



**Technical  
Institute of America**

# Security+ 701

---

ANDREW RAMDAYAL



CompTIA Security+ 70 Course Notes

# CompTIA Security+

## SY0-701

- **90-minute time limit**
- **Maximum of 90 Questions**
  - **Multiple choice**
    - Pick one or many answers.
  - **Drag & Drop**
    - Match objects to a diagram.
  - **Performance-based (Simulators)**
    - These are hands-on troubleshooting scenarios where you'll have to perform a series of steps/commands
- **750 (83%) out of a scale of 100-900**



CompTIA Security+ 70 Course Notes

# CompTIA Security+

## SY0-701

Domain	% of Exam
<b>1. General Security Concepts</b>	12%
<b>2. Threats, Vulnerabilities, and Mitigations</b>	22%
<b>3. Security Architecture</b>	18%
<b>4. Security Operations</b>	28%
<b>5. Security Program Management and Oversight</b>	20%
<b>Total</b>	100%

# IT Security Fundamentals

---



CompTIA Security+ 70 Course Notes

## CIA Triad





CompTIA Security+ 70 Course Notes

## CIA Triad

- Confidentiality: Ensuring that sensitive information is accessed only by an authorized person and kept away from those not authorized to possess it.
- Integrity: Assuring the accuracy and reliability of information and systems. Checks if data or systems has been altered
- Availability: Ensuring that data and resources are available to authorized users when needed.



## CompTIA Security+ 70 Course Notes

# Confidentiality

- Confidentiality refers to the measures taken to ensure that sensitive information is not disclosed to unauthorized individuals, entities, or processes.
- Involves preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Here's a breakdown of what this entails:
  - **Access Controls:** Mechanisms such as passwords, biometric verification, or access cards that limit resource access to authorized personnel to prevent unauthorized access to information.
  - **Encryption:** The process of encoding information in such a way that only authorized parties can read it. If an unauthorized party intercepts the encrypted data, they will not be able to interpret it without the encryption key.



## CompTIA Security+ 70 Course Notes

# Confidentiality

- **Secure Communication:** Using secure protocols like SSL/TLS for transmitting data to prevent interception by unauthorized entities.
- **Policies and Procedures:** Establishing guidelines for who has access to information and under what conditions, and what the protocols are for handling and sharing that information.
- **Training and Awareness:** Educating employees and users about the importance of confidentiality and how to ensure it is maintained.
- **Data Classification:** Categorizing data based on its level of sensitivity and the impact to the organization if it is disclosed or improperly accessed.



## CompTIA Security+ 70 Course Notes

# Integrity

- Integrity refers to the trustworthiness and veracity of data or resources.
- It is about protecting data from unauthorized changes to ensure that it is reliable and correct.
- Here are key aspects of integrity within IT security:
  - Data Accuracy
  - Data Consistency
  - Data Trustworthiness



## CompTIA Security+ 70 Course Notes

# Integrity

- Various methods and mechanisms are used, such as:
- Checksums and Cryptographic Hash Functions: These are algorithms that produce a short, fixed-size bit string from arbitrary-length strings of data. If the data changes, so will the hash value, which can be used to detect changes or corruption.
- Digital Signatures: Provide a means to verify that a message, document, or other data file comes from a specific entity and has not been altered.
- Access Controls: Limit data access to authorized users to prevent unauthorized modifications.



## CompTIA Security+ 70 Course Notes

# Availability

- Availability refers to ensuring that data, systems, and services are accessible to authorized users when needed,
- Here's how availability is maintained in IT:
  - Redundancy: Creating multiple copies of data or system components that can take over in case of a failure.
  - Fault Tolerance: Building systems that can continue operating properly even if some of their components fail.
  - Backup Systems: Regularly backing up data and systems to enable recovery in case of data loss or corruption.



## CompTIA Security+ 70 Course Notes

# Availability

- Disaster Recovery Plans: Having a plan in place to recover from significant adverse events, such as natural disasters, power outages, or cyberattacks.
- The goal of ensuring availability is to prevent service disruptions due to system failures, infrastructure problems, or malicious attacks like Distributed Denial of Service (DDoS).



CompTIA Security+ 70 Course Notes

## DAD Triade

- Opposite of the CIA Triade





## CompTIA Security+ 70 Course Notes

# DAD Triade

**Disclosure:** This is analogous to a breach in confidentiality. It refers to the unauthorized access and exposure of information.

**Alteration:** This threat corresponds to a loss of integrity, where unauthorized changes are made to data.

**Destruction:** This represents a direct attack on availability. Destruction involves the deletion or corruption of data or physical damage to hardware, rendering the information irrecoverable.



## CompTIA Security+ 70 Course Notes

# Non-repudiation

Ensure that a party in a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

Can be implemented using a digital signatures.

- Digital signatures uses cryptographic techniques, a digital signature binds a person to the digital data they send.



## CompTIA Security+ 70 Course Notes

# AAA

**Authentication:** This is the process of verifying the identity of a user, device, or other entity in a computer system, typically as a prerequisite to granting access to resources in a system.

**Authorization:** Once a user is authenticated, the authorization process determines what that user is permitted to do by matching user or system credentials against an access control list.

**Accounting (sometimes referred to as Auditing):** Accounting is ensured by keeping a track of activities. It involves the logging and monitoring of user actions



## CompTIA Security+ 70 Course Notes

# Authentication

Verifying the identity of a user, device, or other entity in a system, usually as a prerequisite for accessing resources in that system.

- Comes after identification



## CompTIA Security+ 70 Course Notes

# Authentication

### Factors of Authentication:

- **Something you know:** This involves verifying identity based on knowledge of something confidential, such as a password, PIN, or answers to secret questions.
- **Something you have:** This involves items in your possession that can be used to verify your identity, such as security tokens, smart cards, or a mobile phone (used for receiving OTPs or push notifications).
- **Something you are:** This refers to biometrics - unique physical characteristics such as fingerprints, facial recognition, iris scans, or voice patterns.
- **Somewhere you are:** Authentication can also be based on the user's location, which can be determined through IP addresses, GPS, or other geolocation methods.
- **Something you do:** Behavioral biometrics such as keystroke dynamics or mouse use patterns can also be used to authenticate a user.



CompTIA Security+ 70 Course Notes

# Authentication

## Multiple Factor Authentication (MFA):

- Is a security process that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.
- MFA combines two or more independent credentials: what the user knows (password), what the user has (security token), and what the user is (biometric verification).



## CompTIA Security+ 70 Course Notes

# Authentication

Authenticating People can be done using:

- **Biometrics:** Utilizing physical characteristics (e.g., fingerprints, facial recognition, retina scans) unique to an individual.
- **Knowledge-Based Authentication:** Requiring information only the user should know (e.g., passwords, PINs, security questions).
- **Multiple Factor Authentication (MFA):** Combining something the user knows (password) with something they have (a phone or token) or are (biometric verification).

Authenticating Systems can be done using:

- **Certificates and Keys:** Using digital certificates and cryptographic keys to establish trust between machines.
- **IP Allow list:** Allowing only systems with certain IP addresses to access a service or network.
- **MAC Address Filtering:** Restricting access to a network to devices with specific MAC addresses.



# Authorization

**Authorization determines what that user is allowed to do by establishing their rights and privileges.**

**Can be done using:**

- Permissions and Privileges: It involves granting permissions to access specific resources or data. Permissions define the actions permitted, such as read, write, execute, delete, or modify.
- Access Control: Authorization is enforced through access control mechanisms such as an Access control lists (ACLs).
- Authorization Models such as Mandatory Access Control (MAC) or Discretionary Access Control (DAC).



## CompTIA Security+ 70 Course Notes

# Accounting

Refers to the tracking of user activities and resource usage within a system.

Ensures that users are not only authenticated and authorized but also held accountable for their actions while accessing and using system resources.

Can be done using:

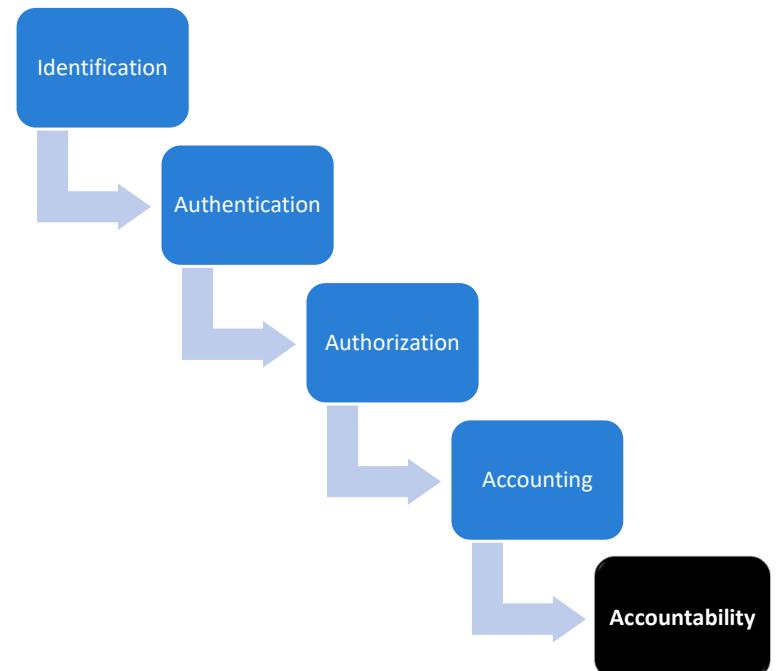
- User Activity Tracking: Accounting involves collecting data on user activities, such as login times, duration of sessions, accessed resources, network services used, system changes made, and data transferred
- Audit Trails and Logs: Systems maintain logs and audit trails that capture detailed information on various events.



CompTIA Security+ 70 Course Notes

# Accountability

Principle that ensures individuals or entities are held responsible for their actions within a system.





## CompTIA Security+ 70 Course Notes

# Gap Analysis

Is a methodical assessment that organizations use to compare their current security posture with a set of standards, best practices, or regulatory requirements to identify areas that need improvement.

Involves:

- Identification of Current State: This involves mapping out the existing security measures, policies, and controls.
- Determination of Target State: The target state is typically defined by industry standards, regulatory requirements, or the organization's internal objectives for security.
- Analysis of the Gap: The core of gap analysis is identifying the differences between the current state and the target state.



CompTIA Security+ 70 Course Notes

## Zero Trust

Centers on the belief that organizations should not automatically trust anything inside or outside their perimeters and instead must verify anything and everything trying to connect to its systems before granting access.

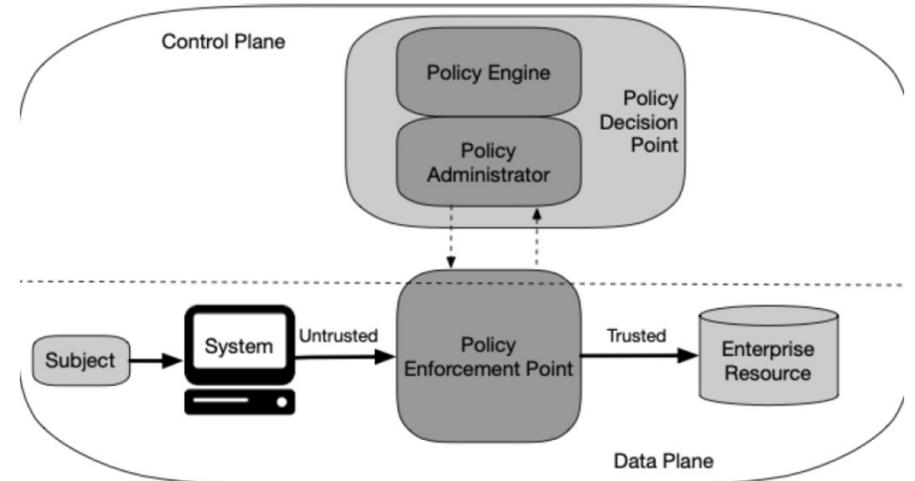
Includes:

- Strict Identity Verification
- Least Privilege Access
- Multi-Factor Authentication (MFA)
- Monitor and Log All Traffic



## CompTIA Security+ 70 Course Notes

# Zero Trust



NIST Core Zero Trust Logical Components. NIST.SP.800-207,  
Page 9



## CompTIA Security+ 70 Course Notes

# Zero Trust

- **Data Plane:**
  - **Implicit Trust Zones:** Areas where trust is assumed by default.
  - **Subject/System:** Entities requesting or being granted access.
  - **Policy Enforcement Point:** Responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource.
- **Control Plane:**
  - **Adaptive Identity:** Dynamically adjusting user/system identity verification based on context.
  - **Policy-driven Access Control:** Access granted based on policies rather than static permissions.
  - **Policy Administrator:** responsible for establishing and/or shutting down the communication path between a subject and a resource
  - **Policy Engine:** responsible for the ultimate decision to grant access to a resource for a given subject
  - **Threat Scope Reduction:** Minimizing the attack surface.

# Security Controls Categories and Types

---



## CompTIA Security+ 70 Course Notes

# Security Controls

Security controls are safeguards or countermeasures employed to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

They help to maintain the confidentiality, integrity, and availability of information

Broken down into:

- Categories
  - Technical
  - Managerial
  - Operational
  - Physical
- Types
  - Preventive
  - Deterrent
  - Detective
  - Corrective
  - Compensating
  - Directive



CompTIA Security+ 70 Course Notes

# Security Controls Categories

**Technical security controls**, also known as logical security controls, are mechanisms implemented in hardware, software, or firmware that automate the process of preventing, detecting, and responding to security threats.

Includes:

- Access Control Mechanisms
- Firewalls
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- Encryption
- Antivirus and Antimalware Software
- Virtual Private Networks (VPN)



CompTIA Security+ 70 Course Notes

# Security Controls Categories

**Managerial security controls**, also known as administrative controls, are the policies, procedures, and guidelines that govern the behavior of people within an organization and the operation of the IT systems.

Includes:

- Security Policies and Procedures
- Risk Management
- Incident Response and Recovery Plans
- Business Continuity and Disaster Recovery Planning



CompTIA Security+ 70 Course Notes

# Security Controls Categories

**Operational security controls** are the day-to-day methods and procedures that are implemented by an organization to ensure and maintain the security of its information and assets.

Done by people in the organization.

Includes:

- Security Awareness Training
- Physical media protection



# Security Controls Categories

**Physical security controls** in IT security are measures taken to protect the actual hardware and facilities that house the systems, networks, and data.

These controls are designed to prevent unauthorized access, damage, and interference to the organization's physical resources.

Includes:

- Lighting
- Signs
- fences
- Security guards
- Cameras



## CompTIA Security+ 70 Course Notes

# Security Controls Types

### Preventive controls

- Attempts to stop a security incident from occurring.
- e.g., IPS, firewalls, encryption, access controls

### Detective controls

- Attempts to detect events that resulted in a security incident.
- e.g., IDS, SIEM, video surveillance, motion detection

### Corrective controls

- Attempts to remediate an incident that has occurred.
- e.g., UPS, restoring backups, incident response procedures



## CompTIA Security+ 70 Course Notes

# Security Controls Types

### Deterrent controls

- Attempts to discourage a threat.
- e.g., Guard dogs, Cameras, barbed wire

### Directive controls

- Provides directions on how to systems.
- e.g., Policies, Procedures

### Compensating controls

- Provides alternate controls when the primary control may not be sufficient.
- e.g., Segregation of duties



CompTIA Security+ 70 Course Notes

## Layered Security

Layered security, also known as **Defense in Depth**, is an information assurance concept where multiple layers of security controls (defensive mechanisms) are placed throughout an information technology (IT) system.

Utilizing multiple controls in a layered manner to protect information.

# Threats

---



CompTIA Security+ 70 Course Notes

# Threats

## Threat actors:

- Nation-state
- Unskilled attacker
- Hacktivist
- Insider threat
- Organized crime
- Shadow IT



## CompTIA Security+ 70 Course Notes

# Attributes of Actors

**Internal/External:** Whether the threat actor originates from within (e.g., Insider Threat) or outside (e.g., Nation-State) the organization.

**Resources/Funding:** The amount of money and resources available to the threat actor. For example, Nation-States typically have significant resources.

**Level of Sophistication/Capability:** The technical skill level of the threat actor. Nation-States and Organized Crime groups often have high sophistication, while Unskilled Attackers are at the lower end.



# Threats Motivations

1. **Data Exfiltration:** Stealing data from a target, often for selling or leverage.
2. **Espionage:** Spying on entities to gather sensitive information, common with Nation-States.
3. **Service Disruption:** Disabling or disturbing a service, often seen with hacktivists protesting against specific services or companies.
4. **Blackmail:** Threatening to release sensitive data unless a demand (usually monetary) is met.
5. **Financial Gain:** Stealing data or directly siphoning money, a common motivation for organized crime.



## CompTIA Security+ 70 Course Notes

# Threats Motivations

6. **Philosophical/Political Beliefs:** Acting based on personal or group beliefs, commonly seen with hacktivists.
7. **Ethical:** Acting on perceived ethical obligations, sometimes seen with whistleblowers or "white hat" hackers identifying vulnerabilities.
8. **Revenge:** Targeting an entity out of vengeance for a perceived wrong.
9. **Disruption/Chaos:** Motivated purely by the desire to create disorder, sometimes without specific political or financial goals.
10. **War:** Cyber-operations that are a component of larger warfare, typically driven by Nation-States.



## CompTIA Security+ 70 Course Notes

### Nation-state

A country's government which can engage in or sponsor cyber activities.

Activities can range from espionage or cyber warfare.

Motivations including political, economic, or military advantage over other nations, groups, or individuals.

Typically well-funded and sophisticated, uses a wide array of resources that enable them to conduct prolonged and targeted cyber operations.

They may use advanced persistent threats (APTs) to infiltrate and remain undetected within a target's infrastructure for long periods, gathering intelligence or preparing for a cyberattack.



## CompTIA Security+ 70 Course Notes

### Nation-state

Operations can be highly complex and difficult to detect or defend against.

They may target critical infrastructure, government agencies, corporations, or other nation-states.

The impact of their attacks can be substantial, leading to the theft of sensitive information, disruption of services, or even damage to physical assets.

Defending against nation-state actors requires robust cybersecurity measures.



## CompTIA Security+ 70 Course Notes

# Unskilled attacker

Individual with limited technical expertise in conducting cyber attacks.

Often dubbed as "script kiddies," these attackers typically use pre-made tools, scripts, or software developed by others to exploit known vulnerabilities in systems.

They do not usually have the ability to discover new vulnerabilities or create their own sophisticated hacking tools.

Danger posed by unskilled attackers comes from the widespread availability of attack tools and the abundance of unpatched or poorly secured systems that can be readily exploited.



## CompTIA Security+ 70 Course Notes

# Hacktivist

Someone who uses hacking techniques and digital tools to promote a political agenda, social change, or ideological beliefs.

Hacktivism is a portmanteau of "hacking" and "activism" and represents the use of technology to promote political ends.

Hacktivists often target websites, servers, and other digital infrastructure as a form of protest or to draw attention to their cause.

Their actions can range from unauthorized access to systems, defacement of websites, denial-of-service attacks, to the release of confidential information.



## CompTIA Security+ 70 Course Notes

# Insider threat

A risk posed by individuals from within the organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems.

Can be malicious, as in the case of an employee who intentionally misuses access to harm the organization.

Can also be unintentional, as in the case of an employee who inadvertently falls prey to a phishing scam, thereby exposing the network to attackers.

Particularly challenging to mitigate because insiders typically have legitimate access to the organization's systems, which can make malicious activities harder to detect.



## CompTIA Security+ 70 Course Notes

# Organized crime

Groups or operations run by criminals who systematically engage in illegal activities for profit, often involving sophisticated and coordinated cyber attacks.

These criminal organizations are known for their structured hierarchy, strategic planning, and use of technology to conduct a range of illicit activities, such as

- Financial fraud
- Identity theft
- Ransomware attacks
- Sale and distribution of stolen data.

Organized crime groups are well-funded, have access to advanced tools, and possess the technical know-how to execute large-scale cybercrimes.

They often target financial institutions, retail businesses, and individuals, exploiting weaknesses in security systems and human vulnerabilities to steal money, data, and other assets.



## CompTIA Security+ 70 Course Notes

# Shadow IT

Refers to information technology systems and solutions built and used inside organizations without explicit organizational approval.

It includes software, hardware, and cloud services procured and managed outside of the official IT department's purview.

The risks associated with Shadow IT stem from the lack of oversight and control.

Systems and applications that are not vetted by the IT department may not comply with organizational security policies or standards.

This can lead to data breaches, non-compliance with regulations, and potential vulnerabilities in the network.

Common examples of Shadow IT include employees using unauthorized cloud storage services to share company files, installing personal software on work devices, or using unsanctioned messaging apps for communication.



## Threat Vectors and Attack Surfaces

### Message-based:

- **Email:** A popular medium for delivering malicious content or links. Phishing attempts, malware, ransomware, and spam often use this vector.
- **SMS:** Mobile-based text messages can contain phishing links (Smishing) or malicious content targeting smartphones.
- **Instant Messaging (IM):** Real-time messaging services can be exploited to deliver malware or phishing content.

**Image-based:** Malicious payloads can be embedded in images, which, when viewed, can exploit vulnerabilities.

**File-based:** Malicious software can be embedded within files, which, upon opening or execution, can lead to compromise.



## Threat Vectors and Attack Surfaces

**Voice Call:** Vishing (voice-based phishing) involves criminals using phone calls to deceive victims into divulging personal information or following malicious instructions.

**Removable Device:** Devices like USBs can be used to introduce malware or exploit software vulnerabilities when connected to a system.

### Vulnerable Software:

- **Client-based:** Software that requires installation on a user's system can be targeted for vulnerabilities.
- **Agentless:** Software that runs without installations or agents, making them harder to monitor and potentially vulnerable.



## Threat Vectors and Attack Surfaces

### Unsupported Systems and Applications:

Outdated software that no longer receives security updates can be a significant risk.

### Unsecure Networks:

- **Wireless:** Unsecured Wi-Fi networks can be intercepted or exploited.
- **Wired:** Physical access to wired networks can lead to intrusion.
- **Bluetooth:** Vulnerabilities in Bluetooth can be exploited to snoop on or control devices.

**Open Service Ports:** Unsecured open ports can allow unauthorized access or attacks on services running on those ports.

**Default Credentials:** Devices or systems with unchanged default passwords can be easily accessed by attackers.



## Threat Vectors and Attack Surfaces

### Supply Chain:

- **Managed Service Providers (MSPs):** If compromised, can provide access to their client's infrastructure.
- **Vendors:** Their systems, if breached, can act as a gateway to an organization's infrastructure.
- **Suppliers:** A compromise in a supplier's security can have ripple effects on their clients.



## Threat Vectors and Attack Surfaces

### Supply Chain:

- **Managed Service Providers (MSPs):** If compromised, can provide access to their client's infrastructure.
- **Vendors:** Their systems, if breached, can act as a gateway to an organization's infrastructure.
- **Suppliers:** A compromise in a supplier's security can have ripple effects on their clients.

# Vulnerabilities

---



CompTIA Security+ 70 Course Notes

# Vulnerabilities

A vulnerability refers to a weakness in a system that can be exploited by a threat actor, such as a hacker, to gain unauthorized access to or perform unauthorized actions on a computer system.



CompTIA Security+ 70 Course Notes

# Memory injection

Inserting malicious code into a program's memory. The attacker leverages vulnerabilities that allow them to execute arbitrary code. Common techniques include injecting shellcode or scripts into running processes.

Examples includes:

- Code injection
- Buffer Overflows
- DLL injections

Fixed by following secure coding practices such as input validation.



## CompTIA Security+ 70 Course Notes

# Buffer overflow

A buffer overflow occurs when data that is meant to be stored in a buffer, which is a contiguous block of computer memory, exceeds the buffer's storage capacity. This results in adjacent memory locations being overwritten.

Stack-based buffer overflow Example :

- Consider a program that asks for a user's name and stores it in a buffer that can hold 10 characters. If the user enters a name that's 12 characters long, the extra 2 characters could overwrite the adjacent memory. If this adjacent memory is controlling the program's execution flow (e.g., return address for a function), an attacker can manipulate this to execute arbitrary code.

Usually detected during a vulnerability scan.

Fixed by following good coding practices such as checking the length of data before writing it to a buffer.



## CompTIA Security+ 70 Course Notes

# Race conditions

Vulnerability that occurs when the timing of actions affects a system's state and outcome.

The danger arises when the success of a security operation depends on the timing of certain events, and a malicious entity can influence this timing.

Time-of-check to time-of-use (TOCTOU) Vulnerabilities:

- These vulnerabilities happen when a program checks the state of a resource and then uses it after a delay, during which the state may have changed. If an attacker can change the resource between the "check" and "use" steps, they can induce unauthorized behavior.
- Classic TOCTOU bug is found in file access operations. If a program checks for the existence of a file and then opens it, an attacker might swap the file with a symbolic link to a sensitive file after the check but before the use. The program, which now opens the symlink, may inadvertently read, write, or delete sensitive information.



## CompTIA Security+ 70 Course Notes

# Race conditions

### Example:

- Normal excitation of a file in unix:
  - if (access("file", W\_OK) != 0) {
  - exit(1);
  - }
  - fd = open("file", O\_WRONLY);
  - write(fd, buffer, sizeof(buffer));
- Attack:
  - if (access("file", W\_OK) != 0) {
  - exit(1);
  - }
  - symlink("/etc/passwd", "file");
  - fd = open("file", O\_WRONLY);
  - write(fd, buffer, sizeof(buffer));



CompTIA Security+ 70 Course Notes

## Malicious update

Attacker attempts to install a fake update to an operating system that actually weakens the security of the operating system.

Can be protected by using code signing from the operating system maker.



## Operating system (OS)-based

Weaknesses in the OS that can be exploited to gain unauthorized access, elevate privileges, etc.

Usually resolved by updating the operating system.

Many companies still use OS that are not supported anymore such as Windows XP and Windows 7.

- This leads to no updates being available to the operating systems.



## CompTIA Security+ 70 Course Notes

### Structured Query Language injection (SQLi)

Attackers insert malicious SQL code into input fields to run unauthorized SQL queries.

Example and Demo:

- <https://www.codingame.com/playgrounds/154/sql-injection-demo/sql-injection>

Can be fixed by using following secure coding practices such as input validation.



## CompTIA Security+ 70 Course Notes

# Cross-Site Scripting (XSS)

security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users.

An XSS vulnerability arises when a web application includes unvalidated or unencoded user input as output on a page.

Example and Demo:

- <https://xss-game.appspot.com/>

Can be fixed by using following secure coding practices such as input validation.



## CompTIA Security+ 70 Course Notes

# Hardware Vulnerabilities

**Firmware Vulnerabilities:** Weaknesses in low-level software that runs on hardware devices.

**End-of-life Hardware:** Devices no longer supported by manufacturers, resulting in unpatched vulnerabilities.

**Legacy Hardware:** Older hardware that may not be compatible with current security measures.



CompTIA Security+ 70 Course Notes

## Virtualization Vulnerabilities

**Virtual Machine (VM) Escape:** An attacker runs code on a VM which allows them to break out and interact with the host system.

**Resource Reuse:** Sensitive data can remain in system resources and be accessed by other processes.



## CompTIA Security+ 70 Course Notes

# Cloud-specific Vulnerabilities

Cloud computing has become increasingly popular, but it also introduces unique vulnerabilities that are specific to its environment.

Cloud-specific vulnerabilities:

- **Data Breaches:** Data stored on cloud servers may be targeted by hackers, potentially exposing sensitive information.
- **Insufficient Identity, Credential, and Access Management:** Weak authentication processes, inadequate credential management, and insufficient access controls can lead to unauthorized access to cloud resources.
- **Insecure Interfaces and APIs:** Cloud services are accessed through interfaces and APIs, which, if not properly secured, can be exploited.
- **System Vulnerabilities:** Cloud infrastructures can be complex and might contain system vulnerabilities. These vulnerabilities, if not addressed, can be exploited by attackers to gain unauthorized access or disrupt services.
- **Account Hijacking:** An attacker gaining access to a user's cloud account can manipulate data, eavesdrop on transactions, and redirect clients to illegitimate sites.



## CompTIA Security+ 70 Course Notes

# Supply chain Vulnerabilities

Refers to the complex network of suppliers involved in the production and distribution of IT products and services. This includes service providers, hardware providers, and software providers.

## Service Provider:

These entities deliver various IT services, including cloud computing, data storage, and networking services.

Security Concerns: Service providers could be a vector for security breaches if their systems are compromised. They have access to sensitive data and often integrate with the internal systems of their clients. Ensuring their security measures are robust is essential to protect against data breaches, unauthorized access, and other cyber threats.



## CompTIA Security+ 70 Course Notes

# Supply chain Vulnerabilities

### Hardware Provider:

- These are the manufacturers and distributors of physical computing devices and components, like servers, routers, and chips.
- Security Concerns: The integrity of hardware is crucial. Hardware can be tampered with at any point in the supply chain, leading to risks like embedded malware or backdoors. Ensuring hardware is sourced from reputable providers and verifying the integrity of the hardware upon receipt are key measures.

### Software Provider:

- Entities that develop and distribute software, including operating systems, applications, and firmware.
- Security Concerns: Software vulnerabilities can be exploited by attackers to gain unauthorized access or disrupt services. This risk is magnified if the software is widely used across multiple organizations. Regular updates, patch management, and security audits are essential to mitigate these risks.



## Cryptographic Vulnerabilities

Refer to weaknesses within cryptographic algorithms or their implementation that can be exploited to breach security.

Can include:

- Algorithm Weaknesses: Some cryptographic algorithms have inherent weaknesses. For example, older algorithms like DES are no longer considered secure because they can be broken with enough computational power.
- Key Management Issues: If keys are not generated, stored, or handled securely, they can be compromised.
- Poor Implementation: This can include programming errors, such as buffer overflows, which can be exploited to gain unauthorized access or information.



CompTIA Security+ 70 Course Notes

## Misconfiguration Vulnerabilities

Refer to improper setup or configuration of software, hardware, or network systems, which can lead to security weaknesses.

Includes:

- Default Settings
- Unnecessary services being enabled
- Inadequate security controls



## CompTIA Security+ 70 Course Notes

# Mobile device Vulnerabilities

Refer to weaknesses that could potentially be exploited by attackers to gain unauthorized access to a device or its data.

## Includes:

- Outdated Operating Systems: Not installing updates can leave known security holes unpatched.
- Unsecured Network Connections: Using unencrypted Wi-Fi or Bluetooth connections can expose data.
- Physical Access: An unlocked or unsecured device can be easily tampered with.
- System Flaws: Inherent weaknesses in the operating system or hardware that can be exploited.
- User Behavior: Such as sharing passwords or clicking on phishing links.



## Mobile device Vulnerabilities

- **Jailbreaking** refers to the process of removing software restrictions imposed by the operating system on devices, particularly iOS devices. For Android, a similar process is known as "**rooting**".
  - Usually done by replacing the OS on the device with an OS that gives you root access.
- **Side loading** is the process of installing applications on a mobile device from sources other than the official app store (like Google Play Store for Android or Apple App Store for iOS).



CompTIA Security+ 70 Course Notes

## Zero-day Vulnerabilities

A security flaw that is discovered by attackers before the vendor of the software is aware of it, or before they have released a patch to fix it.

"Zero-day" refers to the fact that the developers have zero days to fix the issue after it has already been exploited in the wild.

# Signs of Attacks

---



## CompTIA Security+ 70 Course Notes

### Malware

Malware, short for malicious software, is any software intentionally designed to cause damage to a computer, server, client, or computer network.

Malware is a critical threat that encompasses a range of harmful or intrusive software, including:

- Viruses
- Worms
- trojan horses
- Ransomware
- Spyware
- Keyloggers
- Logic bomb
- Rootkit



## CompTIA Security+ 70 Course Notes

### Viruses

A virus is a type of malicious software (malware) designed to spread to other computers.

It typically attaches itself to legitimate software and executes its code when the host software runs

**Propagation:** Unlike worms, which can spread across networks on their own, viruses usually require some form of user action to replicate, such as opening a file or running a program.



## CompTIA Security+ 70 Course Notes

# Viruses

### Infection Mechanisms:

- **File Infector Viruses:** These attach themselves to executable files and spread to other executables when the program is run.
- **Macro Viruses:** These are written in the macro language of applications (like Microsoft Word) and are spread through documents.
- **Boot Sector Viruses:** They infect the master boot record of a hard drive, ensuring they are executed when the computer boots up.

### Detection and Removal:

- **Antivirus Software:** Uses signatures to detect known viruses and heuristics to detect new, unknown viruses.
- **Regular Updates:** Keeping antivirus software updated with the latest virus definitions is crucial for protection.
- **System Scans:** Regular scanning for viruses to detect and remove them from the system.



## CompTIA Security+ 70 Course Notes

### Worm

A worm is a type of malware that **replicates itself** in order to spread to other computers.

Unlike a virus, it does not need to attach itself to an existing program or require user intervention to spread.

Worms typically exploit vulnerabilities in network services to propagate across networks.





## CompTIA Security+ 70 Course Notes

### Worm

Here are several steps and measures that are typically taken:

- Patch Management
- Antivirus and Antimalware Solutions
- Network Segmentation and Access Controls
- Firewalls
- Traffic Filtering
- Disable Unnecessary Services
- User Training and Awareness



## CompTIA Security+ 70 Course Notes

### Trojan

Short for "Trojan horse," is a type of malware that disguises itself as legitimate software or is hidden within legitimate software.

Named after the ancient Greek story of the deceptive wooden horse that led to the fall of the city of Troy.

Trojan often tricks users into loading and executing it on their systems.





