    - Public key for encryption
    - Private key for decryption

Data Encryption Standard

- Has following criteria:
  - Able to provide a high level of security
  - Specified and easy to understand
  - Publishable
  - Available to all users
  - Adaptable for use in diverse applications
  - Economical to implement in electronic devices
  - Efficient to use
  - Able to be validated
  - Exportable

Advanced Encryption Standard

- Algorithms have to be
  - Unclassified
  - Publicly disclosed
  - Available royalty-free for use worldwide
  - Symmetric block cipher algorithm for blocks of 128 bits
  - Usable with key sizes of 128, 192, and 256 bits

Public key Encryption

- Characteristics:
  - Each user has 2 keys: a public key and a private key
  - User may publish public key freely

$P = D(k_{priv}, E(k_{pub}, P))$

$P = D(k_{pub}, E(k_{priv}, P))$

RSA Encryption

- Operates with arithmetic mod n
- 2 keys, d and e, used for decryption and encryption, which are interchangeable
- Encryption: $c = p^e \bmod n$
- Decryption: $p = c^d \bmod n$

El Gamal Cryptosystem

- Relies on difficulty of computing discrete logarithms over finite fields
- Has similarities to RSA
- For given plaintext, ciphertext has 2 parts

Digital Signature

- A means of associating a mark unique to an individual with a body of text
- Mark should be unforgeable
- Mark should be verifiable

Secret Sharing

- Sharing a secret among a group of participants
- Secret can be reconstructed only when a sufficient number of shares are participated in the decryption process
- Shown by (t,n)-threshold, in which n is the total number of participants and t is the minimum number of required participants for secret reconstruction
- Any combination of fewer than t shares has no extra information about the secret than that with no share

SDLC Phases

- Design: Apply Secure Design Principles
  - Incorporate secure design principles to minimize vulnerabilities
  - Use techniques like threat modelling to identify potential security issues
- Implementation: Secure Coding Practices
  - Follow secure coding practices to prevent common flaws, such as input validation and proper error handling
  - Avoid using deprecated or insecure libraries
- Testing: Identifying and Fixing Vulnerabilities
  - Conduct security testing, including code reviews, penetration testing, and vulnerability scanning
  - Fix vulnerabilities before the software goes live
- Deployment: Implementing Security Measures
  - Implement security controls such as encryption, firewalls, and access management during software development
- Maintenance: Continuous Monitoring and Updates
  - Continuously monitor the software for new threats
  - Regularly update the software to address security vulnerabilities and emerging threats

Application Attacks

- Techniques used by attackers to exploit vulnerabilities in applications due to insecure coding practices
- Application layer is the hardest to defend against as other defences are not effective if the application does not implement secure coding practices.

Common Software Vulnerabilities

- Buffer Overflow:
  - Definition: Occurs when more data is written to a buffer than it can hold, potentially causing crashes or code execution
  - Prevention: Use languages with memory management or carefully check buffer boundaries
- SQL Injection
  - Definition: Inserting malicious SQL code into a query to manipulate the database
  - Prevention: Use parameterized queries and prepared statements to avoid executing harmful code
- Cross-Site Scripting (XSS)
  - Definition: Injecting malicious scripts into web pages viewed by other users
  - Prevention: Sanitize and escape user input and use Content Security Policy (CSP) headers
- Cross-Site Request Forgery (CSRF)
  - Definition: Tricking a user into performing unwanted actions on a website
  - Prevention: Use anti-CSRF tokens, SameSite cookies, and require re-authentication for sensitive actions

Static and Dynamic Code Analysis

- Static Code Analysis
  - Definition: Analyzes source code without executing it to identify vulnerabilities, code smells, and coding standard adherence
- Dynamic Code Analysis
  - Definition: Tests software during runtime to detect vulnerabilities that static analysis might miss
- Advantages of Code Analysis Tools
  - Early Detection: Identify vulnerabilities before deployment, reducing exploitation risks
  - Automated Scanning: Integrate tools into the development lifecycle for continuous security
  - Compliance: Ensure software meets industry security standards and regulations

Buffer Overflows

- Occurs when a program or process attempts to write more data to a fixed length block of memory than the buffer is allocated to hold
- Often happens due to lack of or poor input validation on the application side
- Malicious attacker can exploit this by sending a carefully crafted input to the application can cause execution of arbitrary code, possibly taking over the machine
- Buffer overflow can exist in any software
- Impact
  - Denial of Service
  - Arbitrary code execution
  - Privilege Escalation
- Input validation is a good countermeasure

Time to Check to Time to Use (TOCTOU)

- A race condition can occur if the state of the system changes between the moment when some condition was checked by a process and the moment when the action was taken based on that condition by the same process

Backdoors

- Any method by which authorized and unauthorized users are able to get around normal security measures and gain access on a computer system, network, or software application
- Sources
  - Malware
  - Application developers
- Countermeasures
  - Code review by peers
  - Effective Account management policies
  - MFA for privileged accounts
  - Review of logs

Escalation of Privileges and Rootkits

- Rootkit: Group of programs that hides the fact that the system has been infected or compromised by malicious code
- Once an attacker gets access to a standard account through either password attacks, social engineering or some other method, they use a rootkit to increase their access to a higher privilege user. This is called escalation of privilege
- Countermeasures
  - Apply latest patches to OS
  - Use MFA for higher privilege accounts

Cross Site Scripting (XSS)

- A web application is vulnerable to XSS when it accepts user input and reflects it back to the user browser without validating the input
- XSS attacks enables an attacker to inject malicious scripts into vulnerable web pages
- Attackers can use XSS to:
  - Steal authentication cookies
  - Trick the user into downloading malware on user system
  - Prompt user to enter password and send to third-party website
- Attackers can trick the user by:
  - Sending a malicious email with script embedded in a link
  - Fake page or form displayed to the user

Types of XSS

- Persistent XSS
  - malicious script entered by the malicious user is stored in the website's database
  - Impacts a large number of users and can happen multiple times
- Reflected XSS
  - Malicious script originates from the victim's request
  - Impacts only a single user
- Dom Based XSS
  - Vulnerability is on the client side
  - Malicious script is injected in the client side DOM directly without any server involvement
  - DOM: Document Object Model

XSS Countermeasures

- Input Validation
  - Always validate user input
  - Validate for type and length
  - Validate against a whitelist
- Output Encoding
  - prevents it from treated as code and getting executed
- Content Security Policy (CSP)
  - Allows user to define the trusted Sources from which the browser accessing the page can download resources

Cross Site Request Forgery (CSRF)

- An attack where an attacker tricks a web browser (user) into performing an unwanted action on a vulnerable web site to which the user is already logged in
- The attacker generally gets the user to click this malicious link by sending phishing email or some Social Engineering techniques
- As the user is already logged in, the web application is unable to distinguish a legitimate request from a forged one
- Web applications that use query strings to perform actions are at higher risk of CSRF
- Preconditions:
  - User already logged into target web application
  - User is logged into multiple websites at a time
- Countermeasures
  - Implement Anti-CSRF tokens
  - Re-authenticate user for critical transactions preferably using MFA
  - keep session cookie expiration/ session time out as short as possible
  - Same Site cookies

SQL Injection

- A vulnerability that allows an attacker to inject malicious SQL queries into SQL queries that an application makes to its database. This usually occurs due to lack of input validation by the developer
- SQL injection can be used to:
  - Access data which attacker is not authorized to
  - Extract metadata of database, structure of the tables, version etc
  - Modify/delete data
  - Bypass authentication in the login page
- Types of SQL injection:
  - Error based
  - Union based
  - Boolean based
  - Time based
- Error Based SQL Injection
  - Attacker performs actions that cause the database to throw error messages. The attacker can potentially use the data provided by these error messages to gather information about the structure of the database
- Union Based SQL Injection
  - Union-based SQL injection leverages the UNION SQL operator to combine the results of two or more SELECT statements into a single result which is then returned as part of HTTP response
- Time Based SQL Injection
  - Time based SQL injection relied on sending SQL query instructing the database to wait a specified amount of time before responding
  - If page is not vulnerable, it will load quickly
  - If it is vulnerable it will take longer than usual to load
  - This enables hackers to extract data
- Boolean Based SQL Injection
  - Relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns True or False
- Countermeasures
  - Input Validation
  - Using Prepared statements/ Parameterized queries and Stored Procedures
  - Least Privileged Accounts

Masquerading Attacks

- Attacks where attackers gain access to protected resources which they are not authorized to by impersonating a person/system who does have the appropriate access permissions
- Two common masquerading attacks
  - IP spoofing
  - Session Hijacking

IP Spoofing

- Two ways:
  - Change the IP of the system to the address of a trusted system and then gains access to the protected resources
  - Changing Source Address field in the IP packets using tools
- Countermeasures:
  - Implement adequate packet filtering

Session Hijacking

- An attack where a user session is taken over by an attacker
- Attacker needs to know the victim's session ID (session key)
- Can be obtained by
  - Stealing (XSS, Malware, MITM) the session cookie
  - Tricking the user to click a malicious link containing a prepared session ID
- Countermeasures:
  - Mark Cookies with "Http Only" and "Secure" flags
  - Enforce HTTPS to prevent attackers from intercepting traffic
  - Regenerate Session ID after initial authentication to prevent session fixation

Malicious Code

- Programs that spread malicious payload to other systems by exploiting vulnerabilities in networks, operating systems, software, and physical security
- Malicious Code spread in 2 ways:
  - Irresponsible computer use by humans
  - On their own
- Sources
  - Skilled malicious code writers
  - Script kiddies
  - Advanced Persistent Threat
- Skilled Malicious Code Writers
  - Extremely skilled software developers specializing in crafting innovative malicious code
- Script Kiddies
  - Individuals who don't understand the technology behind security vulnerabilities but downloads ready-to-use software (or scripts) from the internet and uses them to launch attacks against remote systems
- Advanced Persistent Threats (APT)
  - Sophisticated adversaries with advanced technical skills and significant financial sources
  - Often members of military units, intelligence agencies or shadow groups that are affiliated to Government agencies
  - Often have access to zero-day exploits that are not known to software vendors
  - Perform highly targeted attacks designed to impact only a small number of systems

Virus

- Malicious code written to perform two main functions:
  - Propagation: defines how the virus will spread from system to system infecting each system in turn
  - Destruction: destructive capabilities are delivered using the payload. This could be anything from breaking confidentiality, integrity, or availability of the systems or data
- Implement the above functions in innovative ways to escape detection by antivirus
- The damage caused can vary from displaying a simple message to complete destruction of all the data stored on the local hard drive

Virus Propagation Techniques

- By definition have inbuilt capabilities to spread to other systems
- Spread is aided by the need for computer users to share data by:
  - Exchanging disks
  - Sharing Networked Resources
  - Sending E-mail or some other means of exchange of data
- Once it reaches the new victim it uses one of the propagation techniques to infect the new system and use this to spread even further
- Viruses are mostly classified based on the propagation technique they use

Types of Virus

- Master Boot Record Virus
- File Infector Virus
- Macro Virus
- Service Injection Virus

Master Boot Record Virus

- MBR is the first sector of the media that is read in the initial stages of the boot process and the one a computer uses to load the operating system during the boot process
- MBR determines which media contains the operating system and based on that directs the system to read that partition's boot sector to load OS
- MBR virus attacks the MBR portion of bootable media like hard disk, USB drives, Compact Disc (CD) and Digital Versatile Disc (DVD)
- If the infected media is in the drive during the boot process, the target system reads the infected MBR which loads the virus into memory, infects the MBR on the target system's hard drive and spreads its infection to other machines

File Infector Virus

- Infects the executable files
- Triggers when the files are executed
- Implants the propagation code into the executable in two ways
  - Alter the code of the executable program
  - Replace the entire file with the infected version
- Easily detected by comparing file characteristics before and after the infection or comparing hash values

Companion Virus

- A variation of File Infector virus
- Escapes detection by using file names which are similar to legitimate files but have a different extension

Macro Virus

- Virus written in macro language
- Embedded in the macros associated with excel sheets and word documents
- Executed automatically when the infected file is opened
- Can infect any operating system as they are based on application rather than on operating system
- Accesses the files in the recipient's address book and sends an infected email to everyone on the contact list