## CompTIA Security+ 70 Course Notes

### Trojan

Here are several steps and measures that are typically taken:

- Patch Management
- Antivirus and Antimalware Solutions
- Network Segmentation and Access Controls
- Firewalls
- Traffic Filtering
- User Training and Awareness



## CompTIA Security+ 70 Course Notes

# Ransomware

A type of malicious software designed to block access to a computer system or encrypt files until a sum of money is paid, typically in the form of cryptocurrency.

It's a direct threat to the availability of data and the normal operation of businesses and personal computing use.

Ransomware Characteristics:

- Encryption
- Payment Demand

Distribution Methods:

- Ransomware can spread through phishing emails, malicious web advertisements, and vulnerabilities in software and networks.



## CompTIA Security+ 70 Course Notes

# Ransomware





## CompTIA Security+ 70 Course Notes

### Ransomware

Here are several steps and measures that are typically taken:

- Patch Management
- Antivirus and Antimalware Solutions
- Network Segmentation and Access Controls
- Firewalls
- Traffic Filtering
- User Training and Awareness
- Data Backups



## CompTIA Security+ 70 Course Notes

# Ransomware

A type of malicious software designed to block access to a computer system or encrypt files until a sum of money is paid, typically in the form of cryptocurrency.

It's a direct threat to the availability of data and the normal operation of businesses and personal computing use.

Ransomware Characteristics:

- Encryption
- Payment Demand

Distribution Methods:

- Ransomware can spread through phishing emails, malicious web advertisements, and vulnerabilities in software and networks.



## CompTIA Security+ 70 Course Notes

### Spyware

A type of malware that is designed to gather data from a user or organization without their knowledge or consent.

It can monitor and collect various types of personal and sensitive information, such as internet usage data, login credentials, and confidential information.

#### Characteristics of Spyware:

- Data Collection: It can log keystrokes, capture screen images, record browsing history, and access files.
- Surveillance: Some spyware can activate cameras and microphones to surveil the physical environment.
- Stealth: Spyware typically runs hidden in the background and may be disguised as legitimate software.
- Communication: Collected data is usually transmitted to a third party, often a cybercriminal.



## CompTIA Security+ 70 Course Notes

### Spyware

Here are several steps and measures that are typically taken:

- Patch Management
- Antivirus and Anti-Spyware Software
- Secure Browsing Habits
- Firewalls
- Traffic Filtering
- User Training and Awareness



## CompTIA Security+ 70 Course Notes

### Rootkit

A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence from administrators and other system users.

Rootkits can be installed by a malicious intruder after gaining access to a system or can piggyback on other software installations.



## CompTIA Security+ 70 Course Notes

### Rootkit

Here are several steps and measures that are typically taken:

- Secure System Access
- Antivirus and Anti-Rootkit Tools
- System Hardening
- Patch Management
- Secure Boot:
  - Use hardware and software that supports secure boot processes to prevent unauthorized code from running during system startup.



## CompTIA Security+ 70 Course Notes

### Logic bomb

A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Unlike viruses, logic bombs do not replicate themselves.

They are dormant until triggered by a specific event, such as a date/time, the launch of a program, the deletion of a user account, or a certain command.

#### Characteristics of Logic Bombs:

- Condition-based Trigger: They are activated by conditions written into the code.
- Malicious Intent: Once activated, they perform destructive activities, such as deleting files or corrupting data.
- Stealth: Logic bombs can be hard to detect as they lie dormant until triggered.
- Insider Threat: Often, logic bombs are deployed by disgruntled employees with legitimate access to the system.



## CompTIA Security+ 70 Course Notes

### Logic bomb

Here are several steps and measures that are typically taken:

- Code Reviews and Auditing
- Access Controls
- Change Management
- Regular Backups
- Security Awareness Training
- Antivirus and Antimalware Software



## CompTIA Security+ 70 Course Notes

# Keylogger

A type of surveillance software or hardware that, once installed on a system, has the capability to record every keystroke made on that system.

The primary purpose of a keylogger is to covertly monitor and log all the key presses made by a user, which can include sensitive data like usernames, passwords, credit card numbers, and personal messages.

Keyloggers can be software-based or hardware-based:

- Software Keyloggers: These are programs that get installed on the user's computer. They can be part of a malicious software package, like a virus or a Trojan.
- Hardware Keyloggers: These are small physical devices that can be plugged into a computer, usually between the keyboard and the PC, to capture keystrokes.



## CompTIA Security+ 70 Course Notes

### Keylogger

Here are several steps and measures that are typically taken:

- Antivirus and Antimalware Software
- Access Controls
- Change Management
- Regular Backups
- Security Awareness Training
- Update Operating Systems and Applications
- Two-Factor Authentication (2FA)
- Monitor for Hardware Keyloggers
- Use On-Screen Keyboards



## CompTIA Security+ 70 Course Notes

### Bloatware

Refers to unwanted software that comes pre-installed on a device, typically by the manufacturer, or is included in other software installations.

It is not inherently malicious like malware, but bloatware can slow down systems, take up valuable disk space, and at times, can include vulnerabilities that might be exploited by malicious actors.

Characteristics of Bloatware:

- Pre-installed Applications
- Resource Consumption
- Difficult to Remove
- Potential Security Risks



## CompTIA Security+ 70 Course Notes

# Distributed denial-of-service

A malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

They utilize multiple compromised computer systems as sources of attack traffic.

These systems can include computers and other networked resources such as IoT devices.

### Live DDOS Map

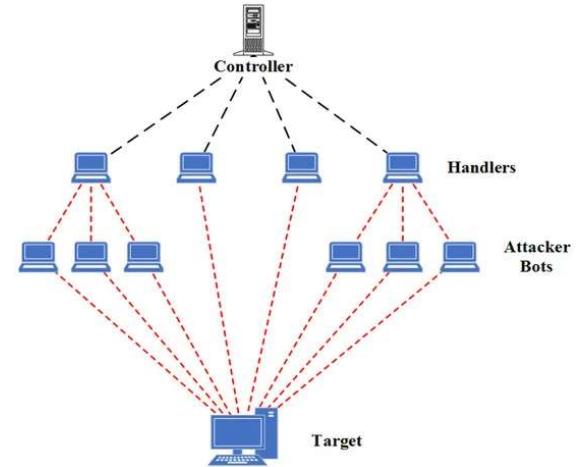
<https://www.netscout.com/ddos-attack-map>



# Distributed denial-of-service

## Network Based DDoS

- A perpetrator uses multiple compromised systems, often infected with a Trojan, to launch a single massive attack. These systems form a network called a botnet.



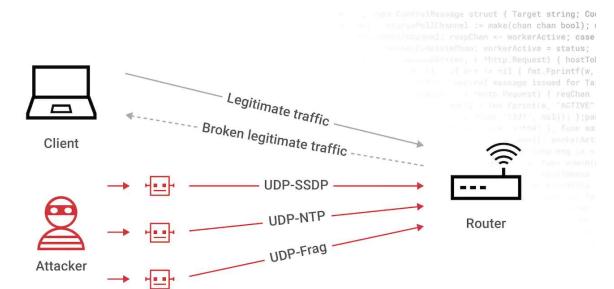
<https://www.mdpi.com/1999-5903/15/2/76>



# Distributed denial-of-service

## UDP Floods

- the attacker overwhelms random ports on the targeted host with IP packets containing UDP datagrams. The aim is to flood the network with enough UDP packets to slow down or crash the targeted system



What is a UDP flood attack?

<https://www.akamai.com/glossary/what-is-udp-flood-ddos-attack>

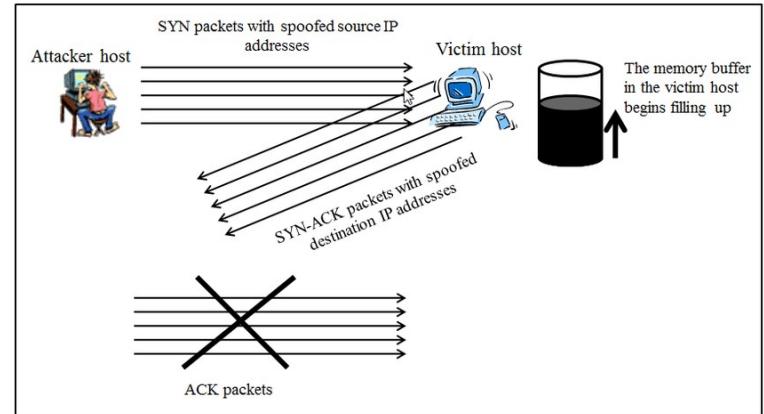


## CompTIA Security+ 70 Course Notes

# Distributed denial-of-service

### SYN Floods

- A SYN Flood is a type of Denial-of-Service (DoS) attack that targets the TCP (Transmission Control Protocol) connection sequence, known as the TCP three-way handshake.
- This attack exploits the way TCP connections are established and can overwhelm a system, rendering it unable to respond to legitimate traffic.



[https://www.researchgate.net/figure/The-TCP-SYN-flood-attack-Hands-on-lab-exercise-on-TCP-SYN-flood-attack\\_fig3\\_320654932](https://www.researchgate.net/figure/The-TCP-SYN-flood-attack-Hands-on-lab-exercise-on-TCP-SYN-flood-attack_fig3_320654932)



## CompTIA Security+ 70 Course Notes

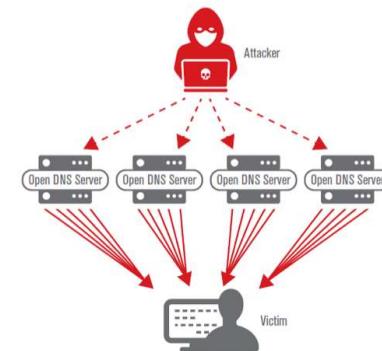
# Distributed denial-of-service

### Amplification Attacks

- These attacks exploit the characteristics of certain protocols to magnify the amount of traffic that is sent to a target, causing a denial of service.
- Uses protocols such as DNS or IP Addressing

### Reflected DDOS

- Characterized by its use of reflection, meaning the attacker forces third-party servers to direct traffic to the victim, often without the third party's knowledge.
- IP Spoofing is one way of doing this.



<https://blog.verisign.com/security/dns-based-threats-dns-reflection-amplification-attacks/>



## CompTIA Security+ 70 Course Notes

# Distributed denial-of-service

Denial-of-service (DDoS) attacks can be mitigated by:

- Increase Bandwidth
- DDoS Protection Services (Cloudflare)
  - <https://www.cloudflare.com/ddos/>
- Network Hardware with DDoS Protection
  - Some network hardware, like routers and firewalls, come with built-in DDoS protection features.



CompTIA Security+ 70 Course Notes

## Domain Name System (DNS)

DNS is essentially the internet's phone book; it translates human-readable domain names (like [www.example.com](http://www.example.com)) into numerical IP addresses that computers use to connect to each other.



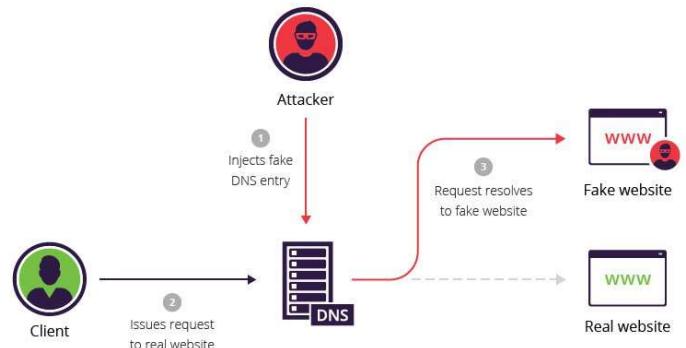


## CompTIA Security+ 70 Course Notes

# Domain Name System (DNS)

Various security concerns and attack vectors:

- DNS Spoofing (or Cache Poisoning): This attack involves corrupting the DNS cache with false information. An attacker can redirect traffic from a legitimate website to a fraudulent one without the user's knowledge. This is often used for phishing attacks.



<https://www.imperva.com/learn/application-security/dns-spoofing/>



CompTIA Security+ 70 Course Notes

## Domain Name System (DNS)

- DNS Amplification Attacks: These are a type of DDoS attack where the attacker exploits publicly-accessible DNS servers to flood a target with DNS response traffic. It's an amplification attack because a small query generates a much larger response in terms of traffic load.



CompTIA Security+ 70 Course Notes

## Domain Name System (DNS)

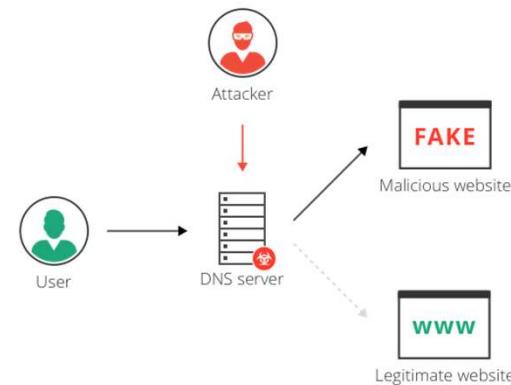
- DNS Tunneling: DNS tunneling involves encoding the data of other programs or protocols in DNS queries and responses. It can be used for legitimate purposes (like bypassing network security controls) but is often used maliciously to exfiltrate data from a compromised system.



## CompTIA Security+ 70 Course Notes

# Domain Name System (DNS)

- DNS Hijacking: In this attack, the attacker diverts queries to a malicious DNS server, leading users to fraudulent websites or intercepting internet traffic. This can be done by compromising the DNS server itself or by modifying the DNS settings in the victim's device.



<https://www.imperva.com/learn/application-security/dns-hijacking-redirection/>



## CompTIA Security+ 70 Course Notes

# Domain Name System (DNS)

- Mitigation Strategies:
  - DNSSEC (DNS Security Extensions): This adds security provisions to the DNS, ensuring that the DNS responses come from the correct source and haven't been tampered with.
  - Securing DNS Servers: Regularly updating and patching DNS servers to protect against vulnerabilities.
  - Monitoring and Analysis: Keeping an eye on DNS traffic for unusual patterns that might indicate an attack.



## CompTIA Security+ 70 Course Notes

### On-path Attack

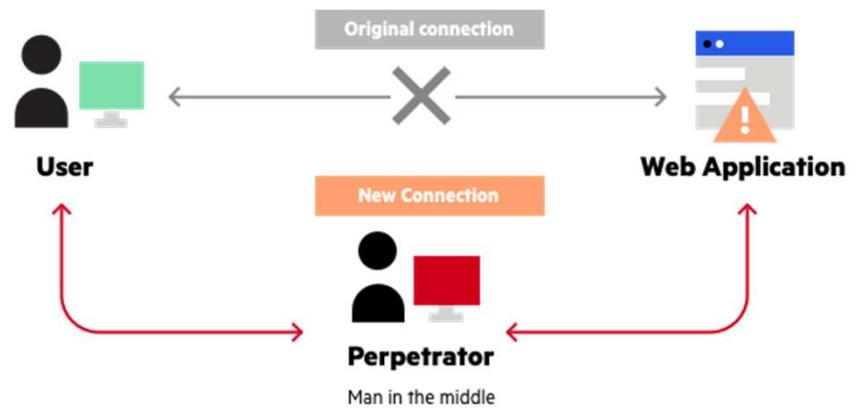
In IT security, the term "On-path" refers to a type of attack where the attacker positions themselves in the communication path between two parties.

This type of attack was previously known as a "Man-in-the-Middle" (MitM) attack.



## CompTIA Security+ 70 Course Notes

### On-path Attack





## On-path Attack

Here's how an on-path attack works:

- **Intercepting Communication:** The attacker intercepts the data traffic flowing between two parties (such as a user and a website). This can be achieved through various means like compromising network equipment, exploiting unsecured Wi-Fi networks, or using ARP spoofing in a local network.
- **Eavesdropping:** In its simplest form, an on-path attack allows the attacker to passively listen to the communication, gaining access to any transmitted information, such as login credentials, personal information, or corporate data.



## On-path Attack

Here's how an on-path attack works:

- **Session Hijacking:** The attacker can hijack sessions, such as web sessions, by stealing session tokens, allowing them to impersonate the victim and gain unauthorized access to systems or information.
- **Data Manipulation:** More sophisticated on-path attackers can alter the communication. They can modify the data being sent between the parties, inject malicious content, or redirect users to fraudulent sites.



## CompTIA Security+ 70 Course Notes

### On-path Attack

Here's how an on-path attack works:

- **SSL Stripping:** In this form of on-path attack, the attacker downgrades a secure HTTPS connection to an unencrypted HTTP connection, enabling them to view and modify the data exchanged.



## On-path Attack

### Mitigation Strategies:

- **Encryption:** Using end-to-end encryption (like **HTTPS**) makes it difficult for an on-path attacker to read or modify the data.
- **Secure Protocols:** Protocols like SSL/TLS and SSH provide secure channels, even over an unsecured network.
- **VPN (Virtual Private Network):** Using a VPN can provide a secure tunnel for data transmission, reducing the risk of on-path attacks.
- **Awareness and Training:** Educating users about the risks of using unsecured networks and the importance of secure communication practices.



## CompTIA Security+ 70 Course Notes

### Credential replay

An attack where an attacker captures and reuses credentials (such as usernames and passwords) to gain unauthorized access to a system.

This attack exploits scenarios where authentication credentials are transmitted over a network or stored in a way that allows an attacker to intercept and reuse them.



## CompTIA Security+ 70 Course Notes

# Credential replay

Here's how it typically works:

- **Credential Capture:** The attacker first needs to capture the credentials. This can be done through various methods, such as using keyloggers, phishing attacks, network sniffers (in cases where credentials are sent over unsecured or poorly secured networks), or through database breaches where credentials are improperly stored.
- **Replay the Credentials:** Once the credentials are obtained, the attacker attempts to use them to log into the system or service for which they are valid
- **Potential for Widespread Access:** If the credentials are reused across multiple systems or services (a common practice known as credential stuffing), the attacker can potentially gain access to a wide range of the victim's accounts.



## CompTIA Security+ 70 Course Notes

# Credential replay

### Mitigation Strategies:

- **Encryption:** Using encryption for data transmission, especially for login processes, can prevent attackers from easily capturing credentials.
- **Two-Factor Authentication (2FA):** Implementing 2FA can significantly mitigate the risk of credential replay attacks, as the second factor (like a one-time code sent to a mobile device) would not be known to the attacker.
- **Regular Password Changes and Strong Password Policies:** Encouraging or enforcing regular password changes and strong, unique passwords for each service can reduce the risks associated with credential replay.
- **Monitoring and Detection:** Systems can be monitored for unusual login attempts, such as from new locations or devices, which might indicate a replay attack.



## CompTIA Security+ 70 Course Notes

### Privilege Escalation

Where an attacker gains elevated access to resources that are normally protected from an application or user. The goal is to obtain higher-level permissions on a system or network.

The attacker starts from a lower permission level and escalates their privileges to gain more control over system components they are not authorized to access.



## Privilege Escalation

There are two main types of privilege escalation:

- **Vertical Privilege Escalation:** This occurs when an attacker gains a higher level of privilege than they are supposed to have. For instance, a regular user gaining administrative access. This type is also known as "privilege elevation."
- **Horizontal Privilege Escalation:** This involves an attacker expanding their control across a network at the same level of privileges. For example, an attacker with restricted user permissions accessing other user accounts at the same level.



## CompTIA Security+ 70 Course Notes

# Privilege Escalation

The process typically involves:

- **Exploiting Vulnerabilities:** Attackers exploit software bugs, design flaws, or configuration oversights in an operating system or software application to gain elevated access.
- **Bypassing Security Mechanisms:** The attacker might bypass security controls that prevent lower-privileged users from executing functions reserved for higher-privileged users.
- **Social Engineering:** Sometimes, privilege escalation involves manipulating people into granting higher-level access.
- **Utilizing Existing Credentials:** If an attacker gains access to higher-privileged user credentials (through techniques like phishing), they can use these to escalate their privileges.



## CompTIA Security+ 70 Course Notes

### Request Forgery

A type of cyber attack where the attacker tricks a user's browser or application into performing an unwanted action on a trusted site where the user is authenticated.

The most common forms of request forgery are Cross-Site Request Forgery (CSRF) and Server-Side Request Forgery (SSRF).



## CompTIA Security+ 70 Course Notes

# Request Forgery

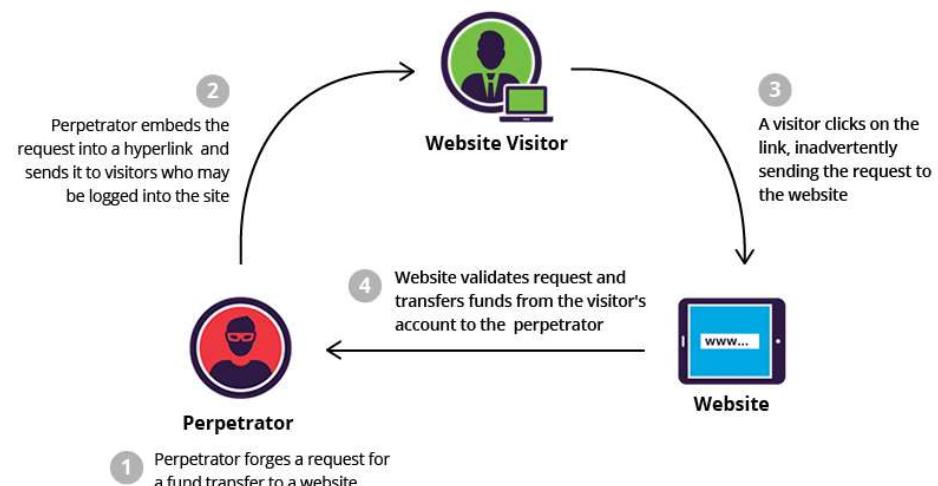
Cross-Site Request Forgery (CSRF):

- In a CSRF attack, the attacker forces a logged-in victim's browser to send a forged request (like changing a password or transferring funds) to a web application.
- The application, unable to distinguish between legitimate requests and forged requests, processes the request.
- CSRF attacks usually exploit the trust that a web application has in the user's browser. For example, if a user is logged into their bank's website and unknowingly visits a malicious site in the same browser, the malicious site could send a request to the bank's site to transfer money without the user's consent.



## CompTIA Security+ 70 Course Notes

# Request Forgery



<https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/>



## Request Forgery

Server-Side Request Forgery (SSRF):

- In an SSRF attack, the attacker manipulates a server to make a request to internal services within the organization or to external third-party systems.
- This is achieved by exploiting a vulnerable application on the server, which then sends a request to an unintended location.
- SSRF attacks can be used to bypass firewalls, access sensitive data, and conduct port scanning of internal networks.



## Request Forgery

### Mitigation Strategies:

#### For CSRF:

- Implement anti-CSRF tokens in applications. These tokens ensure that the requests are generated by the actual user, not by a third party.
- Use of custom headers and checking the 'Referer' header can also help in validating requests.

#### For SSRF:

- Validate and sanitize user input, especially URL inputs that might be used in requests.
- Apply the principle of least privilege to restrict what internal resources can be accessed by the server.
- Use firewalls and network segmentation to limit the reach of requests from web-facing servers.



## CompTIA Security+ 70 Course Notes

### Directory traversal

An attack which aims to access files and directories that are stored outside the web root folder.

By manipulating variables that reference files with "dot-dot-slash (..)" sequences and its variations or by using absolute file paths, it might be possible to access arbitrary files and directories stored on file system including application source code or configuration and critical system files.



CompTIA Security+ 70 Course Notes

# Indicators of Malicious Activity

- **Account Lockout:** Multiple failed login attempts.
- **Concurrent Session Usage:** Single account logged in from multiple locations.
- **Blocked Content:** Firewall or content filters flagging malicious content.
- **Impossible Travel:** Logins from geographically distant locations in a short timeframe.
- **Resource Consumption:** Unusually high CPU, memory, or bandwidth usage.
- **Resource Inaccessibility:** Services or resources being unavailable.
- **Out-of-cycle Logging:** Logs generated outside of expected timeframes.
- **Published/Documented:** Known vulnerabilities or exploits.
- **Missing Logs:** Evidence of logs being deleted or altered.

# Encryption

---



## CompTIA Security+ 70 Course Notes

# Cryptography

Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries.

It involves creating written or generated codes that allow information to be kept secret.

Cryptography both protects information from theft or alteration and can also be used for user authentication.



## Cryptography Main Terms

**Cryptography:** The art and science of hiding the meaning of communications from unintended recipients

**Cryptoanalysis:** The study of methods to defeat codes and ciphers

**Cryptology:** Cryptography + Cryptoanalysis

**Cryptovariables:** Keys are sometimes referred to as cryptovariables



## Goals of Cryptography

**Confidentiality:** Ensuring that information is accessible **only to those authorized to have access**. Encryption plays a crucial role in maintaining confidentiality by converting readable data (plaintext) into a scrambled, unreadable format (ciphertext) that can only be converted back to its original form with the correct decryption key.

**Integrity:** Guaranteeing that information is protected from unauthorized or accidental changes. Cryptographic hash functions, for example, are used to produce a unique hash value for data, which can be used later **to verify that the data has not been altered**.



## Goals of Cryptography

**Authentication:** Verifying the identity of a user, device, or entity in a communication process. For example digital certificates are cryptographic techniques that can confirm the identity of the parties involved in a communication.

**Non-repudiation:** Preventing an entity from denying their involvement in a transaction or activity. Digital signatures ensure that once a party signs a document or a message, they cannot later deny having signed it.



## CompTIA Security+ 70 Course Notes

# Keys vs. Algorithms

### Cryptographic Algorithms:

- These are the methods or procedures used to encrypt and decrypt data. Think of an algorithm as a recipe or set of instructions for the cryptographic process.
- Algorithms define how the encryption and decryption processes are to be carried out. Examples include AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and SHA (Secure Hash Algorithm).
- The strength and security of an algorithm are determined by its ability to withstand cryptanalysis and attacks without being fundamentally flawed.



## Keys vs. Algorithms

### Cryptographic Keys:

- Keys are strings of bits used by the cryptographic algorithms to transform the data. The key is what makes your encrypted data unique.
- The security of encrypted data is directly tied to the length and randomness of the key. The longer and more random the key, the more combinations a potential attacker has to try in order to break the encryption.



## Keys vs. Algorithms

### Key Points to Remember:

- The algorithm is like a lock, while the key is like the key to that lock. The same lock (algorithm) can be used across different instances, but the keys can be different, making each instance unique.
- The security of a cryptographic system relies not just on a strong algorithm but also on the strength and secrecy of the keys.
- Effective cryptography involves not only choosing the right algorithms but also implementing robust key management practices.



## Keys vs. Algorithms

**Kerckhoffs's principle** is a fundamental concept that dates back to the 19th century, formulated by Auguste Kerckhoffs.

It is a guideline for how security systems should be designed and is crucial in the field of cryptography. The principle states:

- "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."



CompTIA Security+ 70 Course Notes

## Keys vs. Algorithms

**Try yourself:**

- Cesar Cipher:
  - <https://www.xarg.org/tools/caesar-cipher/>



## CompTIA Security+ 70 Course Notes

# Ciphers

**Block Ciphers:** Encrypt data in fixed-size blocks (e.g., AES operates on 128-bit blocks). They are suitable for processing large amounts of data.

**Stream Ciphers:** Encrypt data one bit or byte at a time, often used in scenarios where data arrives in a stream (e.g., RC4, although it's now considered insecure). Best for use when the device has limited resources.



## Ciphers

**Substitution Cipher:** Each letter in the plaintext is replaced by another letter. For instance, in the Caesar cipher, each letter in the plaintext is shifted a certain number of places down or up the alphabet.

**Transposition Cipher:** The letters of the plaintext are rearranged according to a certain system. The actual letters are not changed, but their order is altered.



## CompTIA Security+ 70 Course Notes

### Key stretching

A technique used to enhance the security of passwords or other cryptographic keys.

This method involves transforming a relatively weak key, typically a password or passphrase, into a stronger key that is more resistant to attacks, especially brute-force attacks.

**Purpose:** Key stretching is used to strengthen keys that are otherwise considered weak, usually because of low entropy, such as passwords chosen by users.

**Process:** It involves applying a cryptographic hash function to the original key along with some additional data (like a salt) repeatedly for many iterations. This process makes the computation of the final key more resource-intensive.



## CompTIA Security+ 70 Course Notes

### Symmetric Encryption

Symmetric Key Algorithms are a type of cryptographic algorithm that use the same key for both encryption and decryption.

This shared key is used to convert plaintext (readable data) into ciphertext (encoded data) and vice versa.



## Symmetric Encryption

**Key Sharing:** Since the same key is used for both encrypting and decrypting data, it must be shared and kept secret between the communicating parties. Securely distributing and managing this key is a crucial aspect of using symmetric cryptography.

**Speed and Efficiency:** Symmetric key algorithms are generally faster and more efficient than asymmetric key algorithms, making them suitable for encrypting large amounts of data. This efficiency is due to simpler mathematical operations compared to asymmetric cryptography.



## CompTIA Security+ 70 Course Notes

### Symmetric Encryption

**Applications:** Symmetric key algorithms are used in various applications like encrypting data for secure storage, securing data in transit (e.g., in VPNs or wireless networks), and for encrypting files and databases.

**Key Management Challenges:** The major challenge with symmetric key cryptography is key management. Since the same key is used for encryption and decryption, it must be securely shared and stored, which can be challenging, especially in large networks or systems.

**Security:** The strength of a symmetric cipher typically depends on the key length (longer keys are harder to crack due to increased possible combinations) and the security of the algorithm itself.



## CompTIA Security+ 70 Course Notes

# Symmetric Encryption

### Symmetric key problems:

**Key Distribution and Management:** The biggest challenge with symmetric key cryptography is the secure distribution and management of the keys. Since the same key is used for both encryption and decryption, it must be shared among the communicating parties in a secure manner. If a key is intercepted or leaked during distribution, the security of the encrypted data is compromised.

**Scalability Issues:** In a large network, the number of required keys can grow rapidly. For  $N$  users to communicate securely with each other,  $N(N-1)/2$  unique key pairs are needed. This exponential growth makes key management impractical in large systems or networks.



## Symmetric Encryption

### Symmetric key problems:

**Key Storage and Protection:** Keys must be securely stored to prevent unauthorized access. If a key is stolen or exposed, an attacker can decrypt any data encrypted with that key. Secure key storage becomes more complex as the number of users in a system increases.

**Lack of Non-repudiation:** Symmetric key cryptography does not provide non-repudiation since the same key is used by all parties. This means that it cannot be determined which specific user performed an encryption or decryption operation, which is a drawback in scenarios where proof of authorship is important.



## CompTIA Security+ 70 Course Notes

Several different symmetric algorithms

**Data Encryption Standard (DES)** is a symmetric-key 64-bit block cipher

- **DES Specifications**
  - 64-bit Block Cipher
  - 64-bit Key (56 bits effectively since 8 bits are used for parity)
  - DES uses a long series of exclusive OR (XOR) to generate the ciphertext
  - The process is repeated 16 times for each cryptographic operation

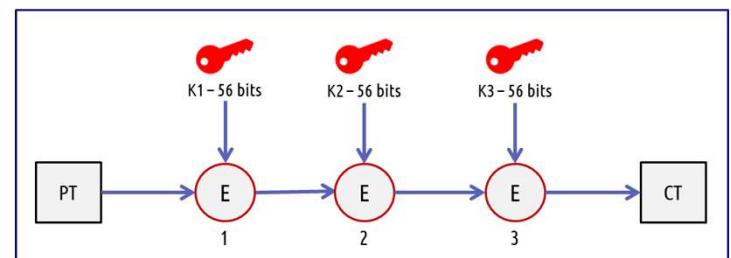


## CompTIA Security+ 70 Course Notes

Several different symmetric algorithms

**Triple-DES (3DES)** applies the DES algorithm three times to each data block

- **Triple-DES Specifications**
  - 64-bit Block Cipher
  - Variable Key Sizes; 64-bit, 112-bit or 168-bit
  - 3 or 2 keys can be used depending on the mode used
  - Effective strength is really 111 bits
  - Approaching end of life, no longer recommended
  - AES would be a faster and stronger replacement





## CompTIA Security+ 70 Course Notes

Several different symmetric algorithms

**International Data Encryption Algorithm (IDEA)** was developed in response to the insufficient key length of the DES

- **IDEA Specifications**
  - 64-bit Block Cipher
  - Variable Key Size: 64 bits or 128 bits
  - Key is divided into 52 16-bit subkeys

**Blowfish** is another symmetric encryption algorithm with larger keys than IDEA

- **Blowfish Specifications**
  - 64-bit Block Cipher
  - Variable Key Size: 32 bits – 448 bits

**Skipjack** is a symmetric encryption algorithm with support for key escrow.

- **Skipjack Specifications**
  - 64-bit Block Cipher
  - 80-bit Key



## CompTIA Security+ 70 Course Notes

Several different symmetric algorithms

**Rivest Cipher 5 (RC5)** is a symmetric algorithm that has not been widely adopted

- **RC5 Specifications**
  - Variable Block Cipher: 32 bits, 64 bits, or 128 bits
  - Variable Key Size: 0 bits or 2048 bits

**Rivest Cipher 6 (RC6)** is a symmetric algorithm developed as the next version of RC5

- **RC6 Specifications**
  - 128-bit Block Cipher
  - Variable Key Size: 128 bits, 192 bits, or 256 bits



## CompTIA Security+ 70 Course Notes

Several different symmetric algorithms

**Rivest Cipher 4 (RC4)** is a symmetric algorithm widely used by WEP and older implementations of SSL and TLS.

- **RC4 Specifications**
  - Stream Cipher
  - Variable Key Size: 40 bits or 2048 bits

**Rivest Cipher 5 (RC5)** is a symmetric algorithm that has not been widely adopted.

- **RC5 Specifications**
  - Variable Block Cipher: 32 bits, 64 bits, or 128 bits
  - Variable Key Size: 0 bits or 2048 bits

**Rivest Cipher 6 (RC6)** is a symmetric algorithm developed as the next version of RC5.

- **RC6 Specifications**
  - 128-bit Block Cipher
  - Variable Key Size: 128 bits, 192 bits, or 256 bits



## CompTIA Security+ 70 Course Notes

Several different symmetric algorithms

**CAST** is a symmetric algorithm that uses a Feistel network

- **CAST-128**
  - 64-bit Block Cipher
  - Variable Key Size: 40 bits - 128 bits
- **CAST-256**
  - 128-bit Block Cipher
  - Variable Key Size: 128, 160, 192, 224, and 256 bit keys

**Two fish** is a symmetric cipher developed to replace Blowfish

- **Two Fish Specifications**
  - 128-bit Block Cipher
  - Variable Key Size: 1-bit - 256 bits
- Uses pre-whitening and post-whitening



## CompTIA Security+ 70 Course Notes

Several different symmetric algorithms

**CAST** is a symmetric algorithm that uses a Feistel network

- **CAST-128**
  - 64-bit Block Cipher
  - Variable Key Size: 40 bits - 128 bits
- **CAST-256**
  - 128-bit Block Cipher
  - Variable Key Size: 128, 160, 192, 224, and 256 bit keys

**Two fish** is a symmetric cipher developed to replace Blowfish

- **Two Fish Specifications**
  - 128-bit Block Cipher
  - Variable Key Size: 1-bit - 256 bits
- Uses pre-whitening and post-whitening



## CompTIA Security+ 70 Course Notes

Several different symmetric algorithms

**Advanced Encryption Standard (AES)** also known as Rijndael (its original name)

- A specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001
- **AES Specifications**
  - 128-bit Block Cipher
  - Variable Key Size: 128 bits, 192 bits, or 256 bits
- **Number of encryption rounds is key size dependent**
  - 128-bit keys require 10 rounds of encryption
  - 192-bit keys require 12 rounds of encryption
  - 256-bit keys require 14 rounds of encryption



## CompTIA Security+ 70 Course Notes

### Symmetric Algorithms Summary

Algorithms	BlockSize	KeySize	Rounds
DES	64	56	16
3 DES	64	112 or 168	48
IDEA (used with PGP)	64	128	8
Blowfish (used with SSH)	64	32 – 448	16
Skipjack	64	80	
RC2	64	128	
RC4	Streaming	128	
RC5 (used with RSA)	32, 64, 128	0 – 2040	255
RC6	128	128, 192, 256	
AES	128	128, 192, 256	10 – 14
Two Fish	128	1 – 256	16



## CompTIA Security+ 70 Course Notes

# Asymmetric Encryption

Asymmetric encryption, also known as public-key cryptography, is a cryptographic system that **uses pairs of keys**: a public key, which may be disseminated widely, and a private key, which is known only to the owner.

Overview of asymmetric encryption:

- Key Pairs:
  - Public Key: Can be used to encrypt and decrypt. Is **shared with anyone**.
  - Private Key: Can be used to encrypt and decrypt. Is **kept with the owner**.
- Encryption and Decryption Process Example:
  - Encryption: A sender encrypts the data using the recipient's public key. Once encrypted, the data can only be decrypted by the corresponding private key.
  - Decryption: The recipient uses their private key to decrypt the data. Since only the recipient possesses the private key, the data remains secure.



## CompTIA Security+ 70 Course Notes

# Asymmetric Encryption

### Advantages:

- Solves the **key distribution problem** of symmetric encryption, as public keys can be shared openly.
- Provides a **method for digital signatures**, which is important for authentication and non-repudiation.

### Disadvantages:

- More **computationally intensive** than symmetric encryption, making it slower for large amounts of data.
- Requires **careful management of the private key**; if the private key is compromised, the security of the system is compromised.

Asymmetric encryption is a cornerstone of modern internet security, providing a means to securely encrypt data and verify identities in a world where trusting communication channels is not always possible.



## CompTIA Security+ 70 Course Notes

### Several different Asymmetric algorithms

#### RSA (Rivest-Shamir-Adleman):

- Description: RSA is one of the earliest and most widely used asymmetric cryptographic algorithms. It's based on the mathematical difficulty of factoring the product of two large prime numbers.
- Key Sizes: Typically ranges from 1024 to 4096 bits for modern security standards.
- Usage: RSA is used for secure data transmission, digital signatures, and key exchange in protocols like SSL/TLS.

#### ECC (Elliptic Curve Cryptography):

- Description: ECC is based on the algebraic structure of elliptic curves over finite fields. It offers a higher degree of security with smaller key sizes compared to RSA.
- Key Sizes: Effective security with significantly smaller keys than RSA (e.g., a 256-bit key in ECC is considered equivalent in security to a 3072-bit key in RSA).
- Usage: ECC is gaining popularity, especially in mobile and wireless environments, due to its efficiency. It's used in applications like secure messaging, cryptocurrency, and SSL/TLS.



## CompTIA Security+ 70 Course Notes

Several different Asymmetric algorithms

### Diffie-Hellman Key Exchange:

- Description: Not an encryption algorithm per se, but a method to securely exchange cryptographic keys over a public channel. It was one of the first public-key protocols.
- Usage: Often used to set up a shared secret key for communication in SSL/TLS and other secure communication protocols.

### ElGamal:

- Description: Based on the Diffie-Hellman key exchange, ElGamal is a public-key cryptosystem for both encryption and digital signatures.
- Usage: It's not as widely used as RSA or ECC but is notable for its mathematical elegance and the basis it provides for other algorithms.



## CompTIA Security+ 70 Course Notes

# Hybrid cryptosystem

System that combines the advantages of both symmetric and asymmetric encryption.

### Combining Symmetric and Asymmetric Encryption:

- Asymmetric Encryption: Used for **secure key exchange**. In hybrid systems, asymmetric encryption is typically used to encrypt and exchange the symmetric key, not the actual data.
- Symmetric Encryption: **Used for encrypting the actual data**. Symmetric algorithms are faster and more efficient than asymmetric ones, making them ideal for encrypting large volumes of data.

### Process of Hybrid Encryption:

- A symmetric key (also known as a session key) is generated for each encryption session.
- The symmetric key is then encrypted using the recipient's public key (asymmetric encryption).
- The encrypted symmetric key is sent along with the encrypted data (using symmetric encryption) to the recipient.
- The recipient uses their private key to decrypt the symmetric key and then uses that symmetric key to decrypt the data.



## CompTIA Security+ 70 Course Notes

### Hybrid cryptosystem

**Efficiency:** Combines the efficiency of symmetric encryption with the secure key distribution of asymmetric encryption.

**Security:** Even if a symmetric key is compromised, it only affects one session (due to the generation of unique session keys).

**Scalability:** More scalable in environments where numerous users or systems are exchanging encrypted data.

**Common Usage:**

- Hybrid encryption is widely used in modern secure communication protocols, such as SSL/TLS, which secures web browsing on the internet.
- Also used in secure email communication, VPNs, and cloud storage services.



## CompTIA Security+ 70 Course Notes

### Hash Function

Refers to the process of converting an input of any length into a fixed-size string of text, using a mathematical function called a hash function

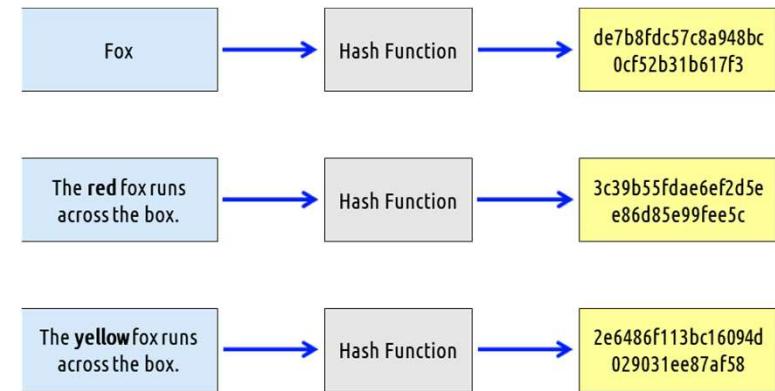
A hash function takes input data (like a message, file, or password) and produces a fixed-size string of characters, which is typically a sequence of numbers and letters known as a hash value or hash digest.

Good hash functions produce unique and distinct hash values for different inputs. Even a small change in the input should result in a significantly different hash value



## CompTIA Security+ 70 Course Notes

### Hash Function



Hash Generator:

<https://passwordsgenerator.net/sha256-hash-generator/>



## CompTIA Security+ 70 Course Notes

# Hash Function

### Characteristics of Hash Functions:

- **Deterministic:** The same input always produces the same hash value.
- **Fast Computation:** Hash functions are typically fast and efficient to compute.
- **Pre-image Resistance:** Given a hash value, it should be computationally infeasible to reconstruct the original input (also known as **one-way property**).
- **Small Changes Lead to Large Differences:** A minor change in the input (even a single character) produces a completely different hash (avalanche effect).
- **Collision Resistance:** It should be extremely unlikely (though not impossible) for two different inputs to produce the same hash value.



## CompTIA Security+ 70 Course Notes

### Collision Hash

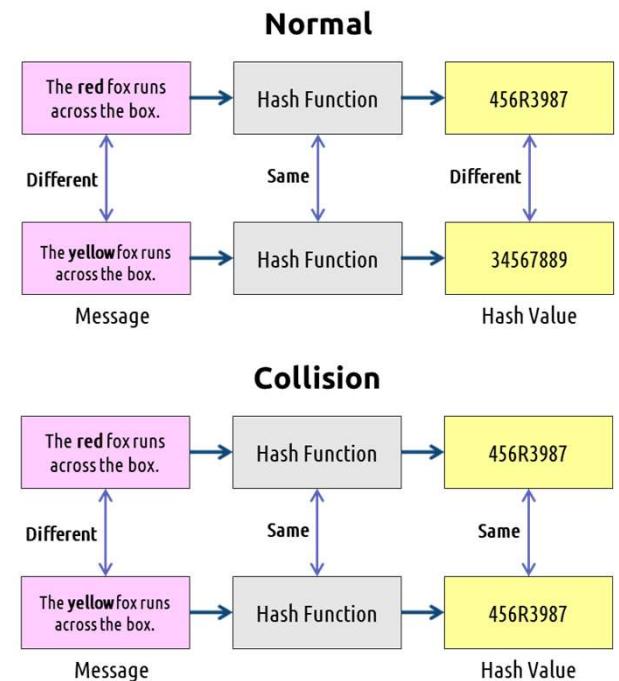
When two different inputs produce the same output

- A sign of weakness
- MD5 today has multiple collision
- Use SHA for forensics or other legal work
- Birthday attack is an example



## CompTIA Security+ 70 Course Notes

### Collision Hash





## CompTIA Security+ 70 Course Notes

# Hash Algorithm

**SHA (Secure Hash Algorithm)** is a series of government hash function standards promoted by NIST.

- Used to produce digital signatures, digital certificates, and various other purposes
- Specified in the Secure Hash Standard (SHS) also known as Federal Information Processing Standard (FIPS) 180.

**SHA-1** processes **512-bit blocks** to produce a **160-bit message digest**

- **Deprecated** by NIST and should no longer be used for any purpose

**SHA-2** processes varying block sizes with varying message digest length.

- **SHA-256** processes **512-bit blocks** to produce a **256-bit message digest**
  - SHA-224 processes **512-bit blocks** to produce a **224-bit message digest**
- **SHA-512** processes **1024-bit blocks** to produce a **512-bit message digest**
  - SHA-384 processes **1024-bit blocks** to produce a **384-bit message digest**

**SHA-3** supports the same modes as SHA-2 and is made as a drop-in replacement.



## CompTIA Security+ 70 Course Notes

# Hash Algorithm

### MD5 (Message Digest 5)

- Processes **512-bit blocks** to produce a **128-bit message digest** in 4 rounds
- It has been demonstrated that MD5 is subject to collisions, preventing its use for ensuring message integrity

**RIPEMD (RIPE Message Digest)** series of hash functions provide an alternative to the SHA series of algorithms.

- Commonly used by cryptocurrencies and SSL/TLS implementations.
- RIPEMD processes **512-bit blocks** to produce a **128-bit message digest** in 48 rounds
  - Insecure should no longer be used
- RIPEMD-128 processes **512-bit blocks** to produce a **128-bit message digest** in 64 rounds
  - RIPEMD-256 processes **512-bit blocks** to produce a **256-bit message digest** in 64 rounds
    - Variant created for when a longer message digest is required
  - Insecure should no longer be used
- RIPEMD-160 processes **512-bit blocks** to produce a **160-bit message digest** in 80 rounds
  - RIPEMD-320 processes **512-bit blocks** to produce a **320-bit message digest** in 80 rounds
    - Variant created for when a longer message digest is required



## CompTIA Security+ 70 Course Notes

### Hash Algorithm

Hash Functions	Hash Value Length
<b>HAVAL</b>	128, 160, 192, 224, & 256 bits
<b>HMAC</b>	Variable
<b>MD5</b>	128
<b>SHA-1</b>	160
<b>SHA-224 (SHA2/SHA3)</b>	224
<b>SHA-256 (SHA2/SHA3)</b>	256
<b>SHA-384 (SHA2/SHA3)</b>	384
<b>SHA-512 (SHA2/SHA3)</b>	512
<b>RIPEMD-128</b>	128
<b>RIPEMD-160</b>	160
<b>RIPEMD-256</b>	256
<b>RIPEMD-320</b>	320



## Digital Signatures

A cryptographic technique used to validate the authenticity and integrity of a message, software, or digital document.

Security and Reliability:

- **Authenticity:** Digital signatures confirm that the signature was created by the known sender (non-repudiation).
- **Integrity:** They ensure the message was not altered in transit.
- **Non-repudiation:** The signer cannot deny the authenticity of their signature on a document since it was created with their private key.



## CompTIA Security+ 70 Course Notes

# Digital Signatures

### Creation of Digital Signatures:

- A digital signature is created using a person's private key, which is part of a key pair (private and public keys).
- The process typically involves taking a message, running it through a hash function to create a message digest, and then encrypting the digest with the signer's private key.

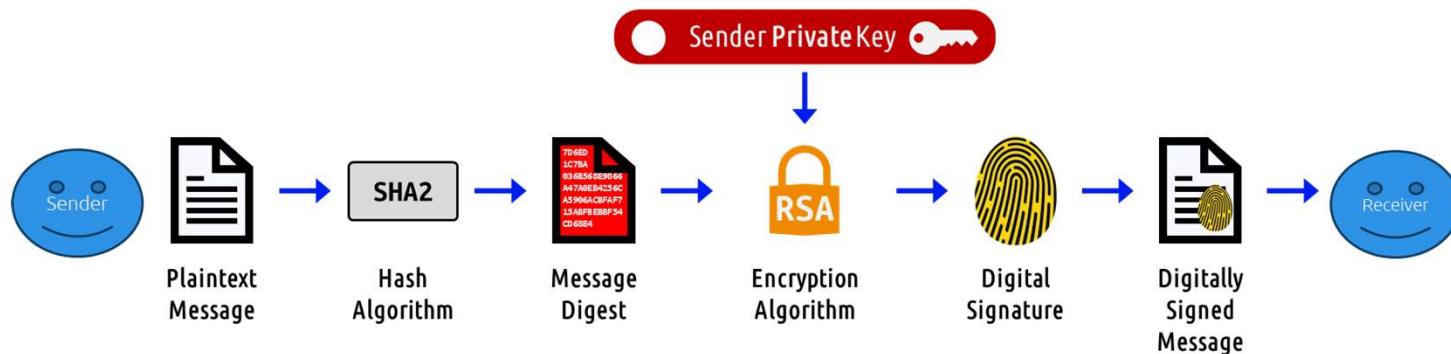
### Verification of Digital Signatures:

- To verify a digital signature, the recipient uses the signer's public key to decrypt the signature.
- The recipient also runs the same hash function on the original message to generate a message digest.
- If the decrypted signature matches the newly generated digest, it confirms that the signature is valid and the message has not been altered.



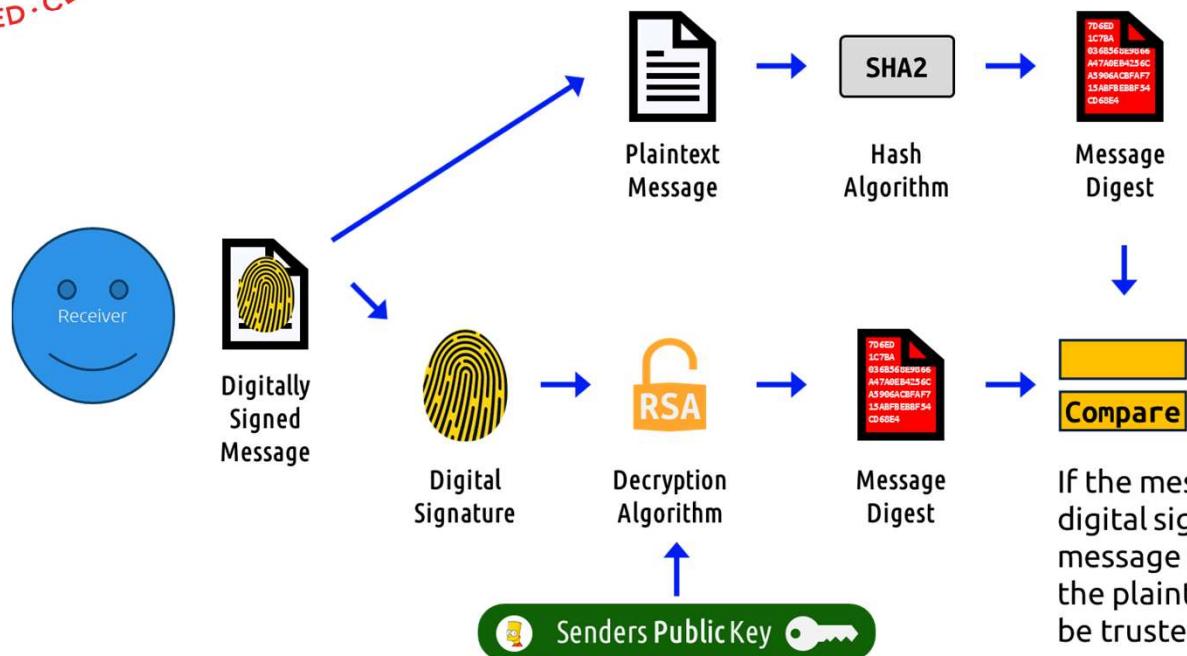
CompTIA Security+ 70 Course Notes

## Digital Signatures





## Digital Signatures



If the message digest from the digital signature matches the message digest produced from the plaintext message, it can be trusted.



## Digital Signature Standard(DSS)

DSS uses the Digital Signature Algorithm (DSA) developed by the U.S. National Security Agency (NSA)

- Generates a digital signature for the authentication of electronic documents
- DSS was put forth by the National Institute of Standards and Technology (NIST) in 1994
- Became the United States government standard for authentication of electronic documents
- Uses SHA2/SHA3 with RSA or DSA or ECDSA



## CompTIA Security+ 70 Course Notes

### Public Key Infrastructure (PKI)

A framework used to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

The purpose of PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking, and confidential email.

#### Functioning of PKI:

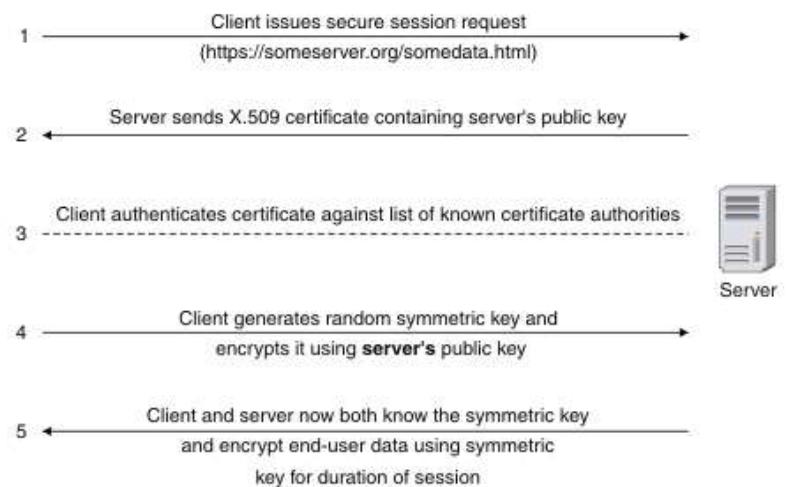
- Encryption and Decryption: PKI allows users to encrypt and decrypt data using public and private keys.
- Digital Signatures: PKI provides for the creation and verification of digital signatures, ensuring the authenticity and integrity of data.
- Certificate Management: The CA issues and revokes certificates as needed. Certificates have a defined lifecycle and must be managed accordingly.

## CompTIA Security+ 70 Course Notes



- 1.** The client sends a request to the server for a secure session. The server responds by sending its X.509 digital certificate to the client.
- 2.** The client receives the server's X.509 digital certificate.
- 3.** The client authenticates the server, using a list of known certificate authorities.
- 4.** The client generates a random symmetric key and encrypts it using server's public key.
- 5.** The client and server now both know the symmetric key and can use the SSL encryption process to encrypt and decrypt the information contained in the client request and the server response.

## SSL Handshake



<https://www.ibm.com/docs/en/cics-tg-zos/9.1.0?topic=ssl-how-connection-is-established>



## CompTIA Security+ 70 Course Notes

### Public Key Infrastructure (PKI)

#### Digital Certificates:

- Provide communicating parties with the assurance that they are communicating with the expected party.
- Certificates are endorsed copies of an individual's public key.
- Users verify that a certificate was signed by a trusted certificate authority (CA)
- Provide data integrity, identification, authentication, non-repudiation, confidentiality, encryption, and digital signature
- Certificates usage
  - Computers/machines
  - Individual users
  - Email addresses
  - Developers (code-signing certificates)



## CompTIA Security+ 70 Course Notes

# Public Key Infrastructure (PKI)

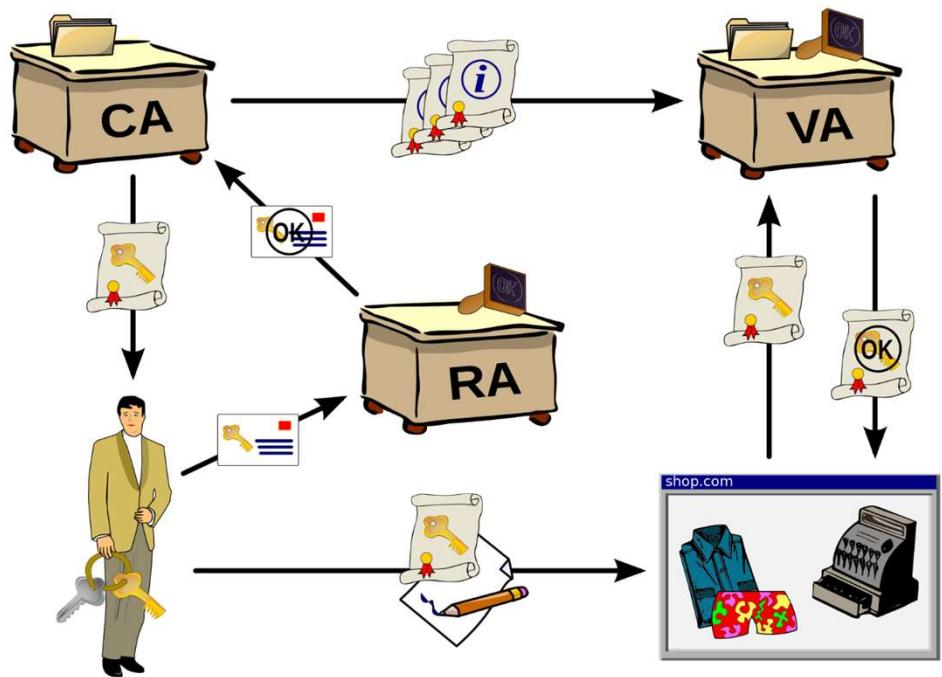
## Key Components of PKI:

- **Digital Certificates:** Electronic documents that contain a public key that use a digital signature to bind a public key with an identity (such as a person or an organization). The certificate provides confirmation that the public key belongs to the specific individual.
- **Certificate Authority (CA):** A trusted entity that issues and manages digital certificates. CA verifies the identity of a certificate applicant before issuing a certificate.
- **Registration Authority (RA):** Often acts as the verifier for the CA before a digital certificate is issued to a requestor.
- **Validation Authority (VA):** Checks if the certificate is still valid.



## CompTIA Security+ 70 Course Notes

### Public Key Infrastructure (PKI)



[https://en.wikipedia.org/wiki/Public\\_key\\_infrastructure](https://en.wikipedia.org/wiki/Public_key_infrastructure)



## CompTIA Security+ 70 Course Notes

# Public Key Infrastructure (PKI)

## Certificate Signing Request (CSR)

- Used to obtain a digital certificate from a Certificate Authority (CA).
- The CSR is a request sent to a CA to apply for a digital identity certificate. It includes information that will be included in the certificate, such as the organization's name, domain name, locality, country, and importantly, the public key. Here's a step-by-step explanation of CSR generation:
- Key Pair Generation:
  - The first step in generating a CSR is to create a key pair, which consists of a public key and a private key. This is usually done using cryptographic software tools.
  - The private key is kept secret and is used to decrypt information encrypted with the public key or to create digital signatures. The public key will be included in the CSR.
- Filling in the Details:
  - The CSR includes important identifying information about the entity requesting the certificate, such as the Common Name (usually the domain name for web server certificates), organization name, organizational unit, city/locality, state/province, and country.
  - This information is used by the CA to create the identity portion of the certificate.



## CompTIA Security+ 70 Course Notes

# Public Key Infrastructure (PKI)

## Certificate Signing Request (CSR)

- Creating the CSR:
  - Using the same software tool that generated the key pair, the entity creates the CSR. The CSR is typically created in a standardized format like PKCS#10.
  - The CSR contains the public key and the identifying information, along with a digital signature produced by the entity's private key. The signature proves that the entity possesses the corresponding private key to the public key in the CSR.
- Submitting the CSR to a RA and CA:
  - The entity then submits this CSR to a RA and CA. This will validate the entity's details – a process that varies in thoroughness depending on the type of certificate.
  - For domain-validated certificates, this might be as simple as responding to an email. For more secure certificates, like Extended Validation certificates will perform a more in-depth verification process.
- Certificate Issuance:
  - Once it has been validated the entity's details, it issues a certificate. This certificate contains the entity's public key and the information from the CSR, and it is digitally signed by the CA.
  - The digital certificate can now be installed on a web server (or other systems) and used for secure communications, ensuring that any communication with the server is encrypted and that the server is verified as being legitimately associated with the domain.



## CompTIA Security+ 70 Course Notes

# Public Key Infrastructure (PKI)

## X.509 Digital Certificates

- X.509 Digital Certificates Attributes
  - Version number
  - Subject name
    - Common name
    - Distinguished name
  - Subject public key
  - Issuer name
  - Validity period
  - Signature algorithm ID
  - Serial number
- Certificate Types
- CA Certificate
  - Grants an organization the ability to be a certificate authority.
- End Entity Certificates
  - Domain Validation (DV) certificate is issued if control of a domain is proven.
  - Extended Validation (EV) certificate is a higher level of assurance if the CA can verify that the applicant is a legitimate business.
- Wildcard Certificates:
  - a wildcard certificate is a type of digital certificate used in SSL/TLS encryption, typically for securing websites.
  - It is a versatile SSL certificate that allows multiple subdomains of a single domain to be secured with a single certificate.
  - \*.tiae.edu.com, \*.Microsoft.com



## CompTIA Security+ 70 Course Notes

# Public Key Infrastructure (PKI)

## Self Signed Vs. Third-party

- Digital certificates can be either self-signed or issued by a third-party Certificate Authority (CA).
- Self-Signed Certificates:
  - Creation: A self-signed certificate is created and signed by the entity it represents, rather than by a trusted third-party CA. Essentially, the creator vouches for itself.
  - Trust Level: These certificates are not inherently trusted by others, as there's no independent verification of the identity of the entity. Trust must be established out-of-band, meaning users must have a separate, secure way to verify the certificate's authenticity.
  - Use Cases: Often used in test environments, internal networks, or applications where the users can reliably verify the certificate's authenticity without needing an external CA. They are also common in situations where the overhead of obtaining a CA-signed certificate is not justified.
  - Cost: There's no cost associated with creating a self-signed certificate.



## CompTIA Security+ 70 Course Notes

# Public Key Infrastructure (PKI)

## Self Signed Vs. Third-party

- Third-Party Certificates (CA-Signed Certificates):
  - Creation: A third-party certificate is issued and signed by a trusted CA. The CA verifies the identity of the entity requesting the certificate, ensuring that the entity is who it claims to be.
  - Trust Level: High. Because a trusted CA verifies the identity of the certificate holder, these certificates are inherently trusted by users and systems that trust the CA. This trust is central to most secure internet communications, like HTTPS.
  - Use Cases: Widely used on the public internet for websites, email servers, and other public-facing services where establishing trust with end-users is essential. CA-signed certificates are a cornerstone of secure online transactions and communications.
  - Cost: Obtaining a certificate from a CA typically involves a cost, which varies depending on the type of certificate and the level of validation provided by the CA.

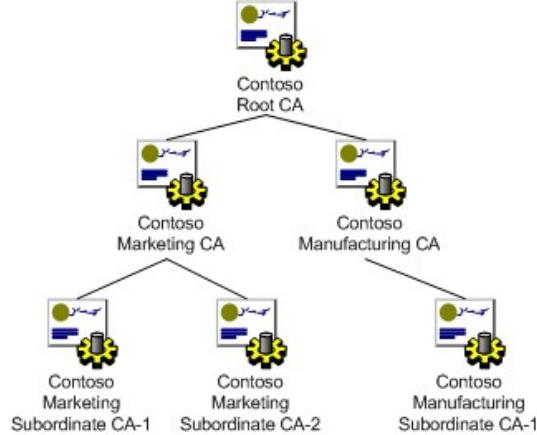


## CompTIA Security+ 70 Course Notes

# Public Key Infrastructure (PKI)

## Root of Trust

- Refers to the trust anchor in a Public Key Infrastructure (PKI) system. This is usually a root certificate authority (CA) that is inherently trusted, and from which the trustworthiness of all other certificates in the network is derived.



<https://learn.microsoft.com/en-us/windows/win32/seccertenroll/about-certificate-hierarchy>



## CompTIA Security+ 70 Course Notes

### Public Key Infrastructure (PKI)

**Verification** is done when user wants to validate your certificate on your device or app.

**Certificate Pinning** a technique that helps to prevent MITM attacks by hardcoding the SSL/TLS certificate's public key into the app or device.

- This means that when the app or device communicates with the server, it will compare the server's SSL/TLS certificate's public key with the one that is hardcoded into the app or device

#### Verification Process

1. Verify the digital signature of the CA is authentic
2. You trust the CA
3. The certificate is not listed on a **CRL (Certificate Revocation List)** or the **OCSP (Online Certificate Status Protocol)**.
4. The certificate actually contains the data you are trusting



## CompTIA Security+ 70 Course Notes

### Public Key Infrastructure (PKI)

**Revocation** is done when a certificate is compromised, issued by accident, certificate details change, or the security association changes.

- **Certificate Revocation Lists (CRL)** contain the serial numbers of certificates that have been revoked.
- **Online Certificate Status Protocol (OCSP)** provides a means for **real-time** certificate verification.
  - Clients send an OCSP request to the CA's OCSP server when they receive a certificate.
- **Certificate Stapling** avoids the client sending OCSP request, instead the webserver itself checks validates the certificate with the CA.
  - Webserver sends the certificate with a time-stamped validation check to the client.



## CompTIA Security+ 70 Course Notes

### Public Key Infrastructure (PKI)

**Revocation** is done when a certificate is compromised, issued by accident, certificate details change, or the security association changes.

- **Certificate Revocation Lists (CRL)** contain the serial numbers of certificates that have been revoked.
- **Online Certificate Status Protocol (OCSP)** provides a means for **real-time** certificate verification.
  - Clients send an OCSP request to the CA's OCSP server when they receive a certificate.
- **Certificate Stapling** avoids the client sending OCSP request, instead the webserver itself checks validates the certificate with the CA.
  - Webserver sends the certificate with a time-stamped validation check to the client.



## CompTIA Security+ 70 Course Notes

### Steganography

The practice of concealing a message, image, or file within another message, image, or file.

#### Techniques:

- Image Steganography: Hiding information within digital images is one of the most common techniques. This can be done by manipulating the pixels or encoding in an image to include additional data.
- Audio Steganography: Concealing information within audio files, either within the audio data itself or in accompanying metadata.
- Video Steganography: Embedding data within video files, which can include manipulating frames or embedding in metadata.
- Text Steganography: Hiding information within text, which can be done through methods like formatting, using white spaces, or altering certain characters.
- Try yourself:
  - <https://stylesuxx.github.io/steganography/>



## CompTIA Security+ 70 Course Notes

### Blockchain

A decentralized and distributed ledger technology known for its pivotal role in underpinning cryptocurrencies like Bitcoin.

Blockchain is a chain of blocks, where each block contains a list of transactions. Every transaction in the blockchain is secured through cryptographic principles.

The blockchain is decentralized and maintained across a network of computers (nodes), making it resistant to central points of failure and control.