Service Injection Virus

- Escape detection by injecting themselves into trusted runtime processes of the operating system
- Detection by antivirus is difficult as trusted processes are compromised
- keeping the system updated with latest patches helps protecting against this virus

Signature Based Detection

- Maintain extremely large database of characteristics of all known viruses
- When scans are started, it checks for files on the storage media that match these criteria
- When a match is found any one of the below actions can be initiated
  - Disinfect the file: If the antivirus can eradicate the virus, it does so and restores the machine to a safe condition
  - Quarantine the file: If the antivirus can recognize the virus but does not know how to disinfect the files, it may quarantine the files and let user or administrator examine them manually and perform the desired action
  - Delete the file: If security settings/policies do not provide for quarantine or the files exceed a predefined danger threshold, the antivirus package may delete the infected files in an attempt to preserve system integrity
- Are only as effective as the virus definitions
- Outdated definitions may not detect newly created viruses rendering it ineffective

Heuristic Based Detection

- This approach analyzes the overall structure of the malicious code, evaluates the coded instructions and logic functions to assess the likelihood of it being malicious in nature
- Static Heuristic Analysis:
  - Involves decompiling a suspect program and examining its source code and try to guess what the code does. If a particular percentage of the source code matches anything in the heuristic database, the code is flagged as a possible threat
  - This code may also be then compared to already known malwares to detect new variants
- Dynamic Heuristic Analysis
  - It evaluates the behaviour at run time. It allows the suspicious program or piece of code to run inside a specialized virtual machine - or sandbox.
  - It examines each command as it's activated and looks for any suspicious behaviours, such as sending out of multiple emails, modifying or observing keystrokes, attempting to alter host files, self-replication, overwriting files, and other actions that are common to viruses

Behaviour Blockers

- It analyses the behaviour of the code in real-time
- It monitors the ACTIONS performed by a program in real-time and steps in when it detects potentially malicious behaviour

- The first generation behaviour blockers only looked for individual actions, which resulted in a large number of false positives
- The newer generation behaviour blockers actually analyze sequences of these types of operations before determining the system is infected
- Can also detect rootkits

Virus Types - Propagation Technique

- Viruses can also be classified based on the technique used to escape detection
  - Multipartite Viruses
  - Stealth Viruses
  - Polymorphic Viruses
  - Encrypted Viruses

Multipartite Viruses

- Use multiple propagation mechanisms to spread between systems. This improves their likelihood of successfully infecting a system because it provides alternative infection mechanisms that may be successful against systems that are not vulnerable to the primary infection mechanism

Stealth Viruses

- A type of virus malware that contains sophisticated means of avoiding detection by antivirus software generally by hiding the modifications it has made to files or boot records
- Monitors the system functions used to read files or sectors from storage media and then forging the results of calls to such functions
- Programs that try to read infected files or sectors see the original, uninfected form instead of the actual, infected form
- Thus, the virus's modifications may go undetected by antivirus programs
- When the antivirus requests a copy of the Master boot record, the modified OS code will provide it with a clean version of the MBR which is free of any virus signatures. This tricks the antivirus into inferring that everything is fine. However, when the system boots, it reads the infected MBR and loads the virus into memory

Polymorphic Viruses

- Evade detection by creating a modified version of itself with different identifiable characteristics
- Change physical file makeup during each infection by encrypting its code with a different encryption key each time
- Renders signature based detection useless

Encrypted Viruses

- Use cryptographic techniques to avoid detection
- Two parts: a decryptor and the encrypted virus body
- May use variable encryption keys
- Decryptor remains the same

Logic Bombs

- Malicious code that is secretly inserted into a computer network, operating system, or a software application
- Primary goal: to steal or corrupt data, crash or gain control of user devices or completely wipe hard drive
- Not executed immediately
- Can be contained into any malicious code
- Also built into custom applications by software developers

Trojan Horse

- Trojan disguises itself as a legitimate software but carries a malicious payload behind the scenes
- User tricked into loading and executing Trojans on the device
- Used to take control of the device, damage systems, steal data and other harmful actions
- Trojan Malware and Trojan Virus are used interchangeably
- Viruses can execute and replicate by themselves but Trojans cannot

Types of Trojans

- Backdoor
  - Used to create backdoors on the target computers to give complete remote control to the malicious user
  - Often used to create a botnet or zombie network of victim computers that can be used for criminal purposes
- Rootkit
  - Primary objective is to prevent malicious programs from being detected
  - Provide complete control to the malicious users
  - Contains tools such as key loggers, bank credential stealers, antivirus disablers
- Trojan-DDOS
  - Infected systems perform DoS attacks against a targeted website
- Ransomware
  - Ransomware infects a target machine and then encrypts data on the computer
  - Attacker demands a ransom for decrypting the data

Worms

- Self-replicating program that can spread throughout a network without human assistance
- Viruses need a host computer or operating system. The worm program operates by itself
- Can modify/delete files, inject additional malicious software on the affected systems, steal data, install backdoors
- Mostly used to deplete system resources like hard drive space or network resources like bandwidth

Spyware and Adware

- Spyware
  - Malicious software code that runs secretly on a computer, gathers information about the user and their browsing habits, and then transmits that information back to a remote entity
  - Can monitor your internet activity, track login credentials, spy on sensitive information
- Adware
  - Malicious code that displays advertisements to generate revenue for the author
  - More nefarious versions may monitor your shopping behavior and redirect you to competitor websites

Access Control

- Process of granting or denying permission to access resources
- Types
  - Physical Access Control: Involves physical barriers that control and limit direct access to devices and sensitive areas
  - Technical Access Control: Uses technological solutions to restrict user access to data or systems
  - Standard Access Control Models