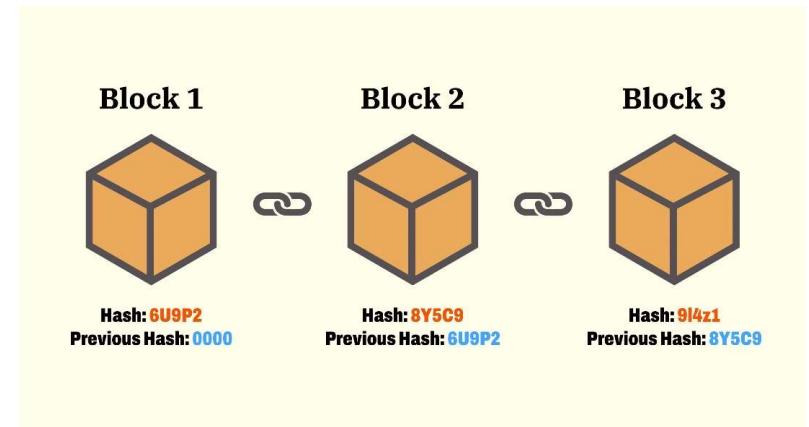
#### Cryptography in Blockchain:

- Hash Functions: Each block contains a cryptographic hash of the previous block, chaining them together. This ensures that once a block is added to the chain, it cannot be altered without changing all subsequent blocks, which requires consensus across the network.



CompTIA Security+ 70 Course Notes

## Blockchain



<https://money.com/what-is-blockchain/>



## CompTIA Security+ 70 Course Notes

### Blockchain

#### Open public ledger

- a decentralized and transparent record-keeping system. This ledger is accessible to anyone and provides a permanent record of all transactions or events that have occurred within a network.



## CompTIA Security+ 70 Course Notes

### Salting

A technique used to enhance the security of stored passwords or other sensitive data. It involves adding a unique, random string of characters, known as a "salt," to each password before it is hashed.

#### How Salting Works:

- When a user creates or updates a password, the system generates a random salt.
- This salt is appended to the actual password, and then the combined string (password + salt) is hashed using a cryptographic hash function.
- The resulting hash, along with the salt, is stored in the database.
- Each user's password has a unique salt, even if two users have the same password.

#### Verification Process:

- When a user logs in, the system retrieves the salt associated with the user's account from the database.
- It appends this salt to the provided password and hashes the combination.
- The system then compares this hash to the stored hash. If they match, the password is correct.

#### Link:

- [https://en.wikipedia.org/wiki/Salt\\_\(cryptography\)](https://en.wikipedia.org/wiki/Salt_(cryptography))



## CompTIA Security+ 70 Course Notes

### Trusted Platform Module

A specialized hardware component designed to secure hardware by integrating cryptographic keys into devices.

#### Functionality and Purpose:

- A TPM is a secure crypto-processor that is designed to carry out cryptographic operations. It includes multiple physical security mechanisms to make it tamper-resistant.
- The primary purpose of a TPM is to safeguard the system at the hardware level, providing a more secure environment than software alone can offer.

#### Key Features:

- Secure Generation and Storage of Cryptographic Keys: TPMs can generate encryption keys, keeping the private portions of those keys safe within the TPM itself.

#### Applications:

- Disk Encryption: TPMs are often used in conjunction with disk encryption software (like BitLocker on Windows) to securely store the encryption keys.
- Secure Boot and System Integrity: TPMs can store and manage the keys used in the process of verifying the boot process, ensuring that only trusted software is loaded during system start-up.



## CompTIA Security+ 70 Course Notes

### Secure Enclave

A Secure Enclave provides a highly secure space within a device where sensitive data can be stored and cryptographic operations can be performed, isolated from the main operating system and processor.

**Data Protection:** It ensures that sensitive data (like fingerprints, facial recognition data, or cryptographic keys) is stored in an environment that is segregated from the rest of the device's operating system and apps, protecting it from potential vulnerabilities or malware.

#### Key Features:

- **Hardware Isolation:** The data and operations within the Secure Enclave are isolated at the hardware level, offering protection against software attacks.
- **Limited Access:** Access to the data and operations within the enclave is tightly controlled and limited, even for the operating system.
- **Tamper Resistance:** Secure Enclaves are designed to be tamper-resistant, making physical attacks difficult.



## CompTIA Security+ 70 Course Notes

### Data Obfuscation

The process of disguising confidential or sensitive data to protect it from unauthorized access

Three main types of data obfuscation:

- Data masking
  - Creates a substitute version of a dataset. The data values are changed, but the format remains the same.
  - An organization can run tests or training sessions as if it were using the real data without actually compromising that user information. Tokenization
- Encryption
- Tokenization



## CompTIA Security+ 70 Course Notes

### Data Obfuscation

The process of disguising confidential or sensitive data to protect it from unauthorized access

Three main types of data obfuscation:

- Data masking
  - Creates a substitute version of a dataset. The data values are changed, but the format remains the same.
  - An organization can run tests or training sessions as if it were using the real data without actually compromising that user information.
- Tokenization
- Encryption
- Try yourself:
  - <https://obfuscator.io/>



## CompTIA Security+ 70 Course Notes

### Tokenization

The process of substituting sensitive data with non-sensitive equivalents, known as tokens, that have no extrinsic or exploitable meaning or value.

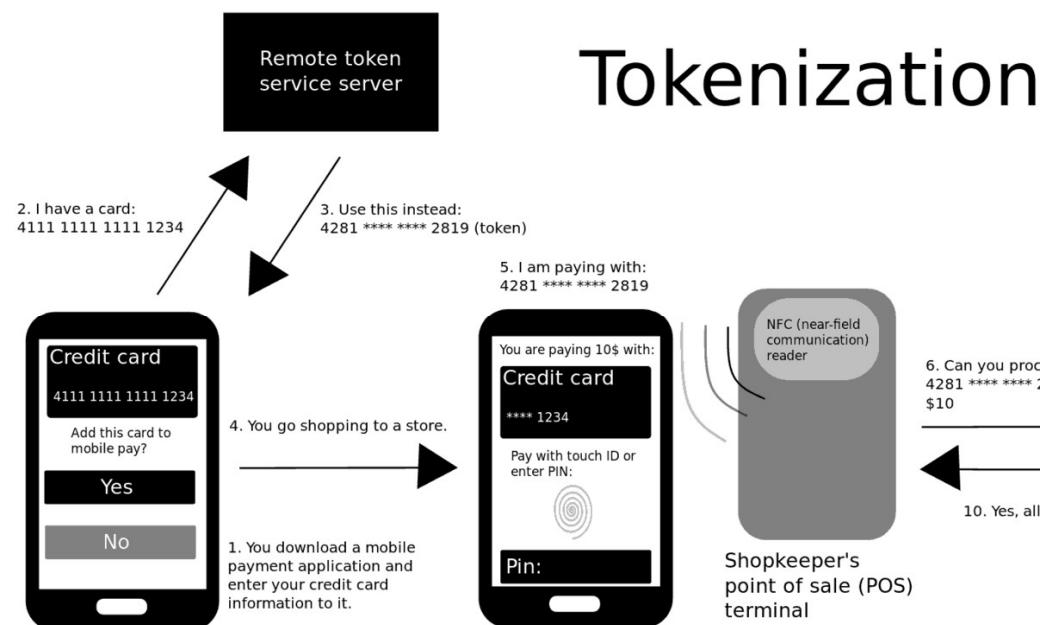
Primary purpose of tokenization is to safeguard sensitive data while maintaining its usability for certain processes or applications.

#### Basic Principle:

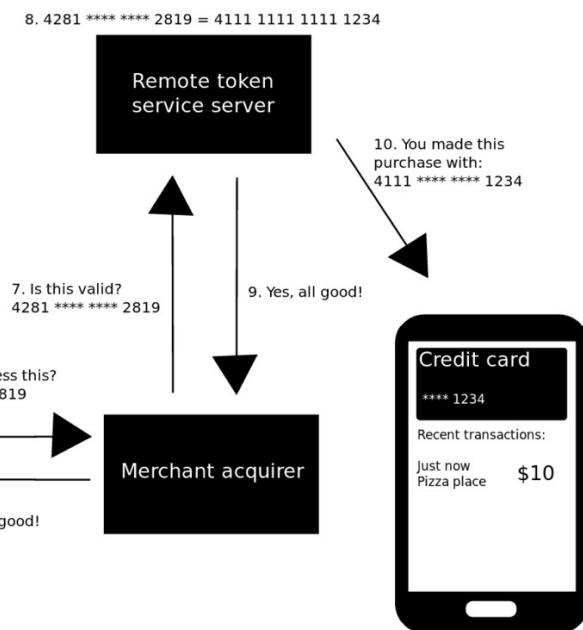
- Data Substitution: In tokenization, sensitive data elements (like a credit card number) are replaced with a randomly generated string of characters, which is the token.
- Reference Mechanism: The actual sensitive data is securely stored in a centralized location, and the token serves as a reference or pointer to this data.



## CompTIA Security+ 70 Course Notes



## Tokenization



[https://en.wikipedia.org/wiki/Tokenization\\_\(data\\_security\)](https://en.wikipedia.org/wiki/Tokenization_(data_security))



## CompTIA Security+ 70 Course Notes

### Key Escrow

Where cryptographic keys are securely stored so that under certain conditions, a third party can access them.

This arrangement is often used to facilitate data recovery, ensure compliance with law enforcement requests, or maintain business continuity.



## CompTIA Security+ 70 Course Notes

### Hardware Security Module

A physical or cloud computing device that provides secure cryptographic processing, key generation and storage, encryption, and decryption services.

#### Secure Cryptographic Processing:

- HSMs perform cryptographic operations like encryption, decryption, digital signing, and key generation within a tamper-resistant hardware device.

#### Key Management:

- They provide a secure environment for managing cryptographic keys throughout their lifecycle, including generation, storage, distribution, archival, and destruction.

#### Cloud HSM's:

- Generate and use cryptographic keys on from a cloud provider such as AWS
  - <https://aws.amazon.com/cloudhsm/>



[https://en.wikipedia.org/wiki/Hardware\\_security\\_module](https://en.wikipedia.org/wiki/Hardware_security_module)



## CompTIA Security+ 70 Course Notes

### Hardware Security Module

- Federal Information Processing Standards (FIPS) 140-2, developed by the National Institute of Standards and Technology (NIST), specifies the requirements for cryptographic modules used within federal information systems.
- Level 1:
  - Basic Security: The lowest level of security, Level 1 provides basic cryptographic capabilities and ensures that the module can perform approved cryptographic algorithms.
  - Physical Security: No specific physical security mechanisms are required beyond the basic requirement that the module must be production-grade and tamper-evident.
  - Application: Suitable for environments where physical security is provided by the surrounding context (like a secure data center) or where a low level of security is acceptable.
- Level 2:
  - Enhanced Security: Adds requirements for physical tamper-evidence and role-based operator authentication to the basic cryptographic capabilities.
  - Physical Security: Requires physical tamper-evidence, meaning any attempt to access the cryptographic module's physical components will leave visible signs of tampering.
  - Application: Appropriate for environments where moderate levels of security are needed and some physical security is present.



## CompTIA Security+ 70 Course Notes

### Hardware Security Module

- **Level 3:**

- Robust Security: Provides stronger physical security measures to prevent the intruder from gaining access to critical security parameters (CSPs) held within the module.
- Physical Security: Requires strong physical security to prevent unauthorized physical access. This includes the use of hard opaque coatings or enclosures designed to leave evidence of tampering and mechanisms to zeroize all plaintext CSPs when an intrusion is detected.
- Application: Suited for high-security environments where it's necessary to thwart attempts at physical access to the cryptographic module.

- **Level 4:**

- Highest Security: Offers the highest level of security and robust protection against environmental attacks.
- Physical Security: In addition to the Level 3 requirements, Level 4 provides complete physical isolation and a high degree of tamper response. It includes environmental failure protections, ensuring that the module remains secure even under fluctuating environmental conditions.
- Application: Ideal for environments where extremely high levels of security are required, and the module may be exposed to hostile operating conditions.

# Social Engineer

---



## CompTIA Security+ 70 Course Notes

### Social Engineering

Refers to a range of malicious activities accomplished through human interactions.

It involves tricking people into breaking normal security procedures and best practices to gain unauthorized access to systems, networks, or physical locations, or for financial gain.





## CompTIA Security+ 70 Course Notes

### Phishing

Phishing attacks typically have one or more of the following objectives:

- Credential Theft
- Financial Fraud
- Malware Distribution
- Identity Theft

Here are several steps and measures that are typically taken:

- User Education
- Email Filtering
- Two-Factor Authentication (2FA)
- Incident Response



## CompTIA Security+ 70 Course Notes

### Vishing: Definition

Malicious actors use **phone calls** to impersonate trusted entities or organizations with the primary goal of manipulating individuals into **disclosing sensitive information** or taking actions that **compromise security**.

Voice Communication:

- Unlike traditional phishing, vishing relies on **spoken communication** through phone calls.



<https://silentbreach.com/BlogArticles/introduction-to-vishing/>



## CompTIA Security+ 70 Course Notes

# Vishing: Key Characteristics

- **Urgent or Coercive Language:** Vishing calls often employ urgency, fear, or intimidation to manipulate victims into **immediate compliance**.
- **Spoofed Caller IDs:** Attackers may manipulate caller IDs to display legitimate-sounding numbers or organizations, increasing their **credibility**.
- **Requests for Sensitive Information:** Vishing calls frequently involve requests for personal identification numbers (PINs), passwords, credit card details, or other **sensitive data**.



<https://www.yubico.com/resources/glossary/vishing/>



## CompTIA Security+ 70 Course Notes

### Vishing: Mitigation

- Education and Awareness: Train individuals to **be cautious of unsolicited phone calls**, recognize vishing attempts, and refrain from sharing sensitive information over the phone.
- Verification: Encourage recipients of phone calls to **independently verify the caller's identity** by calling back on a known and trusted phone number or contact the organization through official channels.
- Use of Authentication: **Implement multi-factor authentication** (MFA) or PIN-based authentication for sensitive transactions over the phone, adding an extra layer of security.



<https://www.g2.com/articles/multi-factor-authentication>





## CompTIA Security+ 70 Course Notes

### Smishing: Definition

Smishing, short for "SMS phishing," is a cyberattack technique where malicious actors use **text messages** to impersonate trusted entities or organizations with the primary goal of manipulating individuals into **disclosing sensitive information** or taking actions that **compromise security**.





## CompTIA Security+ 70 Course Notes

# Smishing: Key Characteristics

- Deceptive Messages: Smishing messages are designed to appear as if they are from **legitimate sources**, and often contain urgent or enticing content to **elicit a quick response** from the recipient.
- Requests for Information: Smishing messages typically **request sensitive information**, such as personal identification numbers (PINs), passwords, credit card details, or other confidential data.
- Spoofed Sender Information: Attackers can **manipulate the sender information** to make it appear as if the message is coming from a trusted source, increasing the likelihood that recipients will fall for the scam.



## CompTIA Security+ 70 Course Notes

### Smishing: Mitigation

- Education and Awareness: Training individuals to **be cautious of unsolicited text messages**, recognize smishing attempts, and avoid clicking on links or sharing sensitive information in response to such messages is a crucial defense.
- Verification: Encourage recipients of suspicious text messages to **independently verify the sender's identity** by contacting the organization or individual through official channels, such as a known and trusted phone number or website.
- Use of Security Software: Employ **mobile security apps** that can detect and block smishing messages. These apps often include features like message filtering and link scanning to protect users from malicious content.



## CompTIA Security+ 70 Course Notes

### Smishing: Mitigation

- Education and Awareness: Training individuals to **be cautious of unsolicited text messages**, recognize smishing attempts, and avoid clicking on links or sharing sensitive information in response to such messages is a crucial defense.
- Verification: Encourage recipients of suspicious text messages to **independently verify the sender's identity** by contacting the organization or individual through official channels, such as a known and trusted phone number or website.
- Use of Security Software: Employ **mobile security apps** that can detect and block smishing messages. These apps often include features like message filtering and link scanning to protect users from malicious content.



## CompTIA Security+ 70 Course Notes

### Spear Phishing

A targeted form of phishing where the attacker customizes their attack emails, messages, or communications to appeal to specific victims.

Unlike general phishing attacks, spear phishing is tailored to particular individuals, often using personal or organizational information to appear more legitimate.





## CompTIA Security+ 70 Course Notes

# Misinformation and Disinformation: Definition

- Misinformation refers to the dissemination of false or inaccurate information, often **unintentionally, without malicious intent**.
- Disinformation, on the other hand, involves the **deliberate** spreading of false or misleading information with the **intent to deceive, manipulate, or harm**.



<https://undark.org/2023/10/26/opinion-misinformation-moral-panic/>



## CompTIA Security+ 70 Course Notes

# Misinformation: Key Characteristics

- Accidental: Misinformation typically occurs **inadvertently** and may result from errors, misunderstandings, or misinformation campaigns.
- Non-Malicious: Individuals or entities spreading misinformation are usually **not acting with harmful intent**.
- Unintentional Consequences: While not deliberate, **misinformation can still lead to security vulnerabilities** if false information is acted upon, potentially causing data breaches or system compromises.





CompTIA Security+ 70 Course Notes

## Disinformation: Key Characteristics

- Deliberate: Disinformation campaigns are carried out with the **intention to deceive** or manipulate, often for political, financial, or competitive gains.
- Malicious Intent: Perpetrators of disinformation **seek to harm**, sow discord, or gain an unfair advantage by spreading false or misleading information.
- Targeted and Coordinated: Disinformation campaigns are often **well-planned**, involving multiple actors and strategies to amplify the false information's impact.



<https://facingtoday.facinghistory.org/when-is-fake-news-propaganda->



# Misinformation and Disinformation: Mitigation

- Media Literacy and Education: Promote media literacy among individuals and organizations to help them **critically evaluate information sources**, identify false information, and differentiate between credible and unreliable content.
- Fact-Checking and Verification: Encourage the use of fact-checking tools and services to **verify information before sharing or acting upon it**. This can help prevent the spread of false information.
- Cyber Hygiene and Security Awareness: **Educate users** about the potential cybersecurity risks associated with misinformation and disinformation, including the importance of verifying the sources of information and avoiding clicking on suspicious links or downloading unverified files.



## CompTIA Security+ 70 Course Notes

### Impersonation: Definition

An attacker **assumes the identity of a legitimate user** to access a system or network.

This can be done through various means such as stealing login credentials, using spoofed email addresses, or mimicking voice or biometric identifiers.



<https://www.cyber.nj.gov/informational-report/impersonation-scams>



## CompTIA Security+ 70 Course Notes

# Impersonation: Key Characteristics

- **Use of Stolen Credentials:** Often involves the **use of credentials** obtained through phishing attacks, keyloggers, or social engineering.
- **Deception and Manipulation:** Attackers may use social engineering tactics to **trick individuals into revealing sensitive information** or credentials.
- **Targets a Range of Systems:** Can be aimed at any platform where user authentication is required.
- **Difficult to Detect:** Since **the attacker appears as a legitimate user**, it can be challenging to detect such intrusions.

A screenshot of a dark blue login interface. At the top, there are input fields for "Username" (containing "username") and "Password" (containing "\*\*\*\*\*"). Below the password field is a "Remember Me" checkbox. At the bottom right are two buttons: "Login" and "Register". To the left of the "Login" button is a yellow padlock icon.

<https://outpost24.com/blog/credential-theft-the-business-impact-of-stolen-credentials/>



## CompTIA Security+ 70 Course Notes

# Impersonation: Mitigation

- Strong Authentication Measures: Implementing **multi-factor authentication** (MFA) which requires more than one method of verification.
- Password Changes and Password Complexity: Change passwords regularly and use complex, hard-to-guess passwords.
- User Education and Awareness Training: **Training users** to recognize phishing attempts and other social engineering tactics.
- Monitoring and Logging: Keeping **detailed logs** and **monitoring systems** for unusual access patterns or login attempts.
- Incident Response Planning: Having a clear **plan for responding** to detected impersonation attempts, including **isolating affected systems** and **changing compromised credentials**.



CompTIA Security+ 70 Course Notes

## Business Email Compromise: Definition

An attacker gains access to a corporate email account and impersonates the owner to defraud the company, its employees, customers, or partners.

Typically, the attacker requests transfers of funds or sensitive data.





CompTIA Security+ 70 Course Notes

## Business Email Compromise: Key Characteristics

- Targeted Email Spoofing: The attacker often **spoofs or hijacks corporate email accounts** to appear legitimate.
- Sophisticated Social Engineering: These attacks usually involve carefully crafted phishing emails and **advanced social engineering tactics** to manipulate employees.
- Financial Motive: BEC attacks are **primarily financially motivated**, often leading to unauthorized fund transfers.
- High Level of Customization: Emails are usually **highly customized and targeted**, using information specific to the business or individual being targeted.
- Lack of Malware: Unlike other cyber attacks, BEC **often doesn't involve malware**, making it **harder to detect** with conventional security tools.



<https://outpost24.com/blog/credential-theft-the-business-impact-of-stolen-credentials/>



CompTIA Security+ 70 Course Notes

## Business Email Compromise: Mitigation

- Employee Education and Awareness: Regular training for employees on recognizing phishing attempts and suspicious email content.
- Email Authentication Protocols: Implementing **email authentication methods** like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance).



## CompTIA Security+ 70 Course Notes

# Pretexting: Definition

Involves **creating a fabricated story** or scenario (the pretext) to deceive a target into divulging sensitive information. The attacker often conducts **extensive research** to make the story as convincing as possible.

Pretexting often involves the attacker pretending to be someone they are not, like a trusted authority figure, to gain the victim's trust.

## THREE TYPES OF PRETEXTING ATTACKS



<https://www.bitlyft.com/resources/unmasking-pretexting-how-to-spot-and-avoid-a-pretexting-attack>



## CompTIA Security+ 70 Course Notes

# Pretexting: Key Characteristics

- Use of Elaborate False Scenarios: Attackers create **believable stories or pretexts** to justify their requests for information.
- Targeting Personal or Sensitive Information: The information sought often includes passwords, financial records, or personal identification data.
- Manipulating Trust: Attackers often **pose as trusted individuals** or authorities, such as bank officials, police, or corporate IT staff.
- High Level of Customization: The scenarios are usually **tailored to the specific target** to increase their effectiveness.





CompTIA Security+ 70 Course Notes

## Pretexting vs Impersonation

While both pretexting and impersonation involve deception and trust manipulation, **pretexting typically relies on a fabricated scenario to extract information.**

Pretexting often involves **more interaction between the attacker and the victim**, with the attacker playing a role that suits the pretext.

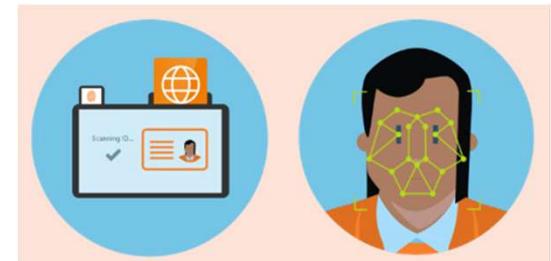
Impersonation **directly assumes the identity of another person**, often using stolen credentials or identities. It's less about building a story and more about **leveraging the existing trust** associated with the assumed identity.



## CompTIA Security+ 70 Course Notes

# Pretexting: Mitigation

- Employee Education and Training: Regular **training sessions for employees** to recognize and respond to pretexting attempts.
- Verification Procedures: Implementing strict **procedures for verifying the identity of individuals** requesting sensitive information.
- Limiting Information Disclosure: **Educating employees** about the dangers of oversharing information, especially in unsolicited calls or emails.
- Incident Reporting Mechanisms: Establishing **clear protocols for reporting** suspected pretexting incidents.



<https://dis-blog.thalesgroup.com/mobile/2018/07/11/identity-verification-service-combating-fraud-and-improving-customer-care/>



CompTIA Security+ 70 Course Notes

## Watering Hole: Definition

A **targeted** cyber attack strategy where the attacker seeks to compromise a **specific group of end users** by infecting **websites they are known to frequently visit**.

The goal is to infect a user's computer and gain access to the network at the user's place of employment.



CompTIA Security+ 70 Course Notes

## Watering Hole: Key Characteristics

- **Targeting Specific User Groups:** The attacker chooses websites that are popular among a particular group, often related to their work, interests, or geographical location.
- **Exploiting Website Vulnerabilities:** The attacker **infects these websites** with malware, often by **exploiting security weaknesses**.
- **Drive-by Downloads or Malicious Redirects:** The attack is often executed through **drive-by downloads** or **redirecting users to a malicious site**, which then installs malware on their device without their knowledge.



## CompTIA Security+ 70 Course Notes

# Watering Hole: Mitigation

- Regular Website Security Audits: For organizations, ensuring that their own websites do not become watering holes through **regular security audits**.
- Employee Awareness and Training: **Educating employees** about the **risks** of visiting untrusted websites and the **signs of a potential compromise**.
- Up-to-date Security Software: Ensuring all systems and software are up-to-date with the **latest security patches and antivirus definitions**.
- Network Segmentation and Monitoring: Implementing **network segmentation** to limit the spread of an attack and **continuous monitoring** for unusual network activities.



<https://www.wizer-training.com/basics/what-is-security-awareness-training-for-employees>





CompTIA Security+ 70 Course Notes

## Brand Impersonation: Definition

This is a type of cyber attack where an attacker mimics or **impersonates the brand identity** of a reputable company to deceive victims, usually for the purpose of stealing sensitive information or spreading malware.

This can occur via emails, websites, social media, or other digital platforms.



<https://www.idagent.com/blog/10-spoofing-facts-you-need-to-see/>



## CompTIA Security+ 70 Course Notes

# Brand Impersonation: Key Characteristics

- Use of Counterfeit Brand Elements: Attackers often use logos, branding styles, and other **visual elements** that closely resemble those of a legitimate brand.
- Phishing Emails and Fake Websites: A common tactic involves sending phishing **emails that appear to be from a trusted brand** or **creating fake websites** that mimic real ones.
- Exploiting Trust in Established Brands: The success of these attacks largely **depends on the victim's trust in the impersonated brand**.
- Targets a Broad Audience: Unlike targeted phishing attacks, brand impersonation can **target a large and diverse group** of individuals who trust or recognize the brand.



## Brand Impersonation: Mitigation

- **Brand Monitoring:** Regularly monitor the internet **for unauthorized uses of the brand's identity**, including domain registrations and social media accounts.
- **Public Awareness and Education:** Inform customers and the public about **how to identify legitimate communications** and websites.
- **Robust Internal Security Measures:** Implementing **strong security protocols** within the organization to **prevent data breaches** that could lend credibility to impersonators.
- **Incident Response Plan:** Having a plan in place to **quickly respond** to instances of brand impersonation, including legal action if necessary.



CompTIA Security+ 70 Course Notes

## Typosquatting: Definition

A form of cyber attack where attackers register domain names that are misspellings of popular websites or **mimic well-known domain names**.

The aim is to **deceive internet users** who make **typographical errors** when entering a URL into their browser, leading them to a **malicious or deceptive website**.



<https://powerdmarc.com/what-is-typosquatting/>



## CompTIA Security+ 70 Course Notes

# Typosquatting: Key Characteristics

- **Similar or Misspelled Domain Names:** The core of typosquatting is the use of domain names that are **slight misspellings or variations of legitimate domain names** (e.g., 'google.com' instead of 'google.com').
- **Exploiting User Mistakes:** The strategy relies on users making **common typing errors or misremembering exact URLs**.
- **Variety of Malicious Intentions:** These sites may host malware, phishing scams, or may be used to sell counterfeit goods or steal personal information.
- **Fake Websites or Redirects:** Typosquatted domains often host websites that **mimic the design of the intended site or redirect users to other malicious sites**.



## CompTIA Security+ 70 Course Notes

# Typosquatting: Mitigation

- Awareness and Training: **Educating employees and users** about the risks of typosquatting and the importance of carefully entering URLs.
- Use of Bookmarks for Important Sites: **Encouraging the use of bookmarks** for frequently visited and critical websites to avoid typing URLs.
- Advanced Web Browsers and Security Tools: Utilizing web browsers and **security tools** that can detect and alert users about suspicious websites.
- Defensive Domain Registration: Organizations should consider **registering common misspellings** of their own domain names to prevent typosquatting.



<https://www.choice.com.au/shopping/online-shopping/buying-online/articles/how-to-spot-a-fake-fraudulent-or-scam-website>

# Securing IT Assets

---



## Segmentation

This is the practice of **splitting a network into multiple segments** or subnets, each functioning as a smaller, separate network.

This division is typically implemented to enhance security, performance, and manageability of the network.

Generally done with Virtual LAN

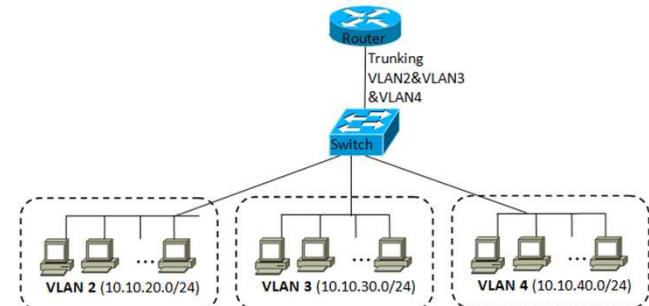


Figure 12.5. 802.1Q trunk between the router and the switch

<https://trac.gateworks.com/wiki/linux/vlan>



## CompTIA Security+ 70 Course Notes

### Isolation

This refers to the process of **completely segregating different parts of a computer network**, system, or application to prevent unauthorized access and minimize the risk of contamination from malicious attacks.

It's a strategy used to contain potential security breaches and limit their impact on the broader system.





# Isolation vs Segmentation

## Key Differences

Level of Separation: Isolation is about **complete separation**, while segmentation is about **dividing a larger entity** into smaller, managed parts.

Interconnectivity: In isolation, the **isolated environments typically do not interact** with each other, whereas in segmentation, different **segments may still have controlled interaction** and connectivity.

Use Cases: **Isolation is often used for highly sensitive operations** or when utmost security is required (e.g., handling classified information), whereas **segmentation is a more common approach** for general network security and management in businesses.



## CompTIA Security+ 70 Course Notes

# Access Control

This is the process of **granting or denying specific requests** to obtain and use information and related information processing services.

Controls access between subjects and objects.

**Users are identified and granted certain rights** to access and perform functions with information systems, networks, or databases.



<https://www.link-labs.com/blog/what-are-access-control-systems-and-how-do-they-work>



## CompTIA Security+ 70 Course Notes

# Principle of Least Privilege

Refers to the practice of limiting access rights for users, accounts, and computing processes to only those resources absolutely required to perform their functions or tasks.

Dictates that individuals or systems should be granted the minimum levels of access – or permissions – necessary to perform their duties.

### Applications:

- **User Access Control:** For employees, access to systems and data is restricted based on their job requirements. For example, a marketing employee may not need access to financial systems.
- **Administrative Accounts:** System administrators may have accounts with extensive privileges for their job, but they should use accounts with standard privileges for routine, non-administrative tasks.
- **Software and Processes:** Applications and services should also operate with the least privilege. They should have only the permissions necessary to function correctly, limiting their ability to access or modify system resources and data.



## CompTIA Security+ 70 Course Notes

# Access Control List

Access Control List (ACL): This is a list used by routers and other network devices to authorize or deny traffic to or from **particular IP addresses, based on a set of rules**.

It is also used in file systems for **managing permissions and controlling access to directories and files**.

A screenshot of the SONICWALL Network Security Appliance interface. The left sidebar shows navigation options like Dashboard, System, Network, and Address Objects. The main pane displays a list of address objects. An entry for "Default ACL Allow Group" is highlighted with a red box. This entry includes a MAC address (00:11:22:33:44:55) and a WLAN name. Other entries include "WLAN Interface IP", "All WAN IP", and "All Interface IP".

Object	Description	Type	Actions
9	WLAN Interface IP	Group	Edit, Delete, Copy
10	All WAN IP	Group	Edit, Delete, Copy
11	All Interface IP	Group	Edit, Delete, Copy
12	All X0 Management IP	Group	Edit, Delete, Copy
13	All SonicPoints	Group	Edit, Delete, Copy
14	All Authorized Access Points	Group	Edit, Delete, Copy
15	All Rogue Access Points	Group	Edit, Delete, Copy
16	Default ACL Allow Group	Group	Edit, Delete, Copy
17	Wireless Client 10 00:11:22:33:44:55 MAC Address: WLAN	Group	Edit, Delete, Copy
18	Default ACL Deny Group	Group	Edit, Delete, Copy
No Entries			
18	Node License Exclusion List	Group	Edit, Delete, Copy

<https://www.sonicwall.com/pt-br/support/knowledge-base/configuring-acls-mac-filter-list-for-individual-virtual-access-point/170503259376841/>



## Filesystem Permissions

These are settings associated with files and directories in a computer's file system that **determine who can read, write, and execute** a particular file or directory.

They are a fundamental aspect of a file system's security and data management.

### User Categories:

- Owner: The **individual who created the file** or directory, typically having full permissions to read, write, and execute.
- Group: A **designated set of users** who share certain access levels to the file or directory.
- Others: **Everyone else who has access to the file system but is not the owner or part of the group.**



## Application Allow List

A control mechanism that **permits only pre-approved applications** to run on a system or network. Applications not on the list are by default disallowed or blocked from running.

This approach is opposite to the more common practice of blocking known malicious applications (blacklisting).





## CompTIA Security+ 70 Course Notes

### Patching

This refers to the process of applying updates ("patches") to software or systems. These patches can fix vulnerabilities, correct bugs, or provide new features.



<https://www.computerworld.com/article/3636790/windows-11-a-guide-to-the-updates.html>



## CompTIA Security+ 70 Course Notes

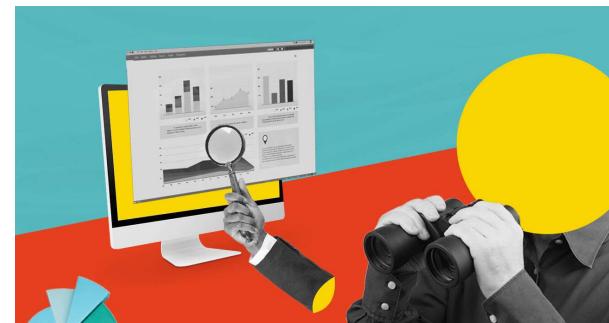
### Monitoring

This refers to the process of continuously and actively examining various aspects of a network, system, or application to ensure that they are operating securely and efficiently.