Access Control Terminology

- Identification: The process of claiming an identity by presenting credentials, allowing the system to recognize a user or entity
- Authentication: Verifies the identity by checking the validity of the credentials presented during identification
- Authorization: Grants permissions based on the identity's verified credentials, allowing the individual to take specific actions
- Accounting: keeps track of the actions performed, maintaining a log of who accessed the system, what they accessed, and when they disconnected
- Object: Represents a specific resource that is protected within the system
- Subject: A user or process that interacts with the object, typically functioning on behalf of a user
- Operation: The action taken by the subject on the subject, dictating the interaction between the two
- key roles in data privacy and security:
  - Privacy Officer: Manager responsible for overseeing data privacy compliance and managing data risks
  - Custodian or Steward: Individual assigned to perform day-to-day tasks by the owner
  - Owner: Person responsible for the data or information
  - End user: user who accesses data as part of their job responsibilities

Access Control Models

- Discretionary Access Control (DAC):
  - The resource owner decides who can access specific resources
  - Users can transfer permissions to others, allowing flexible management of access
- Mandatory Access Control (MAC):
  - Access is based on policies set by the system or organization, not by the users
  - Typically used in highly classified environments
- Role-Based Access Control (RBAC):
  - Access permissions are assigned based on user roles within an organization
  - Users inherit permissions based on their role, streamlining management
- Rule-Based Access Control:
  - Access is granted or denied based on pre-defined rules
  - These rules can be adjusted based on the context of the request, such as time of access or the device used
- Attribute-Based Access Control:
  - Access control is based on attributes
  - This allows for more flexible and fine-grained access control

Discretionary Access Control

- Least Restrictive Model: DAC is the least restrictive of the access control models. Every object has an owner, who has full control over the object
- Owner Control: Owners can decide who has permissions to access their objects and can transfer those permissions to other users
- Commonly used in OS: It is widely implemented in operating systems
- Weaknesses
  - User-Dependent: The system relies heavily on the end user to set the correct security permissions, which poses a risk if the user does not implement proper security measures
  - Inheritance of Permissions: Any programs executed by a user will inherit the user's permissions. This can lead to security vulnerabilities if malicious programs gain the same access rights as the user

Mandatory Access Control

- Most Restrictive Model: This model is the most restrictive among access control frameworks. It operates by entirely removing the user's ability to set permissions. Users cannot distribute access to other subjects
- Common in Military Settings: The MAC model is widely used in military or highly confidential environments where strict access control is essential
- Two Key Elements
  - Labels: Every entity, whether it is a subject or an object, is assigned a classification label. These labels represent the importance of the entity.
  - Levels: The labels operate within a hierarchy
- Permission Matching: MAC grants access by matching the subject's privilege label with the object's classification label. Only subjects with sufficient clearance can access higher-labeled objects
- Strict Labeling for Privilege: The access control is dictated by these labels, ensuring that only authorized personnel access sensitive information
- Comparison of Object and Subject Labels: In MAC, the subject's access to a file or resource is determined by comparing their labels with the object's labels
- Access Rules: For access to be granted, the subject's label must be equal to or greater than the object's classification label
- Two major implementations:
  - Lattice Model
    - Subjects and objects are assigned specific positions or "rungs" in a hierarchy
    - Access is based on this hierarchical structure, where multiple lattices can coexist
  - Bell-LaPadula (BLP) Model
    - Similar to the lattice model, but with stricter rules
    - BLP restricts subjects from creating new objects or performing functions on objects at lower security levels. This prevents data leakage to lower classification levels

Role-Based Access Control (RBAC)

- Definition: RBAC is a method of regulating access to resources based on the roles individuals have within an organization. It is sometimes referred to as Non-Discretionary Access Control because users do not have the discretion to set their own access priveleges
- Role Assignment: Access permissions are tied to specific roles within the organization, and users are assigned to roles based on their job functions.
- Permission Management: Permissions are centrally managed by administrators who assign them based on predefined roles, ensuring that only authorized users can access specific resources according to their responsibilities

Rule-Based Access Control

- Definition: A variation of Role-Based Access Control that dynamically assigns roles to users based on a set of predefined rules managed by a custodian
- Rule-Based Permissions: Each resource contains access rules. When a user attempts access, the system verifies these rules to determine if access is permitted
- Use Case: RB-RBAC is frequently employed to manage user access across multiple systems and is particularly useful when business changes triggers updates to the access control rules
- Dynamic Flexibility: This model ensures that access permissions can be adjusted dynamically based on the evolving rules of an organization

Attribute-Based Access Control

- Flexibility: ABAC provides more adaptable policies compared to Rule-Based Access Control (RBAC), allowing a combination of multiple attributes to determine access
- Attributes Used: The model can incorporate:
  - Object attributes
  - Subject attributes
  - Environmental attributes
- Conditional Rules: Policies in ABAC are commonly structured using "If-Then-Else" logic, enabling a high degree of granularity in access control decisions

Account Setup

- Best Practices:
  - Location-Based Policies: Implementing access control policies based on the geographical location of users, allowing or restricting access depending on where the login request is made
  - Standard Naming Conventions: Establish a consistent naming system for user accounts to maintain clarity and organization across the network, making it easier to manage and audit access
  - Time-of-Day Restrictions: Limit access based on specific times of the day or week
  - Least Privilege Enforcement: Assign users the minimal level of access necessary to perform their duties, preventing unauthorized or unnecessary access to sensitive data or systems.

Location-Based Policies

- Geofencing: A technique used to define geographical boundaries where mobile devices can or cannot be used. Ensures that devices are only operational in authorized areas
- IP Location Data: Geofencing often relies on IP location data to define these boundaries. Stored in a file.
- Policy Generation: This IP location data file becomes the foundation for generating location-based policies that govern where mobile devices can access certain systems
- Authorization Requests: When mobile devices attempt to access resources, the system evaluates authorization requests against the predefined geofencing policies

Standard Naming Conventions

- Definition: Predefined rules established for creating account names in a consistent manner across an organization
- Common Options:
  - First initial of first name followed by the last name
  - Full first name with a punctuation mark followed by the last name
  - Last name followed by department code
- Conflict Resolution: In cases where two users have similar or identical names, a standard procedure should be implemented to resolve the naming conflict
- Purpose: Ensure ease of identification, uniformity, and avoid confusion

Time-of-Day Restrictions

- Can be used to limit when a user can log into their account

Least Privilege

- Definition: The principle of least privilege dictates that individuals or systems should only be granted the minimum levels of access-or permissions-necessary to complete their tasks
- Purpose: By limiting the number of privileges, it reduces the attack surface, minimizing the potential avenues for attackers to exploit vulnerabilities within a system
- Application: This principle applies both to user accounts and to system processes
- Security Benefits: By eliminating unnecessary privileges, the risk of privilege escalation attacks and misuse is significantly reduced

Account Auditing

- It is critical to maintain and audit accounts regularly
- Auditing Processes:
  - Recertification: A periodic revalidation process that ensures a user's account, access controls, and membership roles are still appropriate and necessary
  - Permission Auditing and Review: This process involves examining the specific permissions granted to a user. The audit determines whether these permissions are still required based on user's current roles and responsibilities
  - Usage Auditing and Review: Focuses on how users are interacting with the applications they have access to

Separation of Duties

- Fraud can result from a single user being trusted with complete control of a process
- Requires two or more people responsible for functions related to handling money
- The system is not vulnerable to actions of a single person

Clean Desk Policy

- Designed to ensure that all confidential or sensitive materials are removed from a user's workplace and secured when the items not in use

Technologies for Access Control

- Access Control Lists (ACLs): These are lists that define permissions attached to an object, specifying which users or system processes are granted access to objects and what operations are allowed on given objects
- Group-Based Access Control: Instead of assigning permissions to individual users, permissions are assigned to groups, and users inherit the permissions of the groups they are part of

Access Control Lists

- Definition: ACLs are sets of permissions attached to objects, specifying which subjects may access those objects and what operations they can perform
- Process: When a subject requests to perform an operation on an object, the system checks the ACL for an approved entry
- Usage:
  - Operating Systems: ACLs are widely used in operating systems to provide file system security
  - SQL/Database Systems: ACLs have been adapted for relational database systems to ensure database security
- Each entry in an ACL is referred to as an Access Control Entry (ACE)
- Structure of an ACE in Windows:
  - Security Identifier
  - Access Mask
  - Flag
  - Inheritance Flags

Group-Based Access Control

- Enables the management of access control policies for multiple computers by setting a single unified policy
- Group Policy is a feature in Windows that provides centralized management and configuration of systems, especially in enterprise environments
- Allows for managing computers and remote users using Active Directory (AD)
- Settings are stored in Group Policy Objects
- Local Group Policy (LGP): Used for Systems not part of AD

Identity and Access Services

There are various services and protocols that can be used to manage identity and access control, including:

- RADIUS (Remote Authentication Dial-In User Service)
  - Provides centralized Authentication, Authorization, and Accounting for users who connect and use a network service
- Kerberos:
  - A secure method for authenticating a request for a service in a computer network using secret-key cryptography
- TACACS (Terminal Access Controller Access-Control System):
  - Handles remote authentication for network access, providing centralized control and ensuring security
- LDAP (Lightweight Directory Access Protocol)
  - A protocol for accessing and maintaining distributed directory information services over an Internet Protocol network
- SAML (Security Assertion Markup Language)
  - An XML-based framework for authentication and authorization between an identity provider and a service provider
- Authentication Framework Protocols
  - Various protocols that support and standardize the process of authentication in different environments and applications

RADIUS

- RADIUS has become an industry-standard for managing remote access
- Original Purpose: Initially created to provide authentication, authorization, and accounting for users accessing a corporate network remotely via dial-in
- RADIUS Client: Typically a network device that communicates user credentials and connection information to the RADIUS server
- Centralized User Profiles: User profiles are centrally stored in a database accessible by all remote servers, allowing for seamless access control and data sharing across the network

Kerberos

- Developed at MIT: authentication protocol designed to produce secure communication by using encryption and ensuring that only authorized parties can access the system
- Security via Encryption: It employs strong encryption methods to authenticate users, providing an extra layer of protection for sensitive data
- Analogy: Think of kerberos as working similarly to using a driver's license to cash a check
- Kerberos Ticket Characteristics
  - Difficult to Duplicate
  - User-Specific Information
  - Defined Restrictions
  - Expiration

TACACS +

- Authentication Service: TACTC+ functions similarly to RADIUS but with more granular control over user authentication, authorization, and accounting
- Primarily for UNIX Systems: It is frequently deployed on UNIX-based systems to facilitate centralized authentication management
- Communication: The protocol forwards user authentication data to a centralized server, where the authentication decisions are made
- Current Version: TACACS+ is the latest version, offering enhanced security features and extended support for multiple protocols compared to its predecessors

LDAP

- Definition: A directory service is a centralized database on a network that stores crucial information about users, devices, and network resources

  Functionality: It tracks and manages network resources, including users' access rights and privileges, allowing it to grant or deny access to resources based on stored information
- X.500 Standard: A global standard designed to ensure uniformity in how directory data is stored and accessed across different systems, ensuring compatibility between various platforms
- LDAP (Lightweight Directory Access Protocol): Based on the X.500 standard, LDAP provides a simplified protocol that allows client applications to interact with directory services for querying and managing data efficiently
- Purpose and Design: LDAP is built to run over TCP/IP, offering a simplified subset of the DAP. It uses a less complex encoding method than the full X.500 standard, making LDAP more lightweight and efficient for most directory service use cases
- Security Considerations: By default, LDAP traffic is transmitted in plaintext, making it vulnerable to eavesdropping. However, LDAP can be secured by employing SSL (Secure Sockets Layer) or TLS (Transport Layer Security), resulting in Secure LDAP, also know as LDAP over SSL
- LDAP injection attacks: LDAP can be vulnerable to injection attacks when user input is improperly filtered. This type of attack can exploit weaknesses in how input is handled, allowing attacks to manipulate directory queries for malicious purposes. Proper input validation is essential to prevent these vulnerabilities

Security Assertion Markup Language (SAML)

- A protocol based on XML that enables the secure exchange of authentication and authorization data between web domains
- Single Identity Provider: SAML allows login credentials to be stored with a central identity provider, eliminating the need for multiple service providers to store credentials, thus enhancing security and reducing redundancy
- Broad Usage: Extensively utilized in business-to-business (B2B) and business-to-consumer (B2C) online transactions
- Main Benefit: Facilitates seamless, federated identity management, enabling users to authenticate once and gain access to multiple applications or services across organizational boundaries