It includes:

- Tracking system performance
- Detecting unusual or suspicious activities
- Identifying potential security breaches

Uses IDSD/IPS, Firewalls, SIEM's and DLP's.



<https://middleware.io/blog/what-is-infrastructure-monitoring/>



CompTIA Security+ 70 Course Notes

## Configuration Enforcement

Setting up and maintaining hardware and software configurations in an organization according to **predefined security standards and policies**.

It involves **actively managing and enforcing** these configurations to ensure systems remain secure and compliant.





## CompTIA Security+ 70 Course Notes

# Decommissioning

This refers to the process of **formally removing an IT asset** (hardware, software, or system) from operational use.

It involves safely and systematically retiring these assets to **ensure that no security vulnerabilities are introduced** during or after the process.





CompTIA Security+ 70 Course Notes

## Hardening Techniques

Measures and practices taken to **reinforce the security** of a system or network.

The goal is to **reduce vulnerabilities** and **minimize the attack surface** to protect against threats such as unauthorized access, attacks, or data breaches.

These techniques often involve **configuring system and network settings** in a way that **maximizes security**.



## Hardening Techniques

Encryption involves **converting data into a coded format** that can't be easily understood by unauthorized users. It's used to protect data both at rest (like on hard drives) and in transit (like over the internet).

Disabling Ports/Protocols unsurprisingly, involves **disabling unused or unnecessary network ports** and communication protocols on a device to minimize vulnerabilities and reduce the attack surface.

Endpoint protection involves **installing security software on individual devices** (endpoints) like computers and smartphones. This software typically includes antivirus, anti-malware, and sometimes additional features like firewalls and intrusion detection systems.



## Hardening Techniques

A host-based firewall is a software application that controls network traffic to and from **a single host** (like a computer or server), managing what traffic is allowed based on **predefined security rules**.

- Unlike network firewalls that protect a network's perimeter, host-based firewalls provide **granular control over individual device traffic**.

HIPS (Host Intrusion Prevention System) is a **comprehensive security solution** installed on individual hosts. It **monitors and analyzes** system behavior and configurations to prevent unauthorized access and other anomalous activities.



CompTIA Security+ 70 Course Notes

# Hardening Techniques

## Default Password Changes

- This is the practice of **altering the pre-set (default) passwords** that come with hardware and software products.
- Manufacturers often set these default passwords to be the **same for all similar units** for ease of initial setup, but they are usually **well-known** and can be **easily exploited** by attackers.





## CompTIA Security+ 70 Course Notes

# Hardening Techniques

## Removal of Unnecessary Software

- Involves identifying and uninstalling software applications that are no longer needed or pose security risks
- Removing such software can enhance security by reducing the potential attack surface and improve system performance by freeing up resources.
- Reduced Attack Surface: Unnecessary or outdated software can contain vulnerabilities that are exploited by cyber attackers. Removing these applications lessens the number of potential security weaknesses.
- Prevention of Data Breaches: Software that is not regularly updated or is no longer supported can be an easy target for breaches, leading to data theft or loss.

# Security Principles

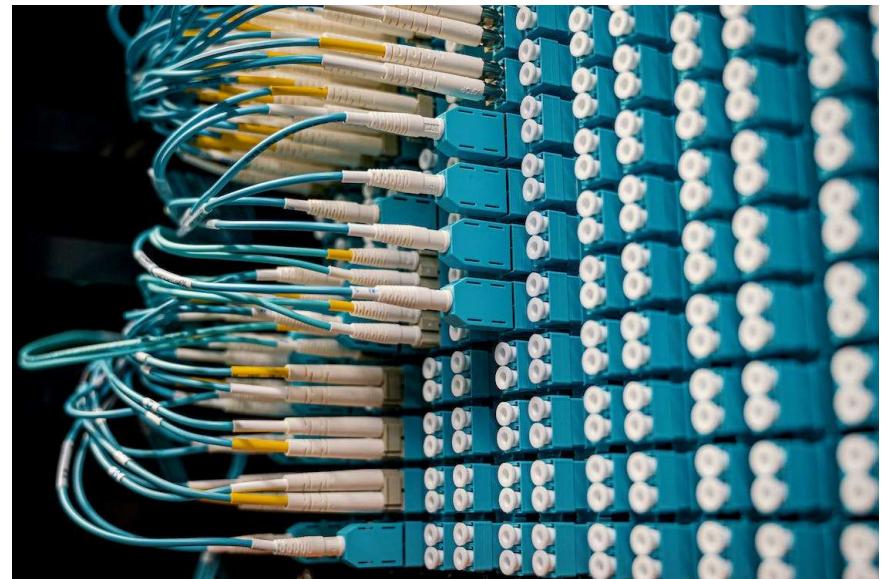
---



CompTIA Security+ 70 Course Notes

## Infrastructure Considerations

Refers to the various aspects of an organization's IT infrastructure that need to be secured and managed to protect against cyber threats.





## CompTIA Security+ 70 Course Notes

# Device Placement

This refers to the **strategic positioning** of hardware components within an IT infrastructure.

This includes considering the **physical and network locations** of devices such as servers, routers, switches, and other network-connected equipment.

**Environmental factors, redundancy, and scalability** are also important considerations.

Effective device placement is crucial for ensuring optimal performance, security, and resilience of the network.



## CompTIA Security+ 70 Course Notes

# Security Zones

These zones are **segments within a network** that have **distinct levels of security controls** and are separated by physical or logical means.

Commonly security zones include **External** zones, **DMZ** zones, and **internal** zones

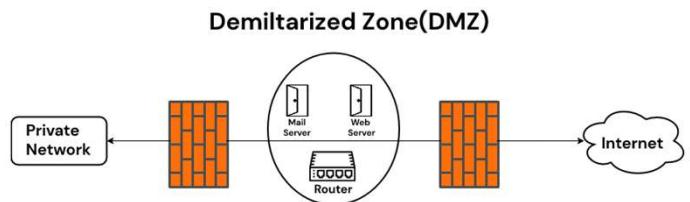
The primary goal is to **control access and exposure** between different areas of the network to enhance security.

For example, an **external** zone may be **more accessible** but would have different security controls than an **internal** zone.



CompTIA Security+ 70 Course Notes

## Security Zones



<https://www.geeksforgeeks.org/what-is-demilitarized-zone/>



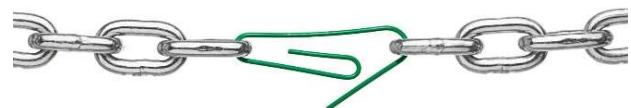
## CompTIA Security+ 70 Course Notes

### Attack Surface

Refers to the **total number of points** where an unauthorized user (the attacker) can try to enter or extract data. It includes all the exposed **areas that are vulnerable to cyber attacks**.

The attack surface encompasses both **physical** and **digital** aspects.

The more complex a system or network, the greater the attack surface.



<https://www.procurious.com/procurement-news/employees-weak-link-cyber-security>



CompTIA Security+ 70 Course Notes

## Failure Modes

These are the **different manners or conditions** under which a system, network, or component can fail to perform its intended function.

This includes both **hardware and software failures** and encompasses scenarios that could lead to **security breaches or data loss**.



<https://krishnappendyala.com/system-failure/>



## Failure Modes: Fail-open vs Fail Closed

In a fail-open scenario, the system defaults to an **open state during a failure**.

- This means if the system fails, it allows access or traffic to pass through.
- In physical security, when a secure systems fail it may fail-open to allow people to get in and out.
- In physical security synonym with fail-safe

In a fail-closed setup, the system defaults to a **closed or locked state when a failure occurs**.

- This means it denies access or stops traffic if a failure is detected.
- In physical security synonym with fail-secure

The choice between fail-open and fail-closed mechanisms is a critical decision in the architecture and configuration of security systems.



CompTIA Security+ 70 Course Notes

## Device Attribute

Device attributes refer to the **inherent properties and operational behaviors** of network security devices.

These attributes determine how the device **interacts with network traffic** and its **role in the network's security architecture**.





CompTIA Security+ 70 Course Notes

## Device Attribute: Active vs Passive

Active devices interact with and **actively modify or influence** the network traffic.

They can make **real-time decisions**, such as blocking, redirecting, or modifying traffic.

---

Passive devices **monitor and analyze** network traffic **without altering** it.

They typically **gather and report** data or alert on suspicious activities.





## Device Attribute: Inline vs Tap/Monitor

In inline mode, the device is placed **directly in the path** of network traffic (hence the term "inline").

**Traffic must pass through the device.**

Essential for **proactive security measures**, where **immediate action** is required against threats.

---

In tap or monitor mode, the device is connected in a way that allows it to **observe traffic passively** without being in the **direct traffic path**.

Ideal for **ongoing monitoring** and **threat detection** without impacting **network performance**.



CompTIA Security+ 70 Course Notes

## Network Appliances

These are **specialized devices** designed to perform **specific functions** within a network, often related to security and data management.

They are typically **optimized** for tasks such as routing, switching, security, load balancing, and storage.

- Sensors
- Jump Server
- Proxy Server
- IDS
- Load Balancer





## CompTIA Security+ 70 Course Notes

### Sensors

Devices or software components that **collect and analyze data** from a network or system to **identify potential security threats** or anomalies.

In cybersecurity exams, questions about sensors might focus on their roles in **detecting and preventing security breaches**, **types of sensors** and their specific uses, and how they **integrate into an overall security infrastructure**.



## CompTIA Security+ 70 Course Notes

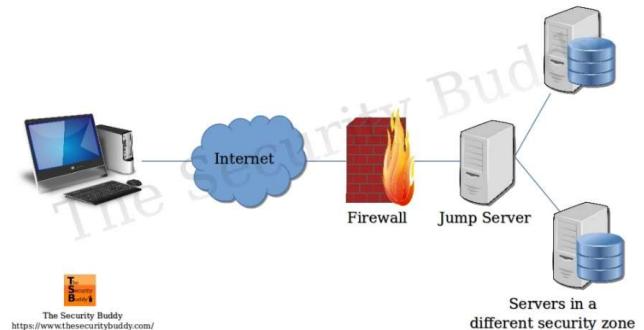
# Jump Server

Is a secure computer that **acts as a controlled entry point into a remote network or server group**.

Essentially, it's a gateway between two networks, often used by system administrators and IT professionals to manage and access devices in a separate security zone.

### Purpose and Function:

- Controlled Access: The jump server is a central point through which administrators connect before launching any management task on remote servers or network devices. This setup enhances security by limiting direct access to the network's critical parts.





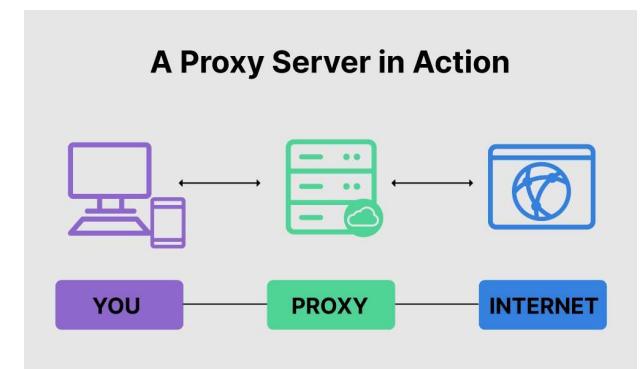
## Proxy Server

A proxy server acts as an **intermediary** between a user's computer and the internet. It requests resources – such as web pages, files, or services – on behalf of the user.

Anonymity and Security: It can **mask the user's IP address**, enhancing privacy and security.

Content Filtering: Often used to **control internet usage** in an organization by blocking access to specific websites.

Caching: Can **cache frequently accessed content** to improve load times and reduce bandwidth usage.





## Proxy Server

**Forward Proxy:** Sits in front of a client and ensures that no direct connection is made between the client and the internet. It can cache content, filter requests, and hide the client's IP address for privacy.

**Reverse Proxy:** Sits in front of web servers and directs client requests to the appropriate backend server. It's commonly used for load balancing, caching, or SSL encryption.

**Open Proxy:** Conceals your IP address from the websites you visit, providing a degree of anonymity online.



## CompTIA Security+ 70 Course Notes

### Intrusion Detection System (IDS)

A technology for real-time monitoring and analysis of network activity and data for potential intrusions and attacks in progress

- Monitor and analyze user and system activities
- Auditing of system and configuration vulnerabilities
- Assess the integrity of critical system and data files
- Recognition of a pattern reflecting known attacks
- Statistical analysis for abnormal activities





## CompTIA Security+ 70 Course Notes

### IDS Detection

#### Knowledge Based Detection

- References a database of previous attack **signatures** and known system vulnerabilities
- The meaning of word signature is the recorded evidence of an intrusion or attack
  - Has **lower false alarm** rates than behavior-based IDS
  - Alarms are more standardized and more easily understood than behavior-based IDS
- **Disadvantages** of knowledge-based systems include these:
  - Signature database must be continually updated and maintained
  - New, unique, or original attacks may not be detected or may be improperly classified



## CompTIA Security+ 70 Course Notes

### IDS Detection

#### Behavior/Anomaly Based Detection

- References a baseline or learned pattern of normal system activity to identify active intrusion attempts
- Build statistical profiles of user activity over time
- Deviations from this baseline or pattern cause an alarm to be triggered
- **Advantages** of behavior-based systems include that they
  - Dynamically adapt to new, unique, or original attacks
  - Are less dependent on identifying specific operating system vulnerabilities
- **Disadvantages** of behavior-based systems include
  - Higher false alarm rates than knowledge-based IDs
  - Usage patterns that may change often and may not be static enough to implement an effective behavior-based IDS



## CompTIA Security+ 70 Course Notes

### IDS Response

When IDs detects an event, it triggers an alarm or alert

**Passive Response** logs the event and sends a notification

- Notifications can be sent to administrators via email, text or pager messages, or pop-up messages
- Alerts can generate reports detailing the activity leading up to the event

**Active Response** changes the environment to block the activity in addition to logging and sending a notification

- Typical responses include modifying ACLs to block traffic based on ports, protocols, and source addresses
- Can disable all communications over specific cable segments



## CompTIA Security+ 70 Course Notes

### Host-Based IDS (HIDS)

A system that monitors a host machine on which it is installed to detect an intrusion and/or misuse

Responds by logging the activity and notifying the designated authority

Advantages:

- Can detect anomalies on the host system that NIDS cannot detect
- Many HIDS include antimalware capabilities

Disadvantages:

- More costly than NIDS
- Require administrative attention on each system
- Can't detect network attacks on other systems
- Often consumes a significant amount of system resources, degrading the system performance
- Easier for an intruder to discover and disable HIDS
- Logs that are maintained in the system are susceptible to modification during a successful attack



## CompTIA Security+ 70 Course Notes

### Network-Based IDS (NIDS)

Used to monitor and analyze network traffic to protect a system from network-based threats

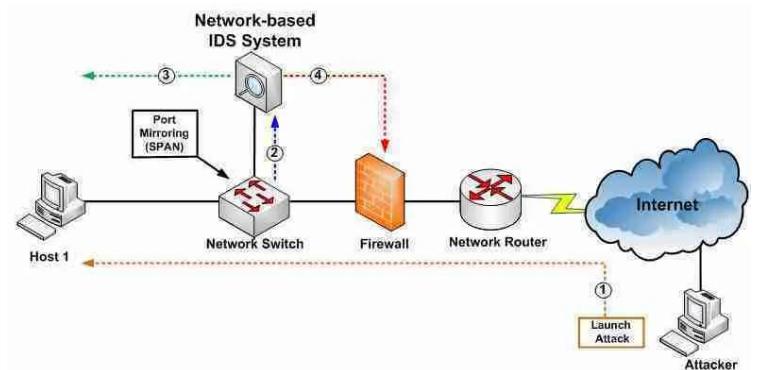
Reads all inbound packets and searches for any suspicious patterns

When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network

Can't monitor the content of the encrypted traffic

Advantages:

- Harder for attackers to discover and disable
- Has very little negative effect on the overall network performance



[https://www.howtonetwork.com/technical/security-technical/intrusion\\_detection\\_and\\_prevention/](https://www.howtonetwork.com/technical/security-technical/intrusion_detection_and_prevention/)



## CompTIA Security+ 70 Course Notes

### Intrusion Prevention Systems(IPS)

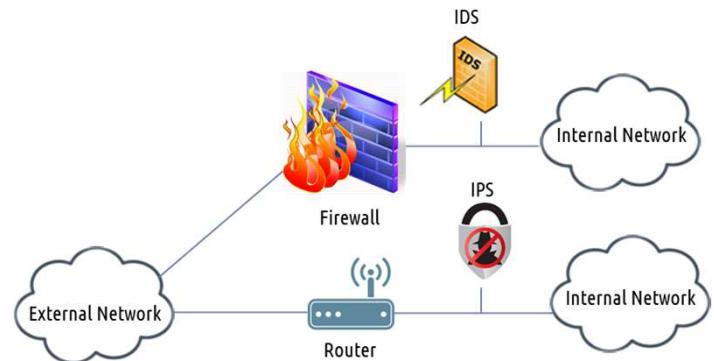
A network security/threat prevention technology

Examines network traffic flows to detect and prevent vulnerability exploits

IPS can choose what traffic to forward and what traffic to block after analyzing it

- This allows IPS to prevent an attack from reaching a target

The active IDS can take steps to block an attack after it starts but cannot prevent it





## CompTIA Security+ 70 Course Notes

# Load Balancer

A device or software that **evenly distributes network or application traffic** across multiple servers to prevent any single server from becoming **overburdened**, which improves overall **performance and reliability**.

**Hardware Load Balancers:** Physical devices specifically designed for load balancing. They are typically more powerful but also more expensive.

**Software Load Balancers:** These are applications that can run on standard hardware or in cloud environments. They offer more flexibility and are often more cost-effective.



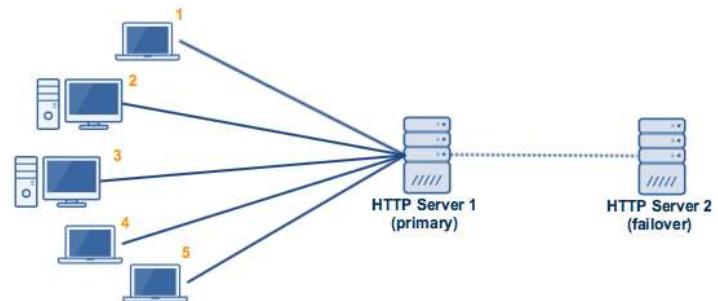


## CompTIA Security+ 70 Course Notes

# Load Balancer Setups

### Active/Passive Setup

- Primary Role: In this configuration, one load balancer is active and handles all the traffic, while the other remains passive (idle) as a standby.
- Failover Mechanism: If the active load balancer fails, the passive load balancer takes over. This switch is typically automated to ensure minimal disruption.
- Usage: Ideal for scenarios where uninterrupted service is critical but where simultaneous operation of two load balancers is not necessary.
- Advantage: Provides a reliable backup in case the primary load balancer fails, ensuring continuity of service.



<https://www.jspa.com/blog/active-active-vs-active-passive-high-availability-cluster>

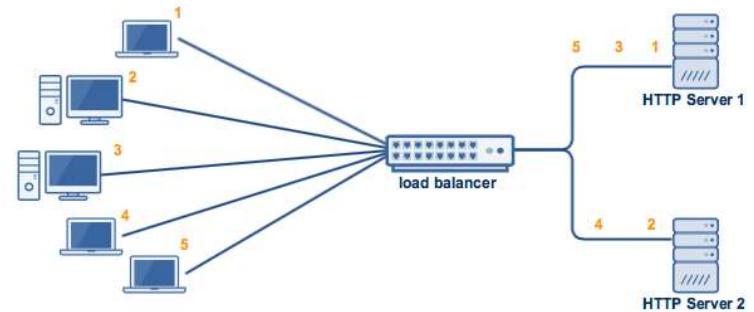


## CompTIA Security+ 70 Course Notes

# Load Balancer Setups

### Active/Active Setup

- Primary Role: Both load balancers are active and share the traffic load simultaneously.
- Load Distribution: Traffic is distributed between the two load balancers based on predefined rules or algorithms (like round-robin, least connections, etc.).
- Usage: Suited for high-traffic environments where load distribution is essential for optimal performance.
- Advantage: Enhances the capacity and reliability of the service, as both load balancers share the workload. If one fails, the other can handle the entire load, reducing the risk of downtime.





CompTIA Security+ 70 Course Notes

## Port Security

Measures and techniques used to secure network ports on computers and network devices, guarding against unauthorized access and ensuring secure communication channels.

Includes:

- Securing Network Switch Ports
- Managing TCP/UDP Ports
- Traffic Filtering

Useful for:

- Preventing Unauthorized Access
- Mitigating Internal Threats
- Reducing Attack Surface



## CompTIA Security+ 70 Course Notes

### 802.1X

This is an **IEEE standard** for port-based Network Access Control (PNAC).

It is used to **authenticate devices** that are attempting to connect to a LAN or WLAN.

How it Works:

When a **device attempts to connect** to a network with 802.1X enabled, the **authenticator blocks all traffic** (except 802.1X traffic) until the client is authenticated.

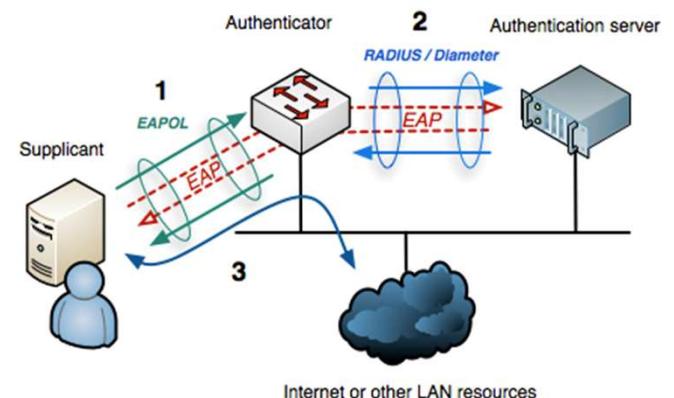
The **suplicant** (client device) **sends credentials** to the authenticator, which forwards them to the **authentication server**.

If the server **approves the credentials**, it instructs the authenticator to **allow access** to the supplicant.



## CompTIA Security+ 70 Course Notes

# 802.1X



[https://en.wikipedia.org/wiki/IEEE\\_802.1X#/media/File:802.1X\\_wired\\_protocols.png](https://en.wikipedia.org/wiki/IEEE_802.1X#/media/File:802.1X_wired_protocols.png)



## CompTIA Security+ 70 Course Notes

### EAP

EAP (Extensible Authentication Protocol) is a **framework** frequently used in network access control for various **authentication** methods.

EAP is designed to support **multiple authentication mechanisms**, including passwords, tokens, certificates, and public key encryption.

**Widely used in protocols** like PPP (Point-to-Point Protocol) and as a part of IEEE 802.1X standard for network access control.

Often used in conjunction with Remote Authentication Dial-In User Service (RADIUS) servers for **centralized authentication** in larger networks.



## CompTIA Security+ 70 Course Notes

# Firewalls

A network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules

Typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted

Implemented in Software or HW (appliances)

Enforces security policies on traffic

Controls the flow of traffic

Does not differentiate data versus commands

Controls flow of traffic between networks or hosts





## CompTIA Security+ 70 Course Notes

# Firewall Types

### Packet Filtering Firewalls:

- The most basic type, which inspects packets and permits or denies them based on source and destination IP addresses, ports, and protocols.

### Stateful Inspection Firewalls:

- More advanced than packet filtering, these firewalls track the state of active connections and make decisions based on the context of the traffic.

### Web Application Firewall (WAF):

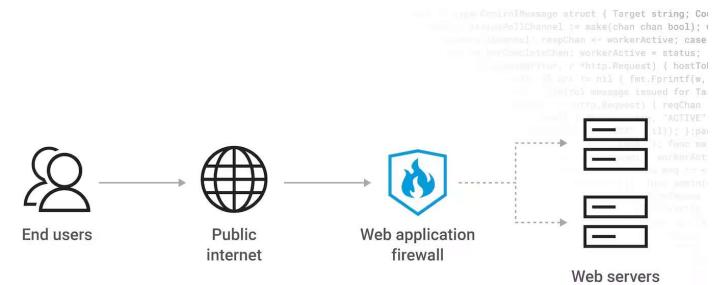
- WAFs are specifically designed to protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.
- They are particularly effective in preventing web application attacks such as cross-site scripting (XSS), SQL injection, and session hijacking.
- WAFs operate at the application layer and apply a set of rules to an HTTP conversation. These rules are generally customized to the application, so they can be more effective in preventing threats specific to the application.
- WAFs can be deployed as hardware, software, or as part of a cloud service.



CompTIA Security+ 70 Course Notes

# Firewall Types

## Web Application Firewall (WAF):



What is a WAF?





## CompTIA Security+ 70 Course Notes

# Firewall Types

### Unified Threat Management (UTM):

- UTMs provide a comprehensive solution that combines multiple security features and services in a single device.
- These features typically include anti-virus, anti-spyware, firewall, intrusion detection and prevention, and content filtering.
- The main advantage of UTM is its simplicity and ease of management, as it consolidates various security functions into one device, making it ideal for small to medium-sized businesses.

### Next-Generation Firewalls (NGFW):

- NGFWs are a more advanced form of the traditional firewall, integrating additional functionalities such as deep packet inspection, intrusion prevention systems, and application awareness.
- **Deep Packet Inspection:** Unlike traditional firewalls, NGFWs go beyond port/protocol inspection and blocking, to inspect the data within the packets themselves, thereby providing more robust security.
- Threat Intelligence Integration: Many NGFWs integrate with threat intelligence services to provide up-to-date information about emerging threats.



## CompTIA Security+ 70 Course Notes

# Layer 4 vs Layer 7

Layer 4 (Transport Layer) and Layer 7 (Application Layer) in the OSI model directly impacts the firewall's **capabilities** and the **types of threats** it can mitigate.

Layer 4 firewalls focus on **data transport** and operate at the transport layer. They control traffic based on **TCP/UDP ports** and **session information**.

Layer 7 firewalls inspect the **content** of the traffic. They can make more **informed decisions** based on actual data and application-specific **behaviors**.





CompTIA Security+ 70 Course Notes

## Securing Communication/Access

This concept encompasses the methodologies and technologies used to ensure that communication over networks is conducted in a **secure** manner and that access to networked resources is controlled and **protected**.





## CompTIA Security+ 70 Course Notes

### Virtual Private Network (VPN)

A technology that creates an encrypted connection over a less secure network

Built on top of existing physical networks

#### Benefits

- Provides secure communication mechanisms
- Protect sensitive data over public networks
- Secure connections between endpoints
- Allow employees to securely access a corporate intranet while located outside the office
- Can securely connect geographically separated offices of an organization, creating one cohesive network
- Creates a secure connection over the public Internet to private networks at a remote location



## CompTIA Security+ 70 Course Notes

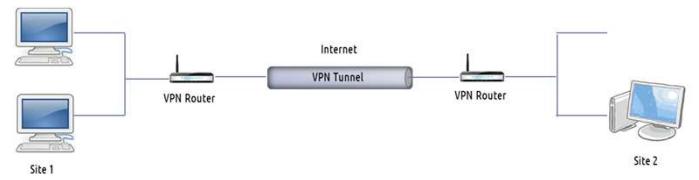
### Virtual Private Network (VPN)

Establishes secure communication paths through the internet between two distant networks

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, data encapsulation, virtual tunneling protocols, or traffic encryption

Tunneling: The encapsulation of a protocol-deliverable message within a second protocol

- The second protocol often performs encryption to protect message contents





## CompTIA Security+ 70 Course Notes

### Tunneling: TLS

Transport Layer Security (TLS) operates at the **transport layer** (Layer 4 of the OSI model).

Uses TLS/SSL for encryption of data

No need to open additional ports, uses port 443.

Mostly used on user access VPN's.

Maybe just a website to access or a client to install

Try Yourself:

- <https://livedemo.sonicwall.com/products/remote-access/ssl-vpn/>



## CompTIA Security+ 70 Course Notes

### Tunneling: L2TP

**L2TP** is a standard protocol for tunneling L2 traffic over an IP network

- Hybrid of Layer 2 forwarding (L2F) and PPTP
- Creates a point-to-point tunnel between communication endpoints
- Uses **IPSec** as the security mechanism
- Supports TACACS+ and RADIUS



## CompTIA Security+ 70 Course Notes

### Tunneling: IP Security (IPSec) Protocol

A standalone VPN protocol

A security mechanism for L2TP

Provides secure authentication and encryption

#### IPSec Components

- Authentication Header (AH)
  - Provides authentication, integrity, and nonrepudiation
  - Has replay protection using sequence numbers
- Encapsulating Security Payload (ESP)
  - Provides encryption to protect the confidentiality of transmitted data
  - Also performs limited authentication



## CompTIA Security+ 70 Course Notes

# Tunneling: IP Security (IPSec) Protocol

### Tunnel Mode

- Payload and headers are protected
- Must decrypt packet at each of the hop
- Final destination is hidden

### Transport Mode

- Payload protected
- Can be routed without decryption
- Final destination is visible



Tunnel Mode: Whole packet is encapsulated

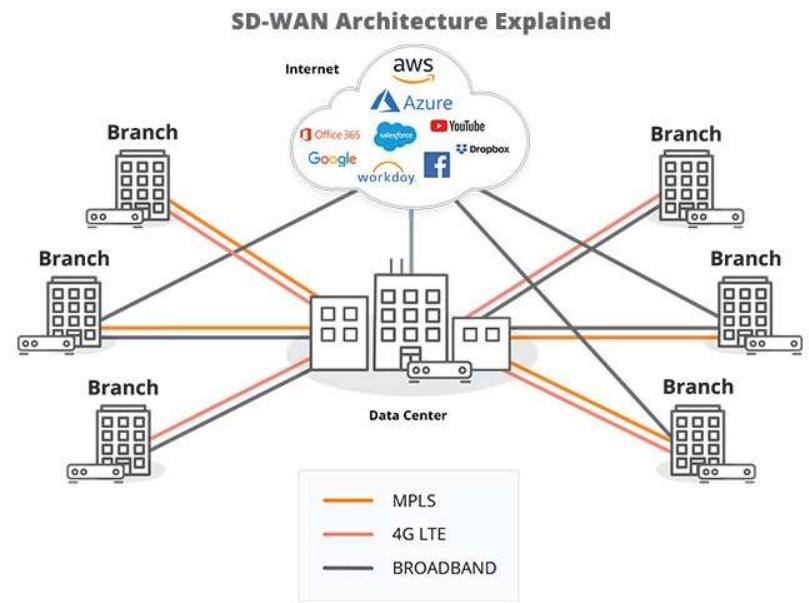


Transport Mode: Only the payload is encapsulated



CompTIA Security+ 70 Course Notes

## SD-WAN



<https://www.arubanetworks.com/faq/what-is-sd-wan/>



CompTIA Security+ 70 Course Notes

## SD-WAN

Software-defined wide area network

Approach to simplify branch office networking and assure optimal application performance.

SD-WAN provides a centralized control function to securely and intelligently direct traffic across the WAN. This ensures more efficient data routing, reduced latency, and improved overall network performance.



## CompTIA Security+ 70 Course Notes

### SASE

Secure Access Service Edge (SASE) is a **cloud-native** networking architecture that combines network security functions with **WAN capabilities** to support the dynamic secure access needs of organizations.

It merges **SD-WAN capabilities** with comprehensive **security services**.

Secure Cloud Architecture: SASE models often use **encrypted tunnels** to connect users directly to **cloud-based services**, ensuring secure and efficient access to applications and data regardless of the user's location.



CompTIA Security+ 70 Course Notes

## Selecting Effective Controls

The process of **identifying** and **implementing** the right security measures to mitigate risks and enhance an organization's overall security.





## CompTIA Security+ 70 Course Notes

# Critical Considerations

Risk Assessment Foundation: The process starts with a thorough **risk assessment** to identify and prioritize potential threats and vulnerabilities.

Layered Defense Approach: Implementing a variety of controls at **different layers** to ensure **no single point of failure**.

Evaluating Cost vs. Benefit: Analyzing the costs of implementing a control against the potential risk reduction benefits.

Adhering to Regulations: Ensuring compliance with relevant **regulations and standards** in control selection.

Technical Suitability: Assessing the **technical compatibility and feasibility** of controls within the existing IT environment.



CompTIA Security+ 70 Course Notes

## Selecting Controls: Key Factors

Addressing Specific Risks: Controls should be **directly relevant** to the risks identified during the risk assessment.

Scalability and Adaptability: Controls should be able to scale with the organization and adapt to **changing threat landscapes**.

Ongoing Evaluation: Regularly monitor, review, and update controls for **continued effectiveness**.

# Security Architecture

---



CompTIA Security+ 70 Course Notes

# Architecture and Infrastructure Concepts

Each architecture and infrastructure model has **unique security implications**.

We will be covering:

- Cloud
- Infrastructure as code (IaC)
- Serverless
- Microservices
- Network infrastructure
- On-premises
- Centralized vs. decentralized
- Containerization
- Virtualization
- IoT
- ICS/SCADA
- RTOS
- Embedded systems
- High availability



# Cloud Characteristics

## Shared resources

- Hardware resources can provide services to devices beyond their physical boundaries
- This provides more flexibility and scalability with resiliency

## Metered utilization

- The cloud is a pay-as-you-go service, you pay for what you use
- This helps optimize cost when using the cloud

## Rapid elasticity

- Resources can be allocated and reallocated as required to optimize resources usage and cost

## High availability

- A hardware failure should have little to no effect on cloud services

## File synchronization

- Makes files available from anywhere you can access the cloud



# Cloud Deployment Models

## Public cloud

- A third-party hosts the equipment for anyone to make use of their service.
- Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine, and Windows Azure Services Platform.