Authentication Framework Protocol

- Extensible Authentication Protocol
- A framework used for transporting authentication protocols in network environments
- Purpose: Created to provide a more secure alternative to legacy protocols such as:
  - CHAP: Challenge-Handshake Authentication Protocol
  - MS-CHAP: Microsoft's version of CHAP
  - PAP: Password Authentication Protocol
- Key Features:
  - Defines Message Formats: EAP doesn't define any one specific authentication mechanism but instead outlines how to transport various authentication messages
  - Four Packet Types:
    - Request: Initiates the authentication process
    - Response: Replies to the request for authentication
    - Success: Signals a successful authentication
    - Failure: Indicates that authentication has failed

Threats In Networks

- Anonymity
  - The potential attacker is safe behind an electronic shield
  - The attack can be passed through many other hosts in an effort to disguise the attacker's origin
- Many points of attack - both targets and origins
  - When a file is stored in a network host remote from the user, the data or the file itself may pass through many hosts to get to the user, with various security policies
  - Administrators have no control over other hosts in the network
- Sharing
  - Because networks enable resource and workload sharing, more users have the potential to access networked systems than on single computers
- Complexity of system
  - A network combines two or more possibly dissimilar operating systems
  - A network operating/control system is likely to be more complex than an operating system for a single computing system
  - The attacker can use computing power of other computers to advantage by causing the victim's computer to perform part of the attack's computation
- Unknown Perimeter
  - A network's expandability also implies uncertainty about the network boundary
  - Although wide accessibility is an advantage, unknown or uncontrolled group of possibly malicious users is a security disadvantage
- Unknown Path
  - There may be many paths from one host to another
  - Network users seldom have control over the routing of their messages

Precursors to an Attack

- Understanding the context of the target
  - Port Scan
    - A program that, for a particular IP address, reports
      - Which ports respond to messages
      - Which of several known vulnerabilities seem to be present
    - Tells an attacker
      - Which standard ports or services are running and responding on the target system
      - What operating system is installed on the target
      - What applications and versions are present

- Social Engineering
  - Using social skills and personal interaction to get someone to reveal security-relevant information
    - Impersonate someone
- Intelligence
  - Gathering discrete bits of information from various sources
  - Putting them together like the pieces of a puzzle
  - Techniques
    - Dumpster diving
    - Eavesdropping
- OS and Application Fingerprinting
  - Sending meaningless messages
  - Receiving meaningful responses
- Bulletin Boards and Chats
- Availability of Documentation

Types of Attack

- Eavesdropping
- Passive Wiretapping
- Active Wiretapping
- Impersonation
  - Guess the identity and authentication details
  - Authentication obtained by Eavesdropping or Wiretapping
  - Nonexistent Authentication
- Spoofing
  - Masquerade
    - URL confusion
    - Phishing
  - Session Hijacking
    - Intercepting and carrying on a session begun by another entity
  - Man-in-the-Middle Attack
    - One entity intrudes between two others
    - Attacker participates from the start of the session

Web Site Vulnerabilities

- Web Site Defacement
  - Change the visual appearance of a website or a webpage
- Buffer Overflows
  - Feed a program far more data than it expects to receive
  - A buffer size is exceeded, and the excess data spill over into adjoining code and data locations
- Dot-Dot-Slash (directory or path traversal)
  - Access a server file that is not intended to be accessible
- Application Code Editors
  - Time-of-check to time-of-use flaw
- Server-Side Include
  - Execute OS commands using web command fields, such as email and if inside the web pages

Denial of Service (DoS Attack)

- Connection Flooding
  - Attacker sends as much data as the target server can handle
  - Using Internet Control Message Protocols
    - Ping: Requests a destination to return a reply
    - echo: Requests a destination to return the data sent to it
    - destination unreachable: Indicates that a destination address cannot be accessed
    - source quench: Means that the destination is becoming saturated and the source should suspend sending packets for a while
- Smurf
  - Large number of ping packets with the victim's spoofed source IP are broadcast to a network of unwitting victims using an IP Broadcast address
  - They will respond by sending a reply to the source IP address
  - The victim's computer will be flooded with traffic
- Syn Flood
  - Attacker can deny service to the target by sending many SYN requests and never responding with ACK's, thereby filling the victim's SYN-RECV queue
- DNS Attacks
  - A domain name system server translates domain names into IP addresses. If the server doesn't know a requested translation it will ask another server
    - DNS Flooding: Sending an overwhelming number of DNS requests to the server, consuming its resources
    - DNS Amplification: An attacker sends small queries to open DNS servers with a spoofed IP address to trigger large responses, causing the DNS server to respond to the victim with a flood of data
    - DNS Reflection: Attackers send requests to DNS servers, using the target's IP address as the return address, causing the target to be flooded with DNS query responses
- Distributed Denial of Service (DDOS)
  - Attacker plants a trojan horse, including various types of DOS attack, on some target machines
  - At some point the attacker chooses a victim and sends a signal to all the zombies to launch the attack
  - Then, instead of the victim's trying to defend against one DOS attack, it must try to counter n attacks from the n zombies all acting at once

Cookies

- A data object that can be held in memory or stored on disk for future access
- A cookie is something that
  - Takes up space on your disk
  - Holding information about you that you cannot see
  - Forwarded to servers you do not know whenever the server wants it, without informing you

Scripts

- An attack from client to server
  - A browser organizes user inputs into parameters to a defined script
  - It then sends the script and parameters to a server to be executed
  - The server cannot distinguish between commands generated from a user and a user's handcrafting a set of orders
  - The malicious user can monitor the communication between a browser and a server to see how changing a web page entry affects what the browser sends and then how the server reacts and manipulate the server's actions

Active Code

- Java Code
  - A hostile applet is downloadable Java code that can cause harm on the client's system
- ActiveX controls
  - Objects of arbitrary type can be downloaded to a client
- Auto Exec by Type
  - When a file arrives with an extension, the OS automatically invokes the appropriate processor to handle it
  - It gives an opportunity to an attacker, such as running malicious macros, from inside a .doc file
- Bots
  - Pieces of malicious code under remote control
  - Used for DDOS attacks, launching attacks from many sites in parallel against a victim
  - Used for spam and other bulk email attacks

Network Security Controls

- Three steps of a security threat analysis
  - Scrutinize all the parts of a system so that we know what each part does and how it interacts with other parts
  - Consider possible damage to
    - Confidentiality
    - Integrity
    - Availability
  - Hypothesize the kinds of attacks that could cause this damage
- Same steps can be taken with a network
- Individual parts of a network
  - Local
    - nodes
    - communications links
    - area network
    - data storage
    - processes
    - Devices
  - Network
    - gateway
    - communications
    - control resources
    - routers
    - resources
- Malicious Activities:
  - Read communications
  - Modify communications
  - Forge communications
  - Inhibit communications
  - Inhibit all communications passing through a point
  - Read data
  - Modify or destroy data
- Network Design Concerns
  - Segmentation
    - Do not run all activities on one machine
    - Distribute the tasks based on the principles of least privilege and encapsulation
  - Redundancy
    - Allowing a function to be performed on more than one node
    - Failover mode
      - Servers communicate with secondary server periodically
  - Single Point of Failure
    - Single point in the network that, if it were to fail, could deny access to all or a significant part of the network
    - Distributing the database by placing copies of it on different network segments
  - Mobile Agents
    - Using mobile code and agents as forces for good
    - Design the system, in which no one agent is critical to the overall success, but the overall group can be trusted
    - Build distributed services that tolerate buggy, selfish, or malicious codes
- Encryption
  - Not a silver bullet
    - A flawed system design with encryption is still a flawed system design
    - Encryption protects only what is encrypted
    - Encryption is no more secure than its key management
  - In network applications, encryption can be applied
    - Between two hosts
    - Between two applications
  - A constant issue
    - Safe key distribution
- Link Encryption
  - Data are encrypted just before the system places them on the physical communications link
  - Decryption occurs just as the communication arrives at and enters the receiving computer
  - Encryption protects the message in transit between two computers, but the message is in plaintext inside the hosts
  - The message is exposed in two layers of all intermediate hosts through which the message may pass
  - This exposure occurs before routing and addressing are not read at the bottom layer, but only at higher layers
  - Appropriate when the transmission line is the point of greatest vulnerability and the communication medium is shared with other users or is not secure
  - Virtual Private Networks (VPN)
    - Firewalls can be used to implement a VPN
    - The larger network is restricted only to those given special access by the VPN
    - Communication passes through an encrypted tunnel or tunnel
- End-to-End Encryption
  - Provides security from one end of a transmission to the other
  - Encryption is performed at the highest levels, layer 7, application, or layer 6, presentation, of the OSI model
- Public key Infrastructure (PKI)
  - A process created to enable users to implement public key cryptography
  - Offers each user a set of services
    - Create certificates associating a user's identity with a key
    - Give out certificates from its database
    - Sign certificates, adding its credibility to the authenticity of the certificate
    - Confirm (or deny) that a certificate is valid
    - Invalidate certificates for users who no longer are allowed access or whose private key has been exposed
  - Certificate Authority
    - Implements the PKI policy on certificates
    - Actions
      - Managing public key certificates for their whole life cycle
      - Issuing certificates by binding a user's or system's identity to a public key with a digital signature
      - Scheduling expiration dates for certificates
      - Ensuring that certificates are revoked when necessary
  - Registration Authority
    - An interface between a user and a certificate authority
  - Quality of registration authority determines the level of trust that can be placed in the issued certificates
- Content Integrity
  - Potential Threats:
    - Malicious modification that changes content in a meaningful way
    - Malicious or non-malicious modification that changes content in a way that is not necessarily meaningful
    - Non-malicious modification that changes content in a way that will not be detected
  - Error Detection
    - Parity check
    - Huff codes
    - Huffman codes
    - Cryptographic Checksum
- Authentication in Networks
  - One-time Password
    - User and host both have access to identical lists of passwords
    - Password token: A device that generates a password that is unpredictable but that can be validated on the receiving end
  - Kerberos
    - Authentication in distributed systems
    - A central server provides authenticated tokens, tickets, to requesting applications
  - Ticket
    - Unforgeable, nonreplayable, authenticated object
    - An encrypted data structure naming a user and a service that user is allowed to obtain

Firewalls

- A device that filters all traffic between a protected (inside network) and a less trustworthy (outside network)
- Main characteristics
  - Always invoked
  - Tamperproof
  - Small and simple

- Types of Firewalls
  - Packet filtering gateways or screening routers
  - Stateful inspection firewalls
  - Application proxies
  - Guards
  - Personal firewalls
- Packet filtering gateways or screening routers
  - Control access to packets on the basis of
    - Packet address
    - Specific transport protocol type
  - Do not see inside a packet
  - Can block all packets from the outside that claimed their source address was an inside address
- Stateful inspection firewalls
  - keep track of the state of network connections
  - Do not treat each packet in isolation
  - Maintain state information from one packet to another in the input stream
- Application Proxy
  - A firewall that simulates the effects of an application so that the application receives only requests to act properly
  - A two-headed device
    - It looks to the inside as if it is the outside connection while to the outside it responds just as the insider would
- Guard
  - Like a proxy firewall with more detailed functionalities

Intrusion Detection Systems (IDS)