## Private Cloud

- A third-party host the equipment for a single client to have exclusive use of the resources.
- Private clouds are driven by concerns around security and compliance and keeping assets within the firewall.

## Community cloud

- A community cloud is a multi-tenant platform that allows several companies to work on the same platform, given that they have similar needs and concerns.

## Hybrid cloud

- By using a Hybrid approach, companies can maintain control of an internally managed private cloud while relying on the public cloud as needed.



## CompTIA Security+ 70 Course Notes

### Cloud Computing Service Models

#### **Software as a Service**

- Software as a service vendors host the applications, making them available to users via the internet. Metered utilization

#### **Platform as a Service**

- Platform as a service offers developers a platform for software development and deployment over the internet, enabling them to access up-to-date tools.

#### **Infrastructure as a Service**

- Infrastructure as a service is used by companies that don't want to maintain their own on-premises data centers.



## CompTIA Security+ 70 Course Notes

### Cloud Computing Service Models

	SaaS Software as a Service	PaaS Platform as a Service	IaaS Infrastructure as a Service
User	Customer	Customer	Customer
Application	Provider	Customer	Customer
Operating System	Provider	Provider	Customer
Hardware	Provider	Provider	Provider
Network	Provider	Provider	Provider
Facility	Provider	Provider	Provider
Regulatory Compliance	Customer	Customer	Customer

	<ul style="list-style-type: none"><li>The software does NOT require installation instead is accessed via a web browser</li><li>The customer only manages user access</li></ul>	<ul style="list-style-type: none"><li>Customers can develop their own applications and services without the need to manage any infrastructure or operating systems</li></ul>	<ul style="list-style-type: none"><li>Customers manage the operating system, the applications installed, and the access to it</li></ul>
--	--	--	---



## CompTIA Security+ 70 Course Notes

### Cloud

Responsibility Matrix: Cloud computing involves a **shared responsibility model** where security obligations are **divided** between the cloud provider and the client. For instance, the provider might be responsible for securing the infrastructure, while the client must secure their data and applications.

Hybrid Considerations: Hybrid cloud environments, combining on-premises and cloud-based resources, require **careful security integration** and consistent **policy enforcement** across both environments.

Third-Party Vendors: Reliance on third-party vendors in cloud computing **introduces risks** related to vendor security practices and data sovereignty.



## CompTIA Security+ 70 Course Notes

# Infrastructure as Code

**Infrastructure as Code (IaC)** is a concept where hardware is managed like software development.

- Instead of configuring hardware manually it is managed as a collection of elements in the same way that software and code are managed under DevSecOps (security, development, and operations).
- **Hardware infrastructure** is managed like software code with version control, pre-deployment testing, custom-crafted test code, reasonableness checks, regression testing, and consistency in a distributed environment.
- This management approach allows organizations to streamline infrastructure changes so that they occur more easily, more rapidly, more securely and safely, and more reliably
- IaC is not just limited to hardware; it can also be used to oversee and manage virtual machines (VMs), storage area networks (SANs), and software-defined networking (SDN).
- IaC often requires the implementation of configuration management software, such as Puppet.



CompTIA Security+ 70 Course Notes

## Serverless Architecture

**Serverless architecture** is a cloud computing concept where code is managed by the customer and the platform (i.e., supporting hardware and software), or the server is managed by the **Cloud Service Provider (CSP)**.

There is always a physical server running the code, but this execution model allows the software designer /architect/ programmer/ developer to focus on the logic of their code and not have to be concerned about the parameters or limitations of a specific server.

This is also known as **Function as a Service (FaaS)**. Applications developed on serverless architecture are similar to microservices, and each function is crafted to operate independently and autonomously.



## CompTIA Security+ 70 Course Notes

# Microservices

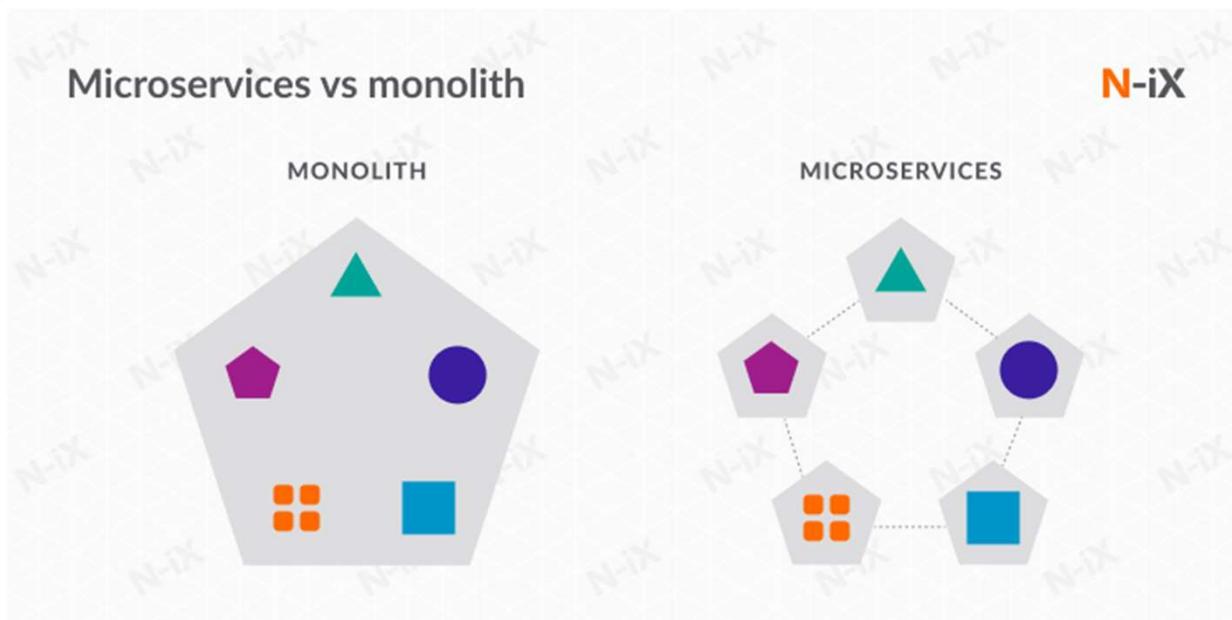
**Microservices** are an emerging feature of web-based solutions

- A **microservice** is a single element of a web application
- Many other web applications can call upon it
- Created to provide **purpose-specific** business capabilities through independently deployed services.
- Microservices are **small and focused** on a singular operation
- Deployments based on **immutable architecture** or **infrastructure as code**
- Allow large complex solutions to be broken into smaller self-contained functions



CompTIA Security+ 70 Course Notes

# Microservices



<https://www.n-ix.com/microservices-vs-monolith-which-architecture-best-choice-your-business/>

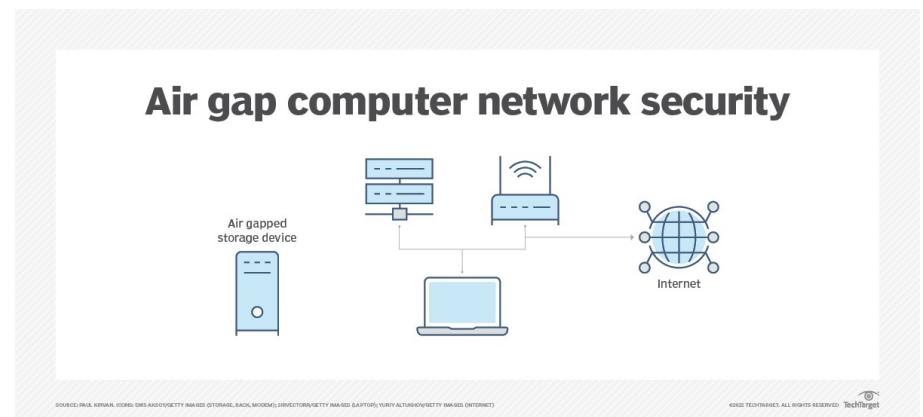


## CompTIA Security+ 70 Course Notes

# Air-Gapped

Physical Isolation/Air-Gapped: Physically isolated or air-gapped networks provide high security by being **disconnected** from the internet, but they can be difficult to update and maintain.

Nothing can access the system on the network.





## CompTIA Security+ 70 Course Notes

# Software-Defined Networking

Approach to network management that seeks to make networks more flexible, scalable, and programmable.

Separation of Control and Data Planes: SDN decouples the network control logic (the **control plane**) from the underlying routers and switches that forward traffic (the **data plane**). This separation allows for centralized network management and control.

### Key Components

- SDN Controller: The brain of the SDN network. It's a software application that manages the flow control to the network devices.
- Southbound Interface: Protocols like OpenFlow that relay instructions from the SDN controller to the switches and routers.
- Northbound Interface: Facilitate communication between the SDN controller and the applications and business logic "above." They allow for the development of applications that can dynamically control network behaviors.

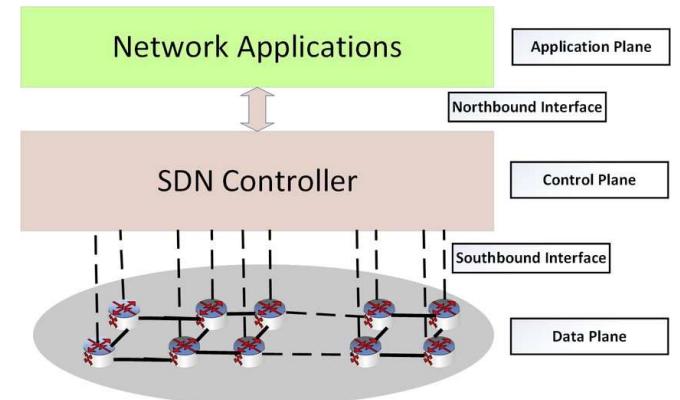
### Advantages

- Flexibility and Agility: Easier to configure and reprogram the network on the fly to meet changing needs.
- Centralized Management: Network administrators can manage the entire network as a single entity from a central location.
- Improved Network Efficiency and Performance: Automated and dynamic traffic routing can lead to more efficient network utilization.
- Cost-Effectiveness: Reduces the need for expensive, proprietary hardware and facilitates the use of commodity hardware.



CompTIA Security+ 70 Course Notes

## Software-Defined Networking



[https://www.researchgate.net/figure/Software-defined-networking-SDN-architecture\\_fig1\\_333873385](https://www.researchgate.net/figure/Software-defined-networking-SDN-architecture_fig1_333873385)



CompTIA Security+ 70 Course Notes

## On-Premises

On-premises infrastructure is fully controlled and managed **internally**, offering **complete control** over security but also requiring **significant resources** for security management.





## CompTIA Security+ 70 Course Notes

# Centralized vs. Decentralized

Centralized systems can enforce **consistent** security policies but create **single points of failure**.

Decentralized systems can **enhance resilience** and reduce single points of failure but can **complicate security monitoring** and consistency.





## CompTIA Security+ 70 Course Notes

# Virtualization

Virtualization is the creation of a virtual version of something

- For example, an operating system, software, a server, a storage device, or network resources

Used to host one or more operating systems within the memory of a single host computer

Allows virtually any OS to operate on any hardware

For examples, VMWare, Hyper-V, VirtualBox

Easier and faster to make backups of the entire virtual system

Malicious code compromise or infection of virtual system rarely affects the host OS

**Offers the following:**

- Individual instances of servers or services
- Real-time scalability
- Quick recovery from damaged, crashed, or corrupted virtual systems
- Help desk support



## Virtualization

Hypervisors: A type of software, firmware, or hardware that creates and runs virtual machines (VMs). It allows multiple operating systems to share a single hardware host. Each operating system appears to have the host's processor, memory, and other resources all to itself, but the hypervisor is actually controlling the host processor and resources

- **Type 1 Hypervisors:** Also known as bare-metal hypervisors, these run directly on the host's hardware to control the hardware and to manage guest operating systems. For example, VMware ESXi or Microsoft Hyper-V for Windows Server.
- **Type 2 Hypervisors:** These run on a conventional operating system just like other computer programs. They are often used for testing and development environments where performance is not a critical issue. Examples, include VMware Workstation, virtualbox and Parallels Desktop for Mac.

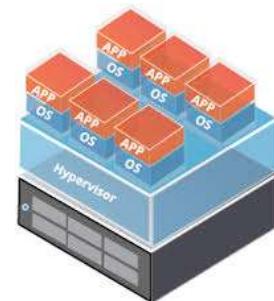


CompTIA Security+ 70 Course Notes

## Virtualization



Traditional  
Architecture



Virtual  
Architecture



## CompTIA Security+ 70 Course Notes

# Containerization

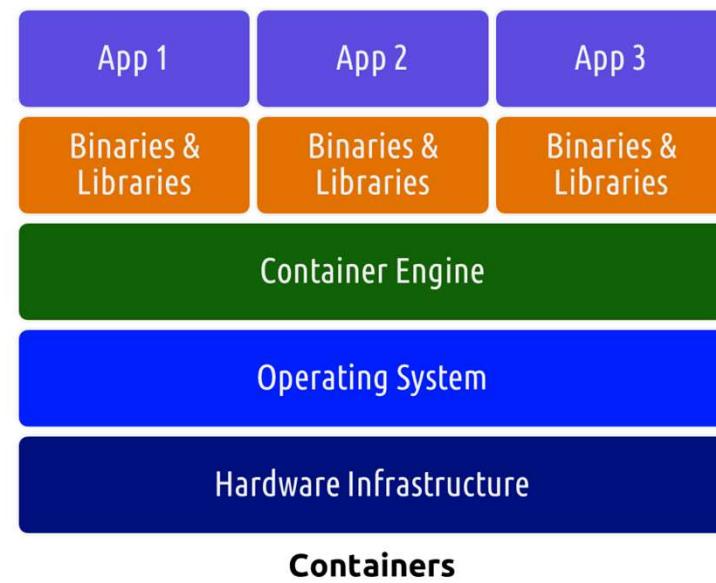
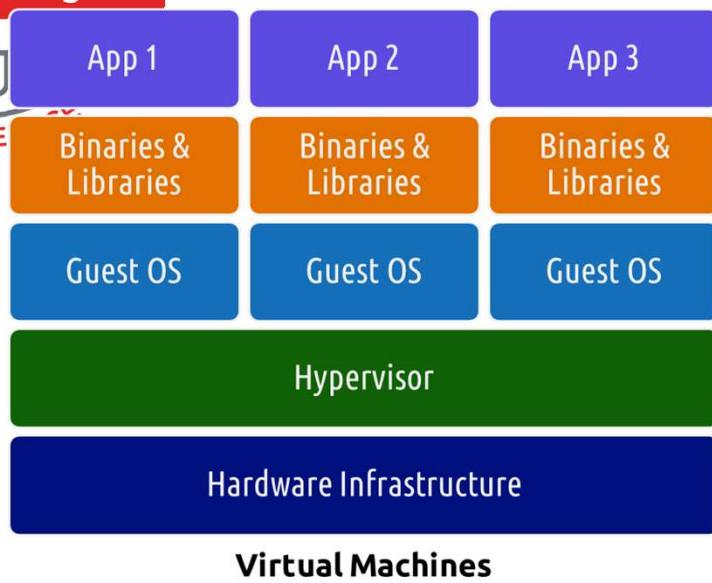
**Containerization** is the evolution of virtualization for internally hosted systems and cloud providers and services.

- **Eliminates duplicating OS elements** like with virtualization. Use a single kernel for multiple operating systems.
- Containers only include the **required resources** to support the functionality of the application in the container.
- Some deployments eliminate the hypervisor altogether and replace it with a collection of common binaries.
- Containerization provides 10 to 100 times more application density per physical server than virtualization solutions.
- Container engines can run multiple, isolated instances, known as containers, on the same operating system kernel.



CompTIA Security+ 70 Course Notes

# Containerization





CompTIA Security+ 70 Course Notes

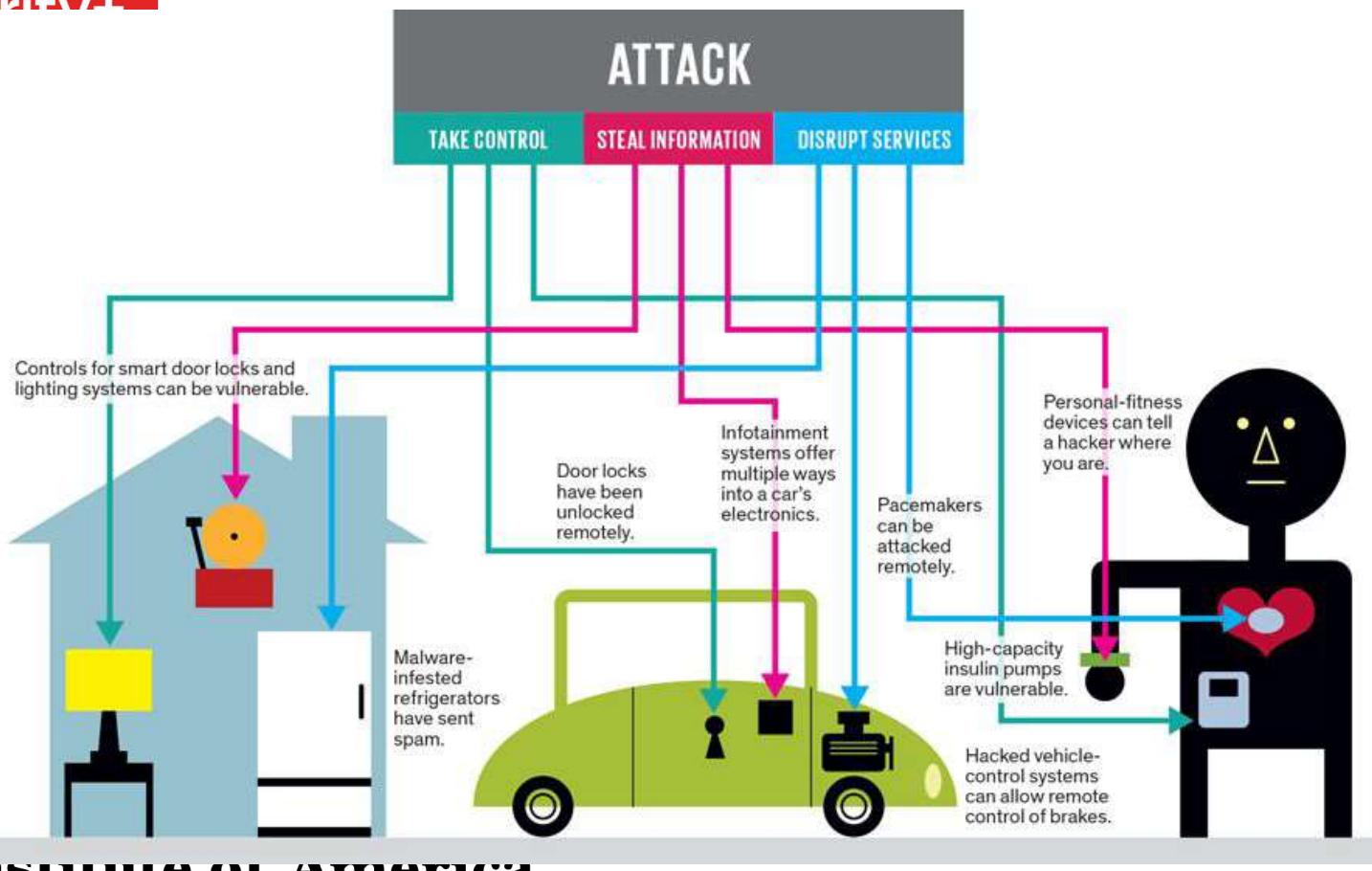
## Internet of Things

The Internet of Things (IoT) is the network of physical objects that traditionally do NOT require access to the internet. They provide home and office automation, remote control, monitoring, and other conveniences.

Embedded systems with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data

Includes house appliances, HVAC systems, A/V systems, cars, and can include almost any other device that requires electrical power.

# Internet of Things





CompTIA Security+ 70 Course Notes

# Industrial Control Systems

**Industrial Control System (ICS)** is a general term that encompasses several types of systems used in industrial production

- **Supervisory control and data acquisition (SCADA)** systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures
- ICSs are typically used in industries such as electrical, water, oil, gas, and data
- Field devices control local operations such as
  - Opening and closing valves and breakers
  - Collecting data from sensor systems
  - Monitoring the local environment for alarm conditions





CompTIA Security+ 70 Course Notes

## Real-Time Operating System

A specialized operating system designed for managing the hardware resources of a computer or embedded system in a way that ensures that specific tasks are executed within strict time constraints.

**Determinism:** Repeating an input will result in the same output.

**High performance:** RTOS systems are fast and responsive, often executing actions within a small fraction of the time needed by a general OS.

**Safety and security:** frequently used in critical systems when failures can have catastrophic consequences, such as robotics or flight controllers.

**Small footprint:** Versus their hefty general OS counterparts, RTOSes weigh in at just a fraction of the size.



## CompTIA Security+ 70 Course Notes

# Embedded Systems

Embedded systems are specialized computing systems that perform dedicated functions or are designed for specific functionalities within a larger system.

**Dedicated Functionality:** Unlike general-purpose computers, embedded systems are designed for specific tasks. For example, the control system in a washing machine or the flight control system in an aircraft.

**Integration with Hardware:** Embedded systems are often closely integrated with their physical environment and hardware. They typically control physical operations of the machine that they are embedded in.





## CompTIA Security+ 70 Course Notes

# High Availability (HA)

Design approach in systems engineering aimed at ensuring an agreed level of operational performance, typically uptime, for a higher than normal period.

- **Minimized Downtime:** The primary goal of high availability is to minimize downtime, both planned and unplanned. This ensures that the system or service is consistently available to users.
- **Redundancy:** Redundancy is a core component of HA. It involves having backup components (like servers, network connections, data storage, etc.) that can take over in case the primary components fail.
- **Failover Mechanisms:** HA systems often have automated failover processes that allow the system to switch seamlessly to backup systems without service interruption in case of a failure.
- **Reliability and Stability:** High availability systems need to be both reliable (operate without failure for a long time) and stable (maintain performance levels under varying conditions).



CompTIA Security+ 70 Course Notes

# Security Architecture Models (Considerations)

When designing and evaluating security architecture models, various considerations come into play.

We will be covering:

- Availability
- Resilience
- Cost
- Responsiveness
- Scalability
- Ease of deployment
- Risk transference
- Ease of recovery
- Patch availability
- Inability to patch
- Power
- Compute



## CompTIA Security+ 70 Course Notes

# Availability

High availability is crucial for ensuring that systems and services are **always accessible** to users.

This involves **redundancy** in critical components, reliable backup solutions, and robust network infrastructure.

**Downtime** not only affects productivity but can also lead to significant financial losses and damage to reputation.





## CompTIA Security+ 70 Course Notes

# Resilience

Resilient systems are designed to handle and **quickly recover** from failures, attacks, or errors.

This involves not only **technical measures** like redundant systems and fault-tolerant designs but also **organizational strategies** like incident response plans and regular testing of recovery procedures.





## CompTIA Security+ 70 Course Notes

### Cost

**Balancing** security needs with budget limitations is a key challenge.

This includes **upfront costs** for hardware, software, and implementation, as well as **ongoing expenses** like maintenance, monitoring, and training.

Overlooking long-term costs, such as those associated with updates and incident response, can be detrimental.





## CompTIA Security+ 70 Course Notes

### Responsiveness

The ability to detect and respond to security threats rapidly is crucial.

This involves having **efficient** monitoring systems, **automated** alerting mechanisms, and **quick** incident response capabilities.

A responsive architecture can significantly **reduce the impact** of security breaches.





## CompTIA Security+ 70 Course Notes

# Scalability

Scalability ensures that the security architecture can **adapt** to the growing needs of the organization.

This means being able to handle increased data volumes, more users, and higher transaction rates without a drop in performance or security levels.





CompTIA Security+ 70 Course Notes

## Ease of Deployment

The **simplicity** and **straightforwardness** of deploying security solutions are critical.

Complex deployment processes can lead to errors, security gaps, and increased time to deployment.

Solutions that are easy to deploy help in maintaining **continuity** and **reducing downtime**.





## CompTIA Security+ 70 Course Notes

# Risk Transference

Transferring certain risks to third parties, such as insurers or managed security service providers, can be a **strategic decision**.

It's important to understand the **terms** of such transfers, including what risks are covered, to what extent, and the reliability of the third party in managing these risks.





CompTIA Security+ 70 Course Notes

## Ease of Recovery

The ability to recover from security incidents quickly **minimizes operational disruption** and data loss.

This includes having effective backup systems, clear recovery protocols, and regular testing of disaster recovery plans.



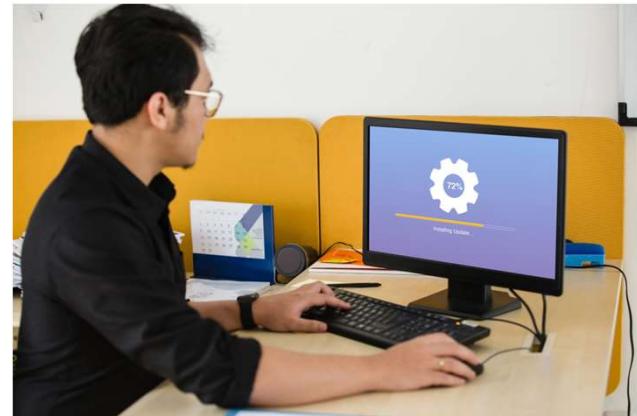


## CompTIA Security+ 70 Course Notes

# Patch Availability

Regularly updating systems with available patches is critical for protecting against **known vulnerabilities**.

This involves having a process for timely patch management and ensuring compatibility of patches with existing systems.





## Inability to Patch

In scenarios where patching is not feasible, **alternative** security measures are necessary.

This could include additional monitoring, compensating controls, or isolating the system.

It's important to assess the risk and implement appropriate security controls to mitigate it.



## CompTIA Security+ 70 Course Notes

### Power

The power requirements of security systems should be considered, especially in environments where **energy resources** are limited or expensive.

Efficient use of power contributes to the **sustainability** and **cost-effectiveness** of the security architecture.





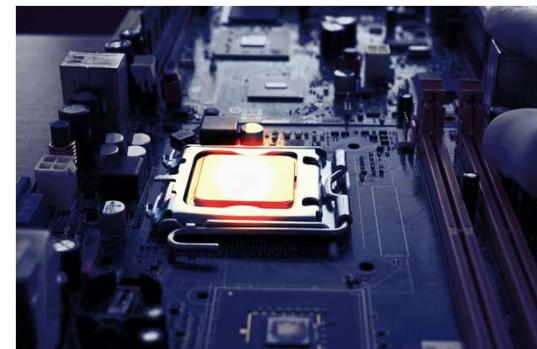
## CompTIA Security+ 70 Course Notes

### Compute

Adequate computational resources are essential for processing security-related tasks.

This includes running advanced security software, analyzing large volumes of data, and supporting encryption and other security mechanisms.

Insufficient compute resources can lead to **bottlenecks** and decreased security effectiveness.



# Data Protection

---



## CompTIA Security+ 70 Course Notes

# Regulated Data

## Regulated Data

This includes data that is subject to regulatory requirements, such as **personal data** protected under laws like GDPR, **health information** covered by HIPAA, or **financial data** under PCI-DSS.

**Compliance** with legal and regulatory standards is crucial. This involves implementing stringent security measures, **access controls**, and ensuring data **privacy** and integrity.





CompTIA Security+ 70 Course Notes

# Data Types: Intellectual Property (IP)

## Intellectual Property (IP)

Intellectual property refers to **creations of the mind** like inventions, literary works, artistic works, designs, symbols, and names used in commerce.

IP theft can result in significant economic loss and competitive disadvantage.

Protection involves rights management, strict access controls, and potentially watermarking or other methods to trace and identify **unauthorized copies**.



## CompTIA Security+ 70 Course Notes

# Intellectual Property : Copyrights

**Copyright** law grants protections against **unauthorized duplications** of an original creative work.

- Protects creative **expression of ideas** or resources rather than the ideas or resources
- Authors can control how their work is distributed, reproduced, and used
- **Protection**
  - **70 years** after the death of the last remaining author of the work, unless it's "work for hire".
  - **Works for hire** and anonymous works are protected **95 years** from the date of first publication or 120 years from the date of creation, whichever is shorter
- **Penalties**
  - Up to \$1,000,000 in damages and ten years in prison for repeat offenders
- **Categories of works protected by copyright**
  - ▶ Literary works
  - ▶ Musical works
  - ▶ Dramatic works
  - ▶ Pantomimes and choreographic works
  - ▶ Pictorial, graphical, and sculptural works
  - ▶ Motion pictures and other audiovisual works
  - ▶ Sound recordings
  - ▶ Architectural works



## CompTIA Security+ 70 Course Notes

### Intellectual Property : Trademarks

A **trademark** protects words, names, symbols, sounds, shapes, colors, musical tones, or combinations used to identify products to distinguish from others

- Protect from someone stealing another company's "**look and feel**"
- The primary purpose is to **avoid confusion** in the marketplace
- Protects the intellectual property rights of people and organizations
- Granted for an initial period of **10 years** and can be renewed an **unlimited** number of times for another 10 years



## CompTIA Security+ 70 Course Notes

### Intellectual Property : Patents

Patents protect the rights of inventors and their inventions

- Protection for those who have legal ownership of the patent
  - Patent Requirements
  - Invention must be new
  - Invention must be useful
  - Invention must NOT be obvious
- Owner has exclusive control of the invention for 20 years
  - After which the invention enters the public domain





## CompTIA Security+ 70 Course Notes

### Intellectual Property : Trade Secrets

Trade Secrets are any form of information, device, method, process, or formula that, if disclosed, will cause significant damage to an organization.

- Resource must provide competitive value
- Must be protected from unauthorized use or disclosure
- Proprietary to the organization and essential for survival
- Economic Espionage Act of 1996: Anyone found guilty of stealing trade secrets
  - From US corporation ↗ Fined up to \$500,000 and 15 years
  - Under other circumstances ↗ Fined up to \$250,000 and 10 years
- Nondisclosure agreements (NDA) should be used to prohibit the sharing of trade secrets.





CompTIA Security+ 70 Course Notes

## Data Types: Legal Information

This encompasses information pertaining to legal matters, including case files, legal advice, and other sensitive legal documents.

Breaches can compromise attorney-client privilege and case integrity, so ensuring confidentiality through **encryption** and **secure communication channels** is critical.





CompTIA Security+ 70 Course Notes

## Data Types: Financial Information

This data includes details about transactions, financial records, credit information, and other monetary data.

Financial data is a **prime target** for cybercrimes like fraud and identity theft. Security measures include encryption, secure transaction processing, and adherence to financial industry standards.





## CompTIA Security+ 70 Course Notes

# Readable Data

Human-Readable Data: **Easily interpretable** by humans, such as text documents, images, and printed information.

Non-Human Readable Data: Requires specific tools or software to **interpret**, like encrypted data, machine code, or log files.

**Both types require protection;** human-readable data is susceptible to **direct reading**, while non-human readable data can be a target for **cyber-attacks** aimed at decryption or misuse.





## Data Classifications

Data classifications help in determining the **level of security controls** and handling protocols that should be applied to various types of data.

- Creation, Usage, Destruction
- **Owners must be assigned to information**
  - Defines **criticality** and what impact if it is destroyed
  - Defines **sensitivity** of the data (Classifications)
  - Will **estimate value** and replacement cost (if it is possible)
  - Defines the **Need to Know (NTK)**
  - Ensure proper **declassification or destruction** at the end of life
- Classification helps in assigning proper controls
- Owner will define retention requirements
- Optimize the use of resources



CompTIA Security+ 70 Course Notes

## Data Classifications

Goals of Data Classification

Confidentiality

Integrity

Availability

Sensitivity

Criticality

Required for different types of information

Private Industry will emphasize CIA

Military will emphasize confidentiality

**Keep your classification simple for greater success**



CompTIA Security+ 70 Course Notes

## Data Classifications

**Protection for each level of classification**

- **Unclassified:** No protection needed
- **Confidential:** Filing cabinet with a metal bar and lock
- **Secret:** An approved safe
- **Top Secret:** A vault

Examples above are used by the military and government



## Government / Military

**Top Secret**  
Example: Wartime weapons, spy satellite information

**Secret**  
Example: Deployment plans for troops

**Confidential**  
Example: Trade secret, health care information

**Unclassified**  
Example: Computer manual, recruiting information

**Class 3**  
Exceptionally Grave Damage

**Class 2**  
Serious Damage

**Class 1**  
Damage

**Class 0**  
No Damage

## Data Classifications

### Non-Government

**Confidential/ Proprietary**  
Example: Trade Secret, Health care information, technical specification of a product

**Private**  
Example: Work history, Human resource information

**Sensitive**  
Example: Profit earnings and forecasts, financial information

**Public**  
Example: How many people are working on a specific project, upcoming projects



CompTIA Security+ 70 Course Notes

## Data Classifications

Some organizations and different governments may use classifications terms such as:

- Sensitive
- Confidential
- Public
- Restricted
- Private
- Critical



CompTIA Security+ 70 Course Notes

## Data States

### Data States:

This refers to the different forms or states in which data can exist, each with its own **security implications and protection strategies**.





## CompTIA Security+ 70 Course Notes

# Data States: Data at Rest

### Data at Rest:

This is data that is **stored** on any device or medium, like hard drives, SSDs, USB drives, or cloud storage. It is **not actively moving** from device to device or network to network.