- A device, typically another separate computer, that monitors activity to identify malicious or suspicious events
- Receives raw inputs from sensors, saves those inputs, analyzes them, and takes some controlling action
- Functions:
  - Monitoring users and system activity
  - Auditing system configuration for vulnerabilities and misconfigurations
  - Assessing the integrity of critical system and data files
  - Recognizing known attack patterns in system activity
  - Identifying abnormal activity through statistical analysis
  - Managing audit trails and highlighting user violation of policy or normal activity
  - Correcting system configuration errors
  - Installing and operating traps to record information about intruders
- Types of IDS
  - Network-based
    - A stand-alone device attached to the network
  - Host-based
    - Runs on a single workstation or client or host
  - Signature-based
    - Performs simple pattern-matching and report situations that match a pattern corresponding to a known attack type
    - Cannot detect a new attack for which a signature is not yet installed in the database
    - Uses statistical analysis and ML models
  - Heuristic
    - Builds a model of acceptable behaviour and flag exceptions to that model
    - For the future, the administrator can mark a flagged behaviour as acceptable so that the heuristic IDS will now treat that previously unclassified behaviour as acceptable
  - State-based
    - See the system going through changes of overall state or configuration
    - Try to detect when the system has veered into unsafe modes
  - Model-based
    - Try to map current activity onto a model of unacceptable activity and raise an alarm when the activity resembles the model
  - Misuse
    - Real activity is compared against a known suspicious area
- Stealth Mode
  - To prevent malicious activities against IDS, such as disabling it
    - Work as a passive wiretap
- Responding to Alarms
  - Monitor, collect data, perhaps increase amount of data collected
  - Protect, act to reduce exposure
  - Call a human
- False Results (System's Sensitivity)
  - False Positive
    - Raising an alarm for something that is not really an attack
  - False Negative
    - Not raising an alarm for a real attack

Secure E-Mail

- Threats to E-mail
  - Message interception (confidentiality)
  - Message interception (Masked delivery)
  - Message interception and subsequent replay
  - Message content modification
  - Message origin modification
  - Message content forgery by outsider
  - Message origin forgery by outsider
  - Message content forgery by recipient
  - Message origin forgery by recipient
  - Denial of message transmission
- Requirements
  - Message confidentiality
    - The message should not be exposed when routing to the receiver
  - Message integrity
    - What the receiver sees should be what was sent
  - Sender authenticity
    - Receiver should be confident about who the sender was
  - Nonrepudiation
    - Sender cannot deny having set the message
- Confidentiality
  - The sender chooses a (random) symmetric algorithm encryption key
  - The sender encrypts a copy of the entire message to be transmitted
  - The sender prepends plaintext headers
  - The sender encrypts the message key under the recipient's public key, and attaches that to the message as well
- PGP (Pretty Good Privacy)
  - Creates a random session key for a symmetric algorithm
  - Encrypt the message, using the session key
  - Encrypt the session key under the recipient's public key
  - Generate a message digest or hash of the message
  - Attach the encrypted session key to the encrypted message and digest
  - Transmit the message to the recipient
- S/MIME (Secure Multipurpose Internet Mail Extensions)
  - The principal difference between S/MIME and PGP is the method of key exchange
    - PGP depends on each user's exchanging keys with all potential recipients and establishing a ring of trusted recipients
    - It also requires establishing a degree of trust in the authenticity of the keys for those recipients
    - S/MIME uses hierarchy validated certificates for key exchange
    - Thus, with S/MIME, the sender and recipient do not need to have exchanged keys in advance as long as they have a common certifier they both trust
  - It handles e-mail attachments as well

Security and Information Event Management

- SIEM Product
  - Consolidates real-time monitoring and management of security information
  - Analyzes and reports on security events
- A SIEM product can be
  - A separate device
  - Software that runs on a computer
  - A service that is provided by a third party
- Has following features:
  - Aggregation
  - Correlation
  - Automated alerting and triggers
  - Time synchronization
  - Event duplication
  - SIEM logs

Security Through Network Architecture

- The design of a network can provide a secure foundation for resisting attackers
- Elements of a secure network architectural design include:
  - Creating security zones
  - Using network segregation

Security Zones

- A secure approach is to create zones to partition the network
  - So that certain users may enter one zone while access is prohibited to other users
- The most common security zones:
  - Demilitarized zones (DMZ)
  - Using network address translation to create zones

Demilitarized Zone (DMZ)

- A separate network located outside secure network perimeter
- Untrusted outside users can access DMZ but not secure network

Network Address Translation (NAT)

- Network address translation (NAT)
  - Allows private IP addresses to be used on the public internet
  - Replaces private IP address with public address
- Advantage of NAT
  - Masks IP address of internal devices
  - An attacker who captures the packet on the internet cannot determine the actual IP address of sender

Other Zones

- Intranet: A private network that belongs to an organization that can only be accessed by approved internal users
- Extranet: A private network that can be accessed by authorized external customers, vendors, and partners
- Great network: A separate open network that anyone can access without prior authorization

Network Segregation

Physical network segregation
- Isolates the network so that it is not accessible by outsiders

- Air gap
  - The absence of any type of connection between devices
  - In this case the secure network and another network
- Networks can be segmented using switches to divide the network into a hierarchy
- Virtual LAN (VLAN)
  - Allow scattered users to be logically grouped together
  - Even if attached to different switches
- Can isolate sensitive data to VLAN members
- Communication on a VLAN
  - If connected to same switch, switch handles packet transfer
  - A special "tagging" protocol is used for communicating between switches

Network Access Control

- Examines the current state of a system or network device before it can connect to the network
- Any device that does not meet a specified set of criteria can connect only to a "quarantine" network where the security deficiencies are corrected
- Goal: To prevent computers with suboptimal security from potentially infecting other computers through the network
- Uses software "agents" to gather information and report back
- An agent may be a:
  - Permanent NAC agent
  - Dissolvable NAC agent - disappears after reporting information to the NAC
- NAC technology can be embedded within a Microsoft Windows Active Directory domain controller
  - NAC uses Active Directory to scan the device

Data Loss Prevention (DLP)

- DLP
  - A system of security tools that is used to recognize and identify data that is critical to the organization
  - Ensures that it is protected
- Two common uses of DLP
  - Monitoring emails through a mail gateway
  - Blocking the copying of files to a USB flash drive
- Most DLP systems use content inspection
  - Defined as a security analysis of the transaction within its approved context
- Content inspection looks at not only the security level of data, but also:
  - Who is requesting it
  - Where the data is stored
  - When it was requested
  - Where it is going
- Three types of DLP sensors:
  - DLP network sensors
  - DLP storage sensors
  - DLP agent sensors
- When a policy violation is detected by the DLP agent, it is reported back to the DLP server
- Different actions can be taken:
  - Block the data
  - Redirect it to an individual who can examine the request
  - Quarantine the data until later
  - Alert a supervisor of the request