The primary security concern for data at rest is **unauthorized access or theft**. **Encryption** is a common method to protect data at rest.





CompTIA Security+ 70 Course Notes

## Data States: Data in Transit

### Data in Transit:

This refers to data that is **actively moving** across a network, such as the internet, or between devices and locations.

It could be an email being sent, a webpage being loaded, or files being transferred.

Security for data in transit typically involves **encryption protocols** like SSL/TLS to protect the data as it travels.





## CompTIA Security+ 70 Course Notes

# Data States: Data in Use

### Data in Use:

This is data that is being **processed** or used by applications, users, or systems. It could be data being accessed during a transaction, data in a computer's RAM, or data being processed by an application.

Protecting data in use is challenging because it needs to be **accessible** and often **decrypted** for processing.

Techniques like using **secure environments** for processing and **access control** measures are employed for its protection.





## Geolocation

This relates to the physical or geographical **location** of data.

In terms of cybersecurity, geolocation can have multiple implications:

- Legal and Regulatory Compliance
- Data Latency and Performance
- Risk Management
- Data Sovereignty and Privacy





## CompTIA Security+ 70 Course Notes

# Data Sovereignty

The legal concept that data is subject to the **laws and governance structures** of the country in which it is collected, stored processed.

**Data sovereignty** is a key consideration in **international** data storage and transfer.

Organizations must ensure that their data handling and storage practices comply with the **laws** of the country where the collected, stored, processed.

This is particularly important for **multinational** companies or those using **cloud services**, where data might reside in **multiple jurisdictions**.



CompTIA Security+ 70 Course Notes

## Methods to Secure Data

Many options exist for securing data. Any of the following may be included in your exam:

- Geographic restrictions
- Encryption
- Hashing
- Masking
- Tokenization
- Obfuscation
- Segmentation
- Permission restrictions





## CompTIA Security+ 70 Course Notes

# Geographic Restrictions

This involves restricting the **physical location** where data can be stored and accessed.

It is often used to comply with **data sovereignty laws** and to reduce the risk of data breaches.

By ensuring data is only stored and processed in certain locations, organizations can more easily comply with **regional regulations** and **mitigate risks** associated with certain jurisdictions.





## CompTIA Security+ 70 Course Notes

# Encryption

Encryption is the process of converting data into a **coded format** that is unreadable without a specific **key or password**.

It's a fundamental method for protecting data confidentiality, particularly **data at rest** (like on a hard drive) and **data in transit** (like over the internet).

Encrypted data requires a **decryption key** to be readable, thereby safeguarding it from unauthorized access.





CompTIA Security+ 70 Course Notes

## Hashing

Hashing is the **transformation** of a string of characters into a usually shorter fixed-length value or key that **represents** the original string.

It is commonly used in securing passwords, as the **hash value** is stored rather than the actual password.

Unlike encryption, hashing is a **one-way** process and **cannot be reversed**, which makes it suitable for verifying data integrity **without revealing** the original data.

```
placeholder"));var k=f.find("option"),l=ent"),v:s.value}}).get();l.sort(function value=l[r].v,a(s).text(l[r].t),a(s).data control").attr("placeholder",j);g.find(".dr s-select-close-button fc'><span class='bs -save'&gt;Zapisz&lt;/span&gt;&lt;/div&gt;");g.find(".fi \\"&gt;check&lt;/i&gt;");g.find(".bs-searchbox").ap -icons mi-search"&gt;search&lt;/i&gt;i class='m control").keyup(function(){console.log("sear ched"),g.find(".dropdown-menu.inner li"). ("ls-sl")):(console.log("long list"),g.ref click(function(){return g.find("refresh")</pre>
```



# **Technical Institute of America**



## CompTIA Security+ 70 Course Notes

# Masking

Data masking is the process of **obscuring** specific data within a database to protect it.

For example, in a customer database, the customer's phone number may be partially masked (e.g., 123-xxx-7890).

This technique is often used to protect sensitive data while still allowing users to work with **realistic data formats** in environments like development or testing.





CompTIA Security+ 70 Course Notes

## Tokenization

Tokenization replaces sensitive data with non-sensitive **substitutes**, known as tokens.

These tokens can be used in the system without bringing sensitive data into the environment.

For instance, in credit card processing, the actual card number is **replaced** with a unique token, and the real data is stored securely offsite.

This method is particularly useful for payment processing and protecting PII (Personally Identifiable Information).





## CompTIA Security+ 70 Course Notes

# Obfuscation

Obfuscation involves making data **ambiguous** or **unclear** to obscure its meaning and thereby protect it.

This can be done through various means like **mixing data** with other non-sensitive data, **changing file names** or types to make them less recognizable, or altering code structures.

It is often used in software development to protect **source code** from being easily understood and exploited.

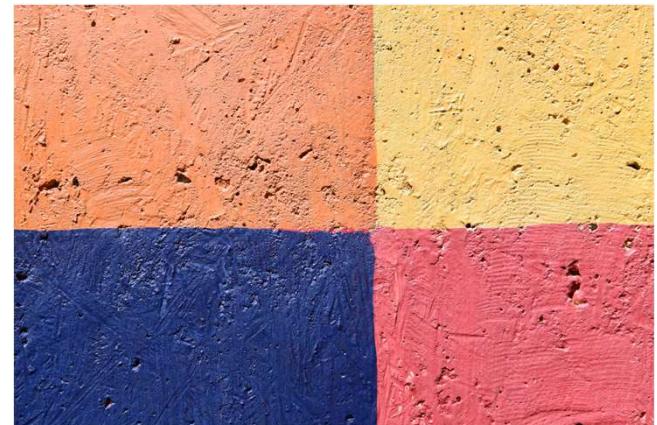




## Segmentation

This refers to **dividing** a network into smaller parts or segments to control access and reduce the risk of widespread network breaches.

By segmenting networks, an organization can **limit access** to sensitive data to only those who need it, and **contain** any breaches to a specific segment, thereby reducing the overall impact.





## Permission Restrictions

This involves setting up and enforcing **policies** that control **who** has access to data and **what** they are allowed to **do** with it

Permissions can be assigned based on **roles**, **responsibilities**, or other criteria.

Properly managing permissions is a key aspect of data security, ensuring that only **authorized** individuals can access, modify, or delete data.



# Common Security Techniques

---



CompTIA Security+ 70 Course Notes

## Secure Baselines

Securing baselines refers to a set of security **standards** and **configurations** that an organization establishes to protect its systems and data.

These baselines are typically developed based on industry **best practices**, regulatory requirements, and the organization's specific security needs.

The concept of a secure baseline encompasses several steps:

1. Establish
2. Deploy
3. Maintain



## CompTIA Security+ 70 Course Notes

# Secure Baselines: Establish

### Assessment and Analysis:

- This initial step involves **assessing** the current security posture and **understanding** the specific needs of the organization. It includes analyzing the threats, vulnerabilities, and risks associated with the organization's systems and data.

### Defining Standards and Configurations:

- Based on the assessment, standard security **configurations** and **controls** are defined. These standards should align with industry best practices (like those from NIST, ISO, etc.) and specific regulatory requirements applicable to the organization.

### Documentation:

- The established baseline configurations and standards are documented. This documentation serves as a reference for **implementing** and **maintaining** these baselines.



## CompTIA Security+ 70 Course Notes

# Secure Baselines: Deploy

### Implementation:

- The secure baseline configurations are **implemented** across the organization's IT infrastructure. This includes servers, workstations, network devices, applications, and other systems.

### Automation and Tools:

- Where possible, automation tools are used to deploy the baseline configurations consistently and efficiently. This can include configuration management tools, scripts, or specialized software.

### Verification and Compliance Checking:

- After deployment, the configurations are verified to ensure they are correctly implemented. Compliance checks are also conducted to ensure that the configurations meet the defined standards.



## CompTIA Security+ 70 Course Notes

# Secure Baselines: Maintain

### Monitoring and Auditing:

- Continuous monitoring is established to ensure that the systems remain in compliance with the baseline configurations. Regular audits are also conducted to assess the effectiveness of the baselines.

### Updating and Patching:

- The baseline configurations are regularly updated to address new threats, vulnerabilities, and technological changes. This includes applying security patches and updating security controls as needed.

### Training and Awareness:

- Ongoing training and awareness programs for staff are essential to maintain the effectiveness of the secure baselines. This helps ensure that all personnel understand their role in maintaining security and are aware of the latest security practices and threats.



CompTIA Security+ 70 Course Notes

## Hardening Targets

Hardening targets in cybersecurity refers to the process of **strengthening** various **hardware components** to make them more secure and resilient to attacks.

This involves implementing **security measures** and **configurations** that reduce vulnerabilities and protect against threats.





CompTIA Security+ 70 Course Notes

## Hardening Targets: Mobile Devices

Hardening mobile devices involves implementing strong **authentication**, **encrypting** data, installing **security software**, controlling app **permissions**, and regularly **updating** the operating system and apps.

It also includes using secure Wi-Fi and VPN services for network connections.





CompTIA Security+ 70 Course Notes

## Hardening Targets: Workstations

Workstations are hardened by installing antivirus and anti-malware **software**, enabling **firewalls**, regularly applying **patches and updates**, and implementing user **access controls**.

**Physical security** measures and data **encryption** are also important.





## Hardening Targets: Switches

Hardening switches involves disabling **unnecessary services**, securing **management interfaces**, implementing **VLANs** for network segmentation, and using **ACLs** (Access Control Lists) to control network traffic.

Regular **firmware updates** and **monitoring** for unusual network activity are also critical.





CompTIA Security+ 70 Course Notes

## Hardening Targets: Routers

Router hardening includes **changing default passwords**, disabling **unused services** and interfaces, **updating firmware**, using strong **encryption** for Wi-Fi, and setting up **firewalls** and intrusion prevention systems.

**VPN** configurations for secure **remote access** are also common.





CompTIA Security+ 70 Course Notes

## Hardening Targets: Cloud Infrastructure

Securing cloud infrastructure involves:

- Using strong **identity and access management**,
- **Encrypting** data at rest and in transit,
- **Securing APIs**,
- Implementing network **security control**
- Following **best practices** provided by the cloud service provider





CompTIA Security+ 70 Course Notes

## Hardening Targets: Servers

Server hardening includes:

- Installing necessary **security updates**
- Minimizing the number of **running services**
- Implementing strong **authentication mechanisms**
- Using **firewalls** and intrusion detection systems
- **Physically securing** server environments.





CompTIA Security+ 70 Course Notes

## Hardening Targets: ICS/SCADA

(Industrial Control Systems)/(Supervisory Control and Data Acquisition)

Hardening ICS/SCADA systems involves:

- **Segmenting** networks
- **Restricting** physical and network access
- **Disabling unnecessary services**
- **Applying patches** carefully
- **Continuously monitoring** for abnormal activities.

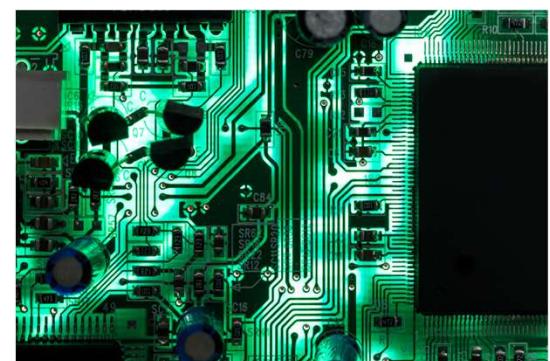


CompTIA Security+ 70 Course Notes

## Hardening Targets: Embedded Systems

Hardening embedded systems includes:

- Using secure **boot processes**
- Implementing **least privilege** access controls
- **Securing** communication channels
- Conducting regular **security audits** to **identify vulnerabilities**.





CompTIA Security+ 70 Course Notes

## Hardening Targets: RTOS

For RTOS (Real-Time Operating Systems), hardening includes:

- Minimizing the **attack surface** by reducing the number of services
- Implementing strict **access controls**
- Securing **communication protocols**
- Regularly **updating** the software to fix **vulnerabilities**.





CompTIA Security+ 70 Course Notes

## Hardening Targets: IoT Devices

Internet of Things (IoT) devices are hardened by:

- Changing **default credentials**
- Securing **network connections**
- Regularly **updating firmware**
- Disabling **unnecessary services**
- Implementing security at the **application layer**.





CompTIA Security+ 70 Course Notes

## Installation of Mobile Devices

The installation of wireless devices requires a heightened focus on both **performance** and **security**.

Conducting site surveys and creating heat maps remain crucial, but with additional emphasis on **mitigating security risks**.





## CompTIA Security+ 70 Course Notes

# Site Surveys

### Identifying Risks and Vulnerabilities:

Involves **identifying** potential security **vulnerabilities** like areas where the wireless signal might bleed outside the intended coverage area.

### Security of Physical Locations:

APs should be placed in **secure**, tamper-resistant locations to prevent physical manipulation.

### Environmental Factors:

This includes understanding how **building materials** might interfere with signal strength and potentially create **blind spots** where intruders could exploit network weaknesses.



## CompTIA Security+ 70 Course Notes

# Heat Maps

### Optimal Placement for Coverage and Security:

Heat maps are **graphical representations** of wireless signal coverage within a space.

They are used for:

- Ensuring uniform coverage
- Identifying areas where the wireless signal might be too strong, **leaking outside secure areas**.

### Adjusting Signal Strength:

Based on the heat map, **signal strength** can be adjusted to minimize the chances of interception or unauthorized access from outside the **intended coverage area**.

### Monitoring and Adjusting Post-Deployment:

Heat maps should be periodically **revisited** after deployment to monitor any **changes in the environment** that might affect wireless security. **New obstacles**, additional network **devices**, or changes in **office layout** can impact both coverage and security.



CompTIA Security+ 70 Course Notes

## Mobile Solutions

Mobile solutions refer to **strategies** and **technologies** used to manage and secure mobile devices used within an organization.

This encompasses:

- Managing the devices themselves
- How they are deployed in the organization
- How they connect to networks and other devices



CompTIA Security+ 70 Course Notes

# Mobile Device Management (MDM)

MDM Solutions: MDM solutions are **software applications** that allow IT administrators to control, secure, and enforce policies on **mobile devices**. This includes remotely managing apps, enforcing security policies, wiping data on lost devices, and configuring settings for email, Wi-Fi, and VPN access.

Security and Compliance: MDM is critical for ensuring that mobile devices **comply with** organizational security policies and **standards**. This can involve enforcing encryption, password protection, and application whitelisting/blacklisting.

Device Monitoring and Management: MDM tools **monitor** the health and security of mobile devices, **providing insights** into compliance status, potential security risks, and usage patterns.



CompTIA Security+ 70 Course Notes

## Deployment Models: BYOD

### Bring Your Own Device (BYOD):

In the BYOD model, employees use their **personal mobile devices** for work purposes.

While BYOD can increase **employee satisfaction** and reduce costs, it also raises **significant security challenges**.

Organizations need to implement strict security policies and controls to protect corporate data on personal devices.





## Deployment Models: COPE

Corporate-Owned, Personally Enabled (COPE):

In this model, the organization **provides mobile devices** to employees but allows for some **personal use**.

COPE makes it easier to enforce security controls since the organization has full ownership and control over the devices.

However, **balancing** corporate security with personal use rights is a key challenge.



CompTIA Security+ 70 Course Notes

## Deployment Models: CYOD

### Choose Your Own Device (CYOD):

CYOD allows employees to choose from a selection of devices **provided by the organization**.

This model offers a **balance** between personal preference and corporate control, allowing companies to **enforce security** controls on devices while giving employees **some choice**.





CompTIA Security+ 70 Course Notes

## Connection Methods: Cellular/Wi-Fi/Bluetooth

Each connection method has a unique set of security considerations.

Ensuring the security of these connections involves:

- Using advanced **security protocols**

- Being aware of potential **vulnerabilities**

- Continuously **updating and monitoring** the network infrastructure.





## CompTIA Security+ 70 Course Notes

### Cellular

Encryption and Security Protocols: Modern cellular networks incorporate strong encryption standards to protect data transmission. This makes **eavesdropping** or **intercepting** data much more difficult.

VPN Use: For accessing sensitive corporate resources, using a VPN over cellular connections is recommended. VPNs **encrypt** data traffic, ensuring that even if data packets are **intercepted**, they remain **unreadable**.

SIM Card Security: SIMs can be a major vulnerability point. SIM swapping attacks, for instance, involve transferring a victim's phone number to a SIM card controlled by an attacker.



## CompTIA Security+ 70 Course Notes

### Wi-Fi

**Encrypted Wi-Fi Protocols:** Always use Wi-Fi networks that are secured with WPA2 or WPA3 **encryption**. Open or unencrypted Wi-Fi networks significantly increase the risk of data **interception**.

**Avoiding Public Wi-Fi for Sensitive Transactions:** Public Wi-Fi networks are more vulnerable to attacks. Avoid conducting **sensitive transactions** like banking or accessing sensitive corporate data on public Wi-Fi networks.

**Network Segmentation:** Segmenting Wi-Fi networks can enhance security. Having **separate networks** for guests, employees, and critical business functions can limit the potential impact of a breach.

**Regularly Update Wi-Fi Network Hardware:** Keep firmware for routers and access points updated to ensure they have the **latest security patches** and features.



## CompTIA Security+ 70 Course Notes

# Bluetooth

Pairing and Discoverability: Set devices to "Non-Discoverable" when not pairing and ensure that pairing is done securely, ideally in a **private setting** to prevent unauthorized devices from connecting.

Use Updated Bluetooth Standards: Newer Bluetooth standards have improved security features. Ensure devices use the **latest Bluetooth versions** and update firmware regularly.

Limiting Usage: Use Bluetooth functionality **only when necessary**. Keeping Bluetooth on at all times increases the attack surface.

Awareness of Bluetooth Vulnerabilities: Be aware of common Bluetooth vulnerabilities, which can exploit Bluetooth connections to **access device data or inject malware**.



## CompTIA Security+ 70 Course Notes

# Wireless Security Settings

- Wi-Fi Protected Access 3 (WPA3)
- AAA/RADIUS
- Cryptographic Protocols
- Authentication Protocols

WPA3 is a specific protocol designed for securing Wi-Fi networks.

AAA/RADIUS, cryptographic protocols, and authentication protocols have broader applications in network security.

Sonicwall Demo:  
<https://tz570w.demo.sonicwall.com/sonicui/7/login/#/>





## CompTIA Security+ 70 Course Notes

### WPA3

WPA3 is the latest security certification program developed by the Wi-Fi Alliance. It improves upon its predecessor, WPA2, by offering **enhanced cryptographic strength** and more **robust authentication methods**.

- Stronger encryption using the Simultaneous Authentication of Equals (SAE) protocol, which replaces the Pre-Shared Key (PSK) in WPA2.
- Protection against offline dictionary attacks.
- Enhanced protection for open networks through individualized data encryption.
- Support for 192-bit security suite for protecting networks with higher security requirements, like government or finance.



CompTIA Security+ 70 Course Notes

## AAA/RADIUS

AAA (Authentication, Authorization, and Accounting) is a framework for intelligently **controlling access** to computer resources, **enforcing policies**, and **auditing usage**.

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized **Authentication**, **Authorization**, and **Accounting management** for users accessing a network.



CompTIA Security+ 70 Course Notes

## Cryptographic Protocols

Cryptographic protocols are a series of processes that **encrypt** data to secure communications.

They use algorithms to transform **readable** data (plaintext) into **unreadable** data (ciphertext) and vice versa.

Cryptographic protocols are the **underlying technology** that makes security protocols like WPA3 secure. WPA3 is an **application** of cryptographic principles **specifically tailored** for Wi-Fi security.





## CompTIA Security+ 70 Course Notes

# Authentication Protocols

Authentication protocols are used to **verify the identity** of a user or device trying to access a network or service.

They are often part of a broader security framework like AAA/RADIUS and can be incorporated into wireless security settings.

While WPA3 focuses on securing the wireless network itself, authentication protocols are concerned with verifying the identity of users or devices accessing any network or service.





CompTIA Security+ 70 Course Notes

# Application Security

Application security is a critical aspect of cybersecurity, focusing on ensuring that software applications are protected from threats and vulnerabilities.

We will be discussing:

- [Input validation](#)
- [Secure cookies](#)
- [Static code analysis](#)
- [Code signing](#)





## CompTIA Security+ 70 Course Notes

# Input Validation

Input validation involves **verifying** the data provided by a user or another application before processing it. This practice is crucial to **prevent common vulnerabilities** such as SQL injection, cross-site scripting (XSS), and command injection.

Input should be treated as untrusted and validated both on the client-side for usability and on the server-side for security.

Effective input validation can prevent attackers from using malicious data to **exploit the logic** of the application, thereby safeguarding the application from a **wide range of attacks**.



## Secure Cookies

Cookies are small pieces of data stored on the user's device by a web browser while browsing a website. Secure cookies are those that have **security attributes** set to protect user data and session information.

Key attributes include '**Secure**' (indicating that the cookie should only be sent over secure HTTPS connections) and '**HttpOnly**' (preventing access to the cookie via client-side scripts).

These attributes help protect cookies from being **intercepted** by an attacker during data transmission (man-in-the-middle attacks) and from being **accessed** through XSS attacks.



## CompTIA Security+ 70 Course Notes

# Static Code Analyses

Static code analysis is the process of **examining** the source code of an application **without executing it**.

The aim is to **find vulnerabilities**, code flaws, and ensure compliance with coding guidelines.

It involves using tools that can **automatically scan the code** to detect issues like security vulnerabilities, performance problems, or non-compliance with coding standards.

This method can identify potential security issues **early in the development lifecycle**, making it easier and more cost-effective to address them.



## CompTIA Security+ 70 Course Notes

# Code Signing

Code signing is a process that involves using a **digital signature** to sign executables and scripts. This signature **confirms** the software author and guarantees that the code has not been **altered or corrupted** since it was signed.

A certificate issued by a trusted **certificate authority** (CA) is used to sign the code. When users download or execute the code, their software checks the signature to verify its authenticity.

Code signing helps in establishing the software's **integrity and authenticity**, thereby building trust among users. It also protects users from downloading **maliciously modified** software.



CompTIA Security+ 70 Course Notes

## Sandboxing

A powerful security technique used to isolate applications, processes, or programs in a separate environment to prevent them from affecting the underlying system.

It's a form of containment and risk mitigation, particularly useful for untrusted code or applications.





## Sandboxing: Concept and Purpose

Isolation: Sandboxing involves running code, applications, or processes in an **isolated environment** that **simulates** the end-user operating environment. The main idea is to **execute** the software **without affecting** the host system or network.

Security: This **isolation** helps in **containing** the effects of malicious or faulty code. If a sandboxed application becomes compromised, the threat is **confined to the sandbox**, protecting the actual system from harm.

Testing and Analysis: Sandboxes are also used for safely running and analyzing **suspicious code**, which is particularly useful in malware analysis and testing new software.



## CompTIA Security+ 70 Course Notes

# Sandboxing: Types of Sandboxing

Application Sandboxing: Used for **individual applications**. For example, many web browsers use sandboxing to isolate websites or plugins, reducing the risk of a malicious site compromising the entire browser or system.

Virtual Machine (VM) Sandboxing: Involves running a **full virtual machine** as a sandbox. It is more secure because it completely separates the sandboxed environment from the host operating system.

Cloud-based Sandboxing: Utilizes cloud resources to create and manage sandboxes. This approach offers **scalability** and the ability to handle large-scale sandboxing needs.



CompTIA Security+ 70 Course Notes

## Sandboxing: Uses in Cybersecurity

Malware Analysis: To safely run and analyze the behavior of **suspected malware** without risking the host system.

Application Testing: For testing applications in a **controlled environment** to identify potential security issues or bugs.

User Protection: **Protecting end-users** from potentially harmful applications or content. For example, opening email attachments in a sandbox to prevent malware infection.



## CompTIA Security+ 70 Course Notes

# Sandboxing: Limits

Resource Intensive: Running multiple sandboxes or VMs might require significant **system resources**.

Sophisticated Threats: Some sophisticated malware can detect when it's running in a sandbox and **alter its behavior** to avoid detection.

Not Foolproof: While sandboxes are highly effective in containment, they are not a complete security solution and should be part of a **layered defense strategy**.





## CompTIA Security+ 70 Course Notes

# Security Monitoring: Key Components

### Network Monitoring:

- Involves tracking and analyzing **network traffic** to detect anomalies, unauthorized access, or signs of malicious activity.

### System and Application Monitoring:

- Focuses on the performance and security of specific **systems** and **applications**.
- Monitors for indicators of security incidents.

### Log Management and Analysis:

- Collecting and analyzing logs from various sources to detect unusual or suspicious activity.
- Tools like Security Information and Event Management (SIEM) systems are used for aggregating, correlating, and analyzing log data.

### Endpoint Monitoring:

- Involves keeping track of all endpoint devices to ensure they comply with security policies and are not compromised.
- Endpoint Detection and Response (EDR) tools are commonly used for this purpose.



CompTIA Security+ 70 Course Notes

## Security Monitoring: Purpose and Benefits

Threat Detection: Early identification of potential security threats, allowing for timely response and mitigation.

Performance Management: Ensuring that IT infrastructure operates efficiently and identifying areas for **improvement**.

Compliance and Auditing: Helps in maintaining compliance with various regulatory standards by **providing evidence** of security monitoring and incident response.

Insight and Analysis: Provides valuable insights into the security posture of the organization and helps in understanding attack patterns and trends.



CompTIA Security+ 70 Course Notes

# Security Monitoring: Types of Monitoring

## Real-Time Monitoring:

**Immediate analysis** and alerts for ongoing activities, crucial for rapid response to potential threats.

Requires significant **processing power** and **sophisticated tools**.

## Periodic Monitoring:

Regularly scheduled checks and analyses, suitable for **less critical systems** or for **complementing** real-time monitoring.



CompTIA Security+ 70 Course Notes

## Security Monitoring: Challenges

Data Volume and Complexity: Managing and analyzing the **vast amount of data** generated by various monitoring tools can be challenging.

False Positives and Alarm Fatigue: Effective filtering and prioritization are necessary to avoid overwhelming security teams with **false alarms**.

Privacy and Legal Concerns: Monitoring must be **balanced** with privacy rights and compliance with legal standards.



CompTIA Security+ 70 Course Notes

## Security Monitoring: Integration

Incident Response: Monitoring feeds into incident response processes, **providing the information** needed for effective mitigation.

Risk Management: Helps in **identifying and assessing** risks, contributing to overall risk management strategies.



# Lesson 13 Hardware, software and Data Asset Management

---



## CompTIA Security+ 70 Course Notes

# Acquisition/Procurement

The acquisition/procurement process for hardware, software, and data assets carries significant security implications for organizations.

Each stage of this process can introduce vulnerabilities and risks if not properly managed.





CompTIA Security+ 70 Course Notes

## Acquisition/Procurement: Needs Assessment

Importance of Accuracy: Failing to accurately assess the organization's requirements can lead to acquiring assets that are either **over-privileged** or **lack necessary security** features, thereby **introducing vulnerabilities**.





CompTIA Security+ 70 Course Notes

## Acquisition/Procurement: Vendor Evaluation

Vendor Risks: Choosing a vendor with a poor **security track record** or **inadequate support** for security features can expose the organization to risks. Vendors compromised by cyber threats can **inadvertently** introduce malware or vulnerabilities into their products.

Supply Chain Attacks: If the vendor's **supply chain** is compromised, it can affect the integrity of the hardware or software even before it reaches the organization.





CompTIA Security+ 70 Course Notes

## Assignment/Accounting: Ownership

Definition and Importance: Ownership in cybersecurity refers to the designation of **responsibility** for an asset to an individual or a department within an organization.

It ensures that there is a **specific party** responsible for the security, maintenance, and compliance of each asset.

Owners are typically in charge of defining access controls, managing permissions, and ensuring that the asset is used in compliance with organizational policies and standards.



CompTIA Security+ 70 Course Notes

## Assignment/Accounting: Classification

Definition and Purpose: Classification involves **categorizing** assets based on their sensitivity, value, and the impact on the organization if compromised.

The purpose is to apply an **appropriate** level of security controls based on the classification. Sensitive or high-value assets require more stringent protections.

Types of Classifications: Common classification levels include public, internal-only, confidential, and highly confidential.



## CompTIA Security+ 70 Course Notes

# Monitoring and Tracking: Inventory Management

### Key Components:

- Asset Identification: Cataloging all assets, including their type, model, specifications, and version.
- Ownership and Responsibility: Recording who is responsible for each asset.
- Lifecycle Management: Keeping track of the **lifecycle stage** of each asset, from acquisition through disposal.

Security Implications: A well-maintained inventory allows for the identification of **unauthorized or rogue devices** and software, which could pose security risks.

Challenges: Keeping the inventory up-to-date in **dynamic environments** where new assets are frequently added, and old ones are retired or repurposed.



CompTIA Security+ 70 Course Notes

# Monitoring and Tracking: Enumeration

Identifying and quantifying network elements.

## Key Aspects:

- Network Scanning: Using tools to **scan** the network for connected devices and open ports.
- Service Identification: Determining what **services** are running on each identified device.
- Vulnerability Mapping: Relating the gathered information to known **vulnerabilities** and potential threats.

Security Implications: Helps in **preemptively** identifying and addressing security weaknesses.

Essential for maintaining **visibility** into the network and understanding how different assets **interact** and potentially expose the network to risks.

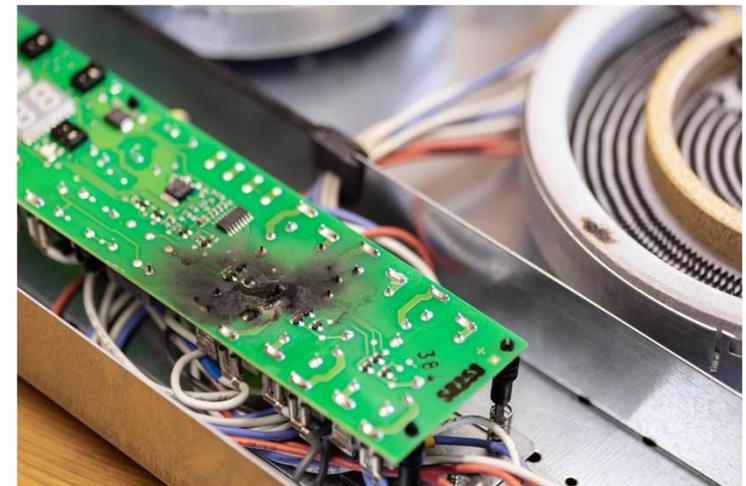
Challenges: Ensuring that enumeration activities do not disrupt **normal business operations**.



CompTIA Security+ 70 Course Notes

## Disposal/Decommissioning

The disposal/decommissioning process in cybersecurity is not just about **removing assets** from the operational environment; it's about ensuring that the **end-of-life handling** of these assets does not introduce new security risks.





## CompTIA Security+ 70 Course Notes

# Disposal/Decommissioning: Sanitization

Sanitization refers to the process of **removing** sensitive data from storage devices to ensure that it **cannot be recovered** by unauthorized individuals.

### Methods:

- Physical Destruction: Physically **destroying** the storage medium (e.g., shredding hard drives).
- Degaussing: Using a powerful **magnet** to disrupt the magnetic field of a storage medium, thus erasing its data.
- Overwriting: **Writing new data** over the existing data, usually several times, to make the original data unrecoverable.

Security Implications: Proper sanitization is crucial to **prevent data breaches** and comply with data protection laws and regulations.

Challenges: Ensuring that the chosen sanitization method is **appropriate** for the type of storage medium and the sensitivity of the data.



## Disposal/Decommissioning: Destruction

Destruction involves the physical **dismantling** or destruction of hardware to ensure that it **cannot be used again**.

It is often used when storage devices cannot be reliably sanitized or when the device itself is a security risk.

Security Implications: Physical destruction is a **definitive** way to ensure that data cannot be recovered and that the device cannot be repurposed for malicious activities.

Challenges: Destruction must be carried out in a way that is **environmentally responsible** and **in compliance** with waste disposal regulations.



CompTIA Security+ 70 Course Notes

## Disposal/Decommissioning: Certification

Certification in the context of asset disposal refers to the **documentation** or certification process that confirms the proper sanitization and destruction of assets.

It serves as **proof** that the organization has responsibly and securely disposed of its IT assets.

Security Implications: Certification helps in **demonstrating compliance** with legal and regulatory requirements related to data privacy and environmental standards.

Challenges: Ensuring that the certification process is thorough and reflects all necessary **compliance and regulatory standards**.



## Disposal/Decommissioning: Data Retention

Data retention involves retaining certain data for a **specified period** as required by **law** or organizational **policies**, even during the disposal process.

It's important to **balance** data retention requirements with the need to eliminate unnecessary data.

Security Implications: Retained data must be protected according to its **classification**, and retention policies must comply with **legal** requirements.

Challenges: Managing the retention of large volumes of data and ensuring that only the **necessary** data is retained, while all other data is securely disposed of.

# Lesson 14 vulnerability management

---



CompTIA Security+ 70 Course Notes

# Vulnerability Identification Methods

## Vulnerability Scan:

**Automated** tools scan systems, networks, and applications to **identify** known vulnerabilities, such as unpatched software, misconfigurations, and security weaknesses.

Usage: Regular scans help in maintaining an **up-to-date** understanding of the security posture and are often the **first step** in vulnerability management.





CompTIA Security+ 70 Course Notes

# Vulnerability Identification Methods

## Vulnerability Scan:

**Automated** tools scan systems, networks, and applications to **identify** known vulnerabilities, such as unpatched software, misconfigurations, and security weaknesses.

Usage: Regular scans help in maintaining an **up-to-date** understanding of the security posture and are often the **first step** in vulnerability management.





## CompTIA Security+ 70 Course Notes

# Application Security

Static Analysis: Involves examining application code to detect security flaws **without executing the program**. AKA Static Application Security Testing (SAST)

- Useful for finding issues like code injection, buffer overflows, and other vulnerabilities that can be identified by reviewing code.

Dynamic Analysis: Testing applications in runtime to identify security issues that only appear **during execution**. AKA Dynamic Application Security Testing (DAST)

- Helps in detecting issues like runtime errors and memory leaks that static analysis might miss.

Package Monitoring: Monitoring the software libraries and packages used in applications for **known vulnerabilities**.

- Involves keeping track of updates and patches for **third-party components** integrated into applications.



## CompTIA Security+ 70 Course Notes

### Threat Feed

Open-Source Intelligence (OSINT): Gathering data from **publicly available sources** to identify emerging threats and vulnerabilities.

- <https://osintframework.com/>

Proprietary/Third-party: Subscribing to **specialized services** that provide information on the latest threats and vulnerabilities. Offers more **tailored** and often **real-time** information.

Information-Sharing Organization: Participating in groups like ISACs (Information Sharing and Analysis Centers) for industry-specific threat intelligence.

Facilitates **collaboration** and sharing of cybersecurity information among members.

Dark Web: Monitoring dark web forums and marketplaces to **gather intelligence** on new vulnerabilities, exploits, and threat actor tactics.



## CompTIA Security+ 70 Course Notes

# Penetration Testing

The practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit

Typically performed using manual or automated technologies

The goals of penetration tests are:

- Determine feasibility of a particular set of attack vectors
- Identify high-risk vulnerabilities from a combination of lower-risk vulnerabilities exploited in a particular sequence
- Identify vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software
- Assess the magnitude of potential business and operational impacts of successful attacks
- Test the ability of network defenders to detect and respond to attacks
- Provide evidence to support increased investments in security personnel and technology



## CompTIA Security+ 70 Course Notes

# Penetration Testing

### Black Box Test - Zero Knowledge

- Also called Closed Test
- Usually from an external location
- From the outsider or hacker's perspective

### Grey Box Test - Partial Knowledge

- Only limited information is provided
- An IP address, a domain name, applications
- Could also mean an internal test
- From an insider's perspective

### White Box Test - Full Knowledge

- Full information is provided
- As much documentation as possible
- Also called Crystal or Open test
- From a system administrator's perspective



## CompTIA Security+ 70 Course Notes

# Penetration Testing

### White Hat

- Ethical Hacker
- Test with permission of the owner
- Use same skills as a Black Hat

### Black Hat

- Unethical Hacker or Cracker
- Test without owner authorization
- Usually has malicious intents

### Grey Hat

- Undecided
- Work as a Black Hat and as a White Hat

### Script Kiddie

- It is a person with little or no skills
- The person uses someone else scripts or programs
- Performs attacks on computer systems and networks
- Usually cannot write their own code or programs
- Like showing off to their friends
- The term is typically meant as an insult



CompTIA Security+ 70 Course Notes

## Penetration Testing

### Rules of Engagement

- Range of IP addresses use by the tester
- Date and time that testing is authorized
- What methodology and tools will be used?
- Is DoS or DDoS allowed?
- Is social engineering allowed?
- Can you attempt a physical intrusion?
- Is there any IP to exclude?
- How often do you have to report?
- How the communications will be protected?





## CompTIA Security+ 70 Course Notes

# Penetration Testing

### Before Proceeding with the Test

Regardless of the type of test:

- A SIGNED document giving the pen tester permission
- Pen tester must have this document on their person while the test is ongoing
- Should include contact information of an authority who will be available during the test
- Signed by a person of authority, not your friend





## Penetration Testing

There are serious risks associated with testing

- Educate your client about what are the risks
- Client must sign that they accepts the risks
- You are in fact launching a portion of the attack to test
- Sometimes results can be unexpected:
- PBX might stop functioning
- VOIP systems really do not like to be scanned
- SCADA system being scanned could results in disaster
- It was fine in the past, today might be different

# Common Methodology

CompTIA Security+ 70 Course Notes



1. Reconnaissance / Discovery  
•Footprinting  
•Scanning  
•Passive versus Active

2. Enumeration  
•Networks, Hosts, Services, Applications, etc...

3. Vulnerability Research / Analysis

4. Execution / Penetration  
- Gaining Access  
- Maintaining Access

5. Clean After Yourself

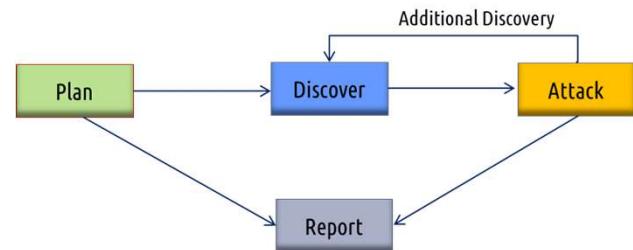
6. Document Findings





CompTIA Security+ 70 Course Notes

## Penetration Testing



NIST 4 Stages Methodology



CompTIA Security+ 70 Course Notes

## Penetration Testing

### What to include in your report

- Finding (low, medium, high)
- Executive Summary
- What to do right now, what to do next, etc...
- A plan of action
- Hosts and Networks discovered
- Rogue hosts or services
- Technical Report
- Progression or Regression since last test done
- Report lack of process or policies



CompTIA Security+ 70 Course Notes

## Penetration Testing

### Manual Versus Automated Reports

- Every tool has its own reporting format
- All results must be validated manually
- It is good practice to use two leading tools
- Automated tools are limited in scope
- Only as good as the last update
- Tools are needed today to create summaries
- There is just too much info to look at
- Manual process alone is not enough



## CompTIA Security+ 70 Course Notes

# Penetration Testing

### Corrective Actions

- Disable or remove unnecessary and vulnerable services
- Modify vulnerable hosts to restrict access to vulnerable services to a limited number of required hosts
  - (i.e., host-level firewall or TCP wrappers)
- Modify enterprise firewalls to restrict outside access to known vulnerable services
- Upgrade or patch vulnerable systems
- Deploy mitigating countermeasures
- Improve configuration management program and procedures
- Assign a staff member to:
  - Monitor vulnerability alerts/mailing lists
  - Examine applicability to environment
  - Initiate appropriate system changes
  - Modify the organization's security policies and architecture



CompTIA Security+ 70 Course Notes

## Responsible Disclosure Program

Bug Bounty Program: Encourages **ethical hackers** to report vulnerabilities in exchange for rewards.

Helps in identifying and addressing vulnerabilities **before they are exploited** in the wild.

Benefits: Gathers **diverse insights** from the global security community, often uncovering issues that internal tests might miss.





# Vulnerability Analysis

## Confirmation:

### False Positive:

- Occurs when a system incorrectly identifies a normal or benign activity as a threat.
- **Requires verification** to avoid wasting resources on non-existent issues.

### False Negative:

- Happens when a system **fails to detect** an actual vulnerability or threat.
- More dangerous as it leaves the system **unknowingly exposed** to potential exploits.



CompTIA Security+ 70 Course Notes

## Common Vulnerability Enumeration (CVE)

A list or database of **publicly known** cybersecurity **vulnerabilities** and exposures.

Each vulnerability is given a **unique identifier** (CVE-ID), facilitating **easy identification** and reference.

<https://www.first.org/cvss/>





CompTIA Security+ 70 Course Notes

## Common Vulnerability Scoring System (CVSS)

A **standardized framework** for rating the severity of vulnerabilities.

Provides scores (ranging from 0 to 10) based on various **metrics** like exploitability, impact, and scope. Higher scores indicate more severe vulnerabilities.

<https://www.first.org/cvss/>





CompTIA Security+ 70 Course Notes

## Prioritization

Involves **ranking** vulnerabilities based on their severity, potential impact, and the likelihood of exploitation.

Prioritization helps in **focusing resources** and efforts on the most critical vulnerabilities that pose the greatest risk.



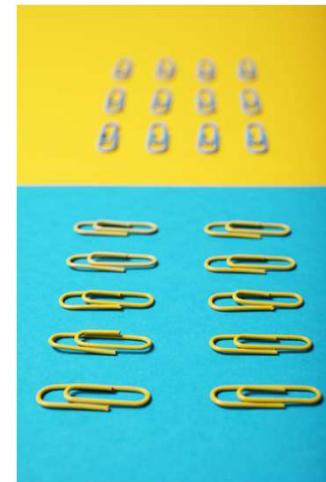


CompTIA Security+ 70 Course Notes

## Vulnerability Classification

Categorizing vulnerabilities into types (e.g., SQL injection, buffer overflow) to **streamline** analysis and remediation.

Classification helps in understanding the nature of vulnerabilities and applying **standardized** mitigation strategies.





CompTIA Security+ 70 Course Notes

## Exposure Factor

Represents the **potential loss** or damage to an asset if a vulnerability is exploited.

Helps in **evaluating the potential impact** of a vulnerability on the organization's assets.





CompTIA Security+ 70 Course Notes

## Environmental Variables

Factors like network architecture, existing security controls, and software dependencies that can **influence the severity** of a vulnerability in a specific environment.

Environmental variables are crucial for **contextualizing** the risk posed by a vulnerability.



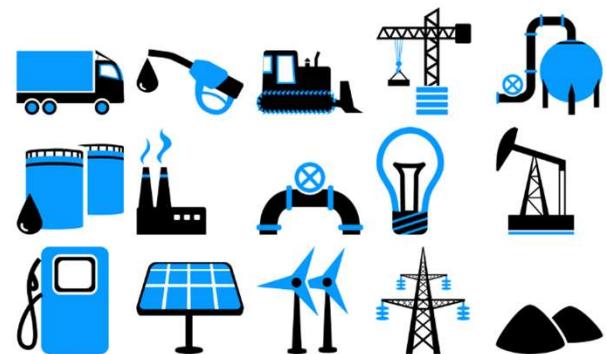


CompTIA Security+ 70 Course Notes

## Industry/Organizational Impact

The potential effect of a vulnerability on **specific industries or organizations**, considering factors like regulatory requirements, business operations, and public image.

Understanding the industry-specific impact is important for **tailoring the response** to vulnerabilities.





## Risk Tolerance

The **level of risk** an organization is willing to accept, influenced by its risk management strategy, business objectives, and regulatory environment.

Determines how aggressively an organization should **respond** to different levels of vulnerabilities.





CompTIA Security+ 70 Course Notes

# Vulnerability Response and Remediation

Vulnerability response and remediation are critical components of cybersecurity, ensuring that vulnerabilities in software or systems are **addressed promptly** to minimize the risk of exploitation.

We will cover:

- Patching
- Insurance
- Segmentation
- Compensating Controls
- Exceptions and Exemptions





## CompTIA Security+ 70 Course Notes

### Patching

Patching involves applying **updates** to software or systems to fix security vulnerabilities that have been identified. These patches are typically released by the **software developers or vendors**.

Importance: Regular patching is crucial because it repairs **security holes** that could be exploited by hackers to gain unauthorized access or damage the system.

Challenges: Challenges include **managing** patches across numerous systems and ensuring **compatibility**, as some patches may cause issues with existing configurations or software.



CompTIA Security+ 70 Course Notes

# Insurance

Cybersecurity insurance is a type of insurance policy that provides coverage against **losses from cyber incidents**, including data breaches and cyberattacks.

**Importance:** This insurance helps mitigate financial risks associated with cyber incidents, providing support for recovery efforts, legal fees, and other related expenses.

**Considerations:** It's important to understand the **coverage scope**, as policies vary in terms of what incidents and expenses are covered.





## CompTIA Security+ 70 Course Notes

# Segmentation

Network segmentation involves **dividing a network** into smaller parts to control access and reduce the potential impact of a breach.

Benefits: By segmenting networks, an organization can **limit the spread** of a breach within its environment, making it harder for attackers to **move laterally** and access sensitive areas.

Implementation: Effective segmentation requires **careful planning** to balance security needs with accessibility and performance requirements.





## Compensating Controls

Compensating controls are security measures that are put in place to offset the risk when standard controls cannot be applied.

Purpose: These controls are used when it's impractical or impossible to implement the preferred security measure, providing an **alternative** way to maintain security levels.

Examples: These might include additional monitoring, alternative security technologies, or manual processes to ensure security.





## CompTIA Security+ 70 Course Notes

# Exceptions and Exemptions

These are situations where standard security policies or controls are not applied, often due to specific requirements or limitations.

**Management:** Managing exceptions and exemptions requires a **formal process** to evaluate and approve them, ensuring that any **deviations** from standard security practices are **justified** and **controlled**.

**Risks:** Although sometimes necessary, exceptions and exemptions can introduce risks, and thus need to be **monitored closely**.



CompTIA Security+ 70 Course Notes

## Validation of Remediation

Validation of remediation is a crucial step in the cybersecurity process. It ensures that the measures taken to fix vulnerabilities are effective and that systems are secure.

We will be covering:

- Rescanning
- Auditing
- Verification





## Rescanning

Rescanning involves using **automated tools** to scan the systems or applications that were subject to remediation efforts. This is done to ensure that the vulnerabilities identified initially have been **successfully patched or mitigated**.

Process: The rescanning process usually **replicates** the conditions of the initial vulnerability scan to ensure a consistent comparison.



## CompTIA Security+ 70 Course Notes

### Audit

An audit in this context refers to a thorough **review** and **examination** of security measures and processes related to the remediation efforts.

#### Components:

- Reviewing documentation,
- Changing management logs
- Interviewing staff involved in the remediation process.

Purpose: The goal is to ensure that the remediation was carried out in accordance with the **planned procedures** and **security standards**. Audits also help in **identifying** any gaps in the security processes and suggest **improvements**.



## CompTIA Security+ 70 Course Notes

# Verification

Verification is the process of **confirming** that the remediation efforts have not only closed the **identified vulnerabilities** but also that they haven't introduced **new vulnerabilities** or negatively impacted the system's **performance** or **functionality**.

Methods: This can include manual testing, reviewing system logs, performance metrics, and conducting functionality tests to ensure that the system is **operating as expected** post-remediation.

User Feedback: Involving end-users or system operators in the verification process can also provide valuable **insights** into any **unforeseen issues** or impacts of the remediation efforts.



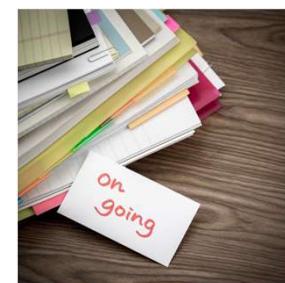
## CompTIA Security+ 70 Course Notes

# Reporting

Reporting is a fundamental aspect of vulnerability management that involves the **documentation** and **communication** of findings related to vulnerabilities in an organization's systems and networks.

Effective reporting is crucial for several reasons:

- Documentation of Vulnerabilities
- Facilitating Decision Making
- Compliance and Regulatory Requirements
- Communication with Stakeholders
- Tracking and Accountability
- Continuous Improvement



# Lesson 15 Alerting and Monitoring IT

---



CompTIA Security+ 70 Course Notes

# Monitoring Computing Resources

This process involves continuously overseeing various components of the IT infrastructure, including systems, applications, and the broader infrastructure.

We will be covering:

- Systems Monitoring
- Applications Monitoring
- Infrastructure Monitoring





## Systems Monitoring

Systems monitoring focuses on the health and performance of **individual computing systems**, such as servers, workstations, and other endpoint devices.

Key Aspects: This includes monitoring for:

- Unusual or unauthorized changes in system configurations
- Resource utilization (like CPU, memory, and disk usage)
- System uptime
- Performance metrics

Security Implications: By monitoring these elements, organizations can **detect** potential security incidents, such as a system compromise or unauthorized access, and respond quickly.



## CompTIA Security+ 70 Course Notes

# Applications Monitoring

Application monitoring is concerned with the performance and security of **software applications**.

It involves tracking:

- Application performance
- User activity
- Error logs
- Transaction times

This also includes monitoring for **unusual activity** that might indicate a security breach, such as unexpected data access patterns, changes in user behavior, or anomalies in transaction volumes.

Benefits: Effective application monitoring helps in quickly **identifying** and **addressing** performance bottlenecks, software bugs, and potential security vulnerabilities within applications.



## CompTIA Security+ 70 Course Notes

# Infrastructure Monitoring

Infrastructure monitoring refers to overseeing the **entire IT infrastructure** of an organization, which includes network components, data centers, cloud services, and any other critical infrastructure elements.

### Scope:

- Network traffic analysis
- Monitoring the health and status of routers, switches, firewalls, and other networking devices
- Performance and security of data storage systems.

Objectives: The primary goal is to ensure the infrastructure's **integrity, availability, and performance**. This includes identifying potential security threats like network breaches, unusual traffic patterns, or attempts to access restricted areas of the network.



CompTIA Security+ 70 Course Notes

## Monitoring Activities

We will be covering the following critical monitoring activities:

- Log Aggregation
- Alerting
- Scanning
- Reporting
- Archiving
- Alert Response and Remediation/Validation
  - Quarantine
  - Alert Tuning





CompTIA Security+ 70 Course Notes

## Log Aggregation

Log aggregation involves **collecting** and **consolidating** logs from various sources within the IT environment, such as servers, applications, network devices, and security systems.

Purpose: Aggregating logs in a central location:

- Simplifies analysis
- Aids in detecting patterns or anomalies
- Is essential for comprehensive security monitoring.





## CompTIA Security+ 70 Course Notes

### Alerting

Alerting refers to the process of **configuring security systems** to **notify** administrators or security teams of potential security incidents.

Key Features: Effective alerting systems should **minimize false positives** and provide **actionable insights**. They typically include thresholds and rules to trigger alerts for specific conditions.





## CompTIA Security+ 70 Course Notes

### Scanning

Scanning encompasses various types of **security scans**, such as vulnerability scans, network scans, and application scans.

Objective: The primary goal is to **identify** vulnerabilities, misconfigurations, or other security weaknesses that need to be addressed.





## CompTIA Security+ 70 Course Notes

### Reporting

Reporting involves the generation of **detailed reports** about the **security status** of the IT environment.

Components: These reports can include details of identified vulnerabilities, incidents, and the outcome of security scans, **providing insights** for decision-makers and compliance purposes.





CompTIA Security+ 70 Course Notes

## Archiving

Archiving is the process of **securely storing** historical security data, such as logs and incident reports, for future reference.

Importance: It's crucial for **compliance** with legal and regulatory requirements, as well as for **historical analysis** and investigating **long-term trends**.





## CompTIA Security+ 70 Course Notes

# Alert Response and Remediation/Validation

Quarantine: Involves **isolating** affected systems or components to prevent the **spread of a threat** or further damage. Quarantining is often an **immediate response** to a security alert.

Alert Tuning: Refers to **refining alerting mechanisms** to reduce false positives and ensure that alerts are **relevant** and **actionable**. This might involve adjusting thresholds, revising rules, or implementing more sophisticated detection algorithms.





CompTIA Security+ 70 Course Notes

## Security Alerting and Monitoring Tools

A variety of tools are utilized to ensure the integrity and security of information systems. We will be covering:

- Security Content Automation Protocol (SCAP)
- Benchmarks
- Agents/agentless
- Security information and event management (SIEM)
- Antivirus
- Data loss prevention (DLP)
- Simple Network Management Protocol (SNMP) traps
- NetFlow
- Vulnerability scanners



CompTIA Security+ 70 Course Notes

## Security Content Automation Protocol

SCAP is a **suite of standards** for automating the process of configuring and monitoring network devices for compliance with security policies.

Use: It's used for vulnerability management, measurement, and policy compliance evaluation. SCAP can **automatically verify** the installation of patches, check system security configurations, and examine software flaws.





## CompTIA Security+ 70 Course Notes

# Benchmark

Benchmarks in security refer to **standardized** sets of **best practices** and configurations that are known to ensure a higher level of security.

Use: Organizations use these benchmarks to configure systems and applications to an industry-accepted standard to mitigate the risk of vulnerabilities and attacks.



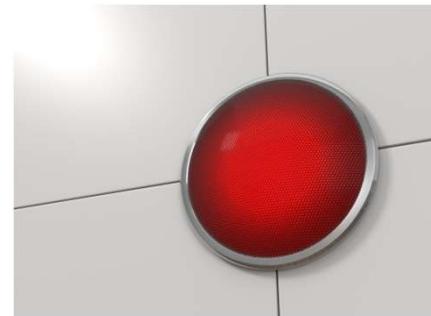


## Agents/Agentless

Software agents are installed on servers or devices to monitor, collect, and send data back to a **central server** for analysis.

Agentless: In contrast, agentless systems monitor devices **without installing dedicated software** on them, often using **existing protocols** and services.

Comparison: Agent-based solutions can provide **more detailed data** but can be more resource-intensive. Agentless solutions are **easier to deploy** but might offer **less comprehensive data**.





CompTIA Security+ 70 Course Notes

## Security Information and Event Management

SIEM is a solution that provides **real-time analysis** of security alerts generated by applications and network hardware.

It is used for:

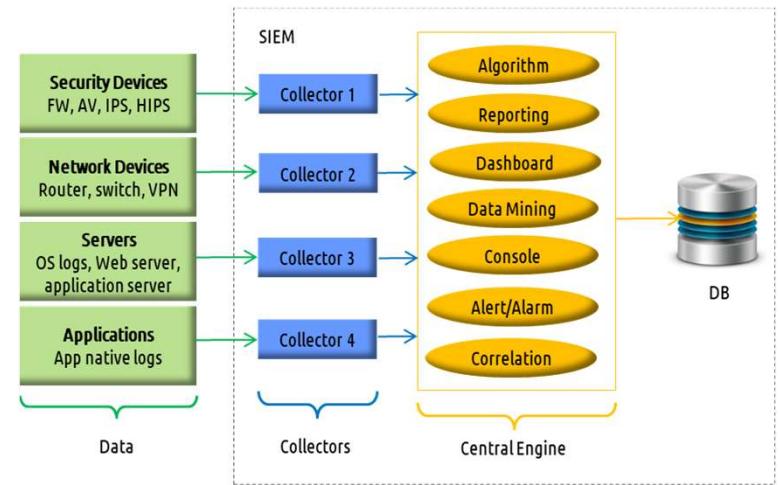
- Log management
- Event correlation
- Alerting
- Reporting

SIEM is crucial for detecting, understanding, and responding to security incidents.



CompTIA Security+ 70 Course Notes

# Security Information and Event Management





## CompTIA Security+ 70 Course Notes

### Antivirus

Antivirus software is designed to detect, prevent, and remove malware, including viruses, worms, and trojans.

It's a fundamental tool in any security setup, providing a **basic level of protection** against **common threats**.





CompTIA Security+ 70 Course Notes

## Data Loss Prevention

DLP solutions identify, monitor, and protect data in use, in motion, and at rest through **deep content inspection** and **contextual security analysis**.

They help prevent sensitive data from being lost, misused, or accessed by unauthorized users.





CompTIA Security+ 70 Course Notes

# Simple Network Management Protocol Traps

SNMP traps are **alerts** sent by network devices to a **management station**, indicating that an event or a change in status has occurred.

They are used for **managing** and **monitoring** network devices, helping administrators stay informed about the health and status of their networks.





CompTIA Security+ 70 Course Notes

## NetFlow

NetFlow is a **network protocol** developed by **Cisco** for collecting IP traffic information and monitoring network flow data.

It's valuable for **network traffic analysis**, helping in understanding traffic patterns, usage trends, and detecting anomalies.



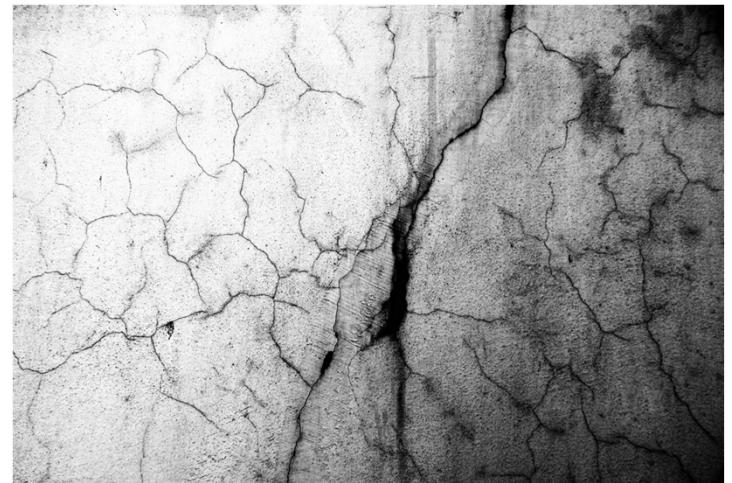


CompTIA Security+ 70 Course Notes

## Vulnerability Scanners

These are tools designed to **assess** computers, networks, or applications for **known vulnerabilities**.

They are essential in a security toolkit for **identifying weaknesses** that could be exploited by attackers and for verifying the efficacy of security measures.



# Lesson 16 Enhance Security

---



## CompTIA Security+ 70 Course Notes

### Firewall

A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.

At its most basic, a firewall is a barrier between a private internal network and the public Internet.

We will be covering:

- Rules
- Access lists
- Ports/protocols
- Screened subnets



## CompTIA Security+ 70 Course Notes

# Firewall

### Rules:

- Function: Firewall rules are **specific configurations** that control how the firewall operates. These rules determine which traffic should be **allowed** or **blocked**.
- Example: A rule might specify that all inbound traffic on port 80 (HTTP) is allowed, while all inbound traffic on port 23 (Telnet) is blocked.

### Access Lists

- Function: Access lists are a **series of commands** applied to a firewall, which selectively **filter traffic** based on the source and destination addresses, protocols, and ports.

### Ports/Protocols

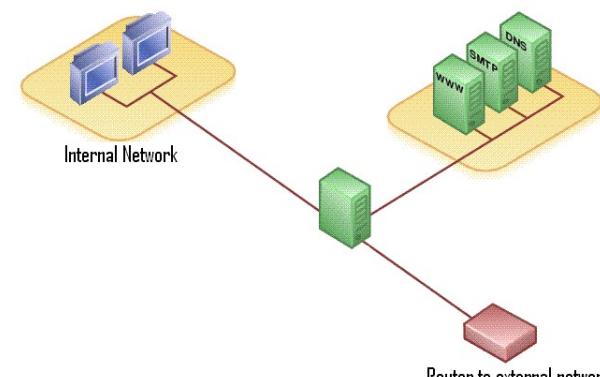
- Ports and protocols are essential components in network communications that must be secured by firewalls.



## Screened Subnets

Concept: A screened subnet or DMZ is a physical or logical **subnetwork** that contains and exposes an organization's external-facing services to an untrusted network, usually the Internet.

Implementation: Firewalls are configured to allow limited traffic from the DMZ to the internal network, with **strict rules** to control what types of interactions are allowed.



[https://en.wikipedia.org/wiki/Screened\\_subnet](https://en.wikipedia.org/wiki/Screened_subnet)



CompTIA Security+ 70 Course Notes

## Web Filter

Implementing a web filter is essential for **controlling** the websites and content that users can access, thus mitigating the risk of exposure to malicious content.





## CompTIA Security+ 70 Course Notes

### Agent-Based

Agent-based web filtering involves installing software agents on **individual user devices**.

These agents enforce web access policies set by the organization, regardless of the network the device is connected to.

Use Case: This approach is particularly useful for managing the web access of **remote or mobile employees** who might not always be connected to the corporate network.





## Centralized Proxy

A centralized proxy, often part of a larger network security appliance, acts as an **intermediary** between users and the internet.

All web traffic passes through this proxy, which enforces web filtering policies.

Advantages: This method offers **centralized** management and control, making it easier to enforce **consistent** web access policies across the entire organization.





## CompTIA Security+ 70 Course Notes

# Universal Resource Locator Scanning

Function: URL scanning involves **examining the URLs** requested by users to determine if they should be allowed or blocked.

This can be based on a **database** of categorized URLs.

Application: URL scanning is effective in preventing access to **known** malicious or inappropriate websites.

It's a fundamental component of most web filtering solutions.



## CompTIA Security+ 70 Course Notes

# Content Categorization

Content categorization **classifies** web pages into different categories (like social media, adult content, gaming, etc.) based on their content.

Purpose: This allows organizations to block or allow **entire categories** of websites, making policy enforcement more **streamlined** and **consistent**.





## CompTIA Security+ 70 Course Notes

### Block Rules

Block rules in web filtering are **specific criteria** set to block access to certain websites or content.

These rules can be based on URLs, keywords, categories, or other identifiable aspects of web content.

Customization: Organizations can customize block rules to align with their security **policies**, regulatory **compliance** needs, and organizational **culture**.





## Reputation

Reputation-based filtering uses the **reputation score** of websites to determine whether they should be allowed or blocked.

Mechanism: Reputation scores are usually derived from various factors like the **website's history**, the **presence of malware**, and **user feedback**.

Effectiveness: This method is particularly effective in protecting against **newly created** malicious sites that may not yet be categorized or have a known URL pattern.





CompTIA Security+ 70 Course Notes

## OS Security (Group Policy)

Group Policy is a feature in Windows operating systems that allows administrators to control the working environment of user accounts and computer accounts.

- It provides **centralized management** and configuration of operating systems, applications, and users' settings.
- Application of Security Settings: Group Policy can **enforce** password policies, lockout policies, and audit policies. It can **configure** user rights, security options, and control access to files, folders, and registry keys.



CompTIA Security+ 70 Course Notes

## OS Security (SELinux)

SELinux is a security module in **Linux** systems that provides a mechanism for supporting access control security policies.

- Mandatory Access Control (MAC): Unlike traditional discretionary access control systems, SELinux enforces **mandatory** access control policies that administrators define to control access to all processes and files.



CompTIA Security+ 70 Course Notes

## Implementation of Secure Protocols

Implementing secure protocols in an enterprise environment is a crucial aspect of ensuring data integrity, confidentiality, and availability.

The process involves careful selection of protocols, ports, and transport methods.





## CompTIA Security+ 70 Course Notes

# Protocol Selection

Each protocol serves different purposes and offers varying levels of security.

HTTP vs HTTPS: For web traffic, HTTPS (Secure Hypertext Transfer Protocol) should be used instead of HTTP. HTTPS **encrypts data** between the client and server, safeguarding against eavesdropping and man-in-the-middle attacks.

SSH over Telnet: For remote administration, SSH (Secure Shell) should be used instead of Telnet. SSH provides **encrypted** connections, while Telnet transmits data in plain text.

TLS for Email: Protocols like SMTP, IMAP, and POP3 should be secured with TLS (Transport Layer Security) to protect email communications.

Secure File Transfer: Instead of FTP, use SFTP (SSH File Transfer Protocol) or FTPS (FTP Secure), which offer **secure channels** for transferring files.



## CompTIA Security+ 70 Course Notes

# Port Selection

Ports are numerical identifiers in host-to-host communication. Using **standard ports** for the corresponding secure protocols is generally recommended, but sometimes altering port numbers can add an extra layer of security.

HTTPS: Default port 443. It's advisable to use this standard port for HTTPS traffic to ensure compatibility with client software.

SSH: Default port 22. Some organizations change this to a **non-standard port** as a security measure to avoid automated attacks, though this should not be the only defense mechanism.

Email Protocols: For secure email transmission, use ports like 587 (SMTP with STARTTLS), 993 (IMAP over SSL), and 995 (POP3 over SSL).



## Transport Method

The transport method refers to how data is **encapsulated** and **transmitted** over the network. It's important to ensure that the data remains secure during transit.

**VPN (Virtual Private Network):** A VPN creates a **secure tunnel** between the user and the network, encrypting all data that passes through. This is crucial for **remote access** to a corporate network.

**IPSec (Internet Protocol Security):** IPSec is used to secure **Internet communications** and can **encrypt** data between various devices like routers, firewalls, desktops.

**TLS/SSL:** Transport Layer Security and its predecessor, Secure Sockets Layer, are **cryptographic protocols** designed to provide secure communication over a computer network.



CompTIA Security+ 70 Course Notes

## DNS Filtering

DNS filtering is a network security technique used to **block** access to malicious **websites** and **content** that is inappropriate or non-compliant with company policies. It involves using the Domain Name System (DNS) to control web traffic based on **domain names**.





CompTIA Security+ 70 Course Notes

## Choosing a DNS Filtering Solution

Commercial DNS Filtering Services: These services offer **robust** filtering options and are often updated with the **latest** threat intelligence. They can be cloud-based or on-premises.

Open Source Alternatives: There are open-source DNS filtering solutions that can be **customized** but may require more technical **expertise to manage**.



## CompTIA Security+ 70 Course Notes



# Email Security



## CompTIA Security+ 70 Course Notes

# Email Security Gateway

Definition: An Email Security Gateway is a hardware or software solution used to **monitor** and **manage** incoming and outgoing emails to prevent spam, phishing attacks, and other malware.

Functionality: It **scans** for viruses and other malware, filters spam, can **encrypt** data, and **prevent data loss**.

Deployment: Gateways can be deployed on-premises or in the cloud and are often used in **conjunction** with DMARC, DKIM, and SPF for comprehensive email security.



## Sender Policy Framework

Function: SPF is an email **authentication** method used to prevent spammers from sending messages on behalf of your domain.

Mechanism: SPF verifies the sender's IP address against the **list of authorized sending IPs** published in the DNS records of the sender domain.





CompTIA Security+ 70 Course Notes

## DomainKeys Identified Mail

Function: **DKIM** provides a method for **validating** a domain name identity associated with an email message through **cryptographic authentication**.

Mechanism: It uses **digital signatures** linked to a **domain name** to verify that the message wasn't altered in transit, thereby authenticating the sender.





CompTIA Security+ 70 Course Notes

## Domain-based Message Authentication Reporting and Conformance

Function: DMARC is an email validation system designed to detect and prevent email spoofing. It uses DKIM and SPF to determine the authenticity of an email message.

Purpose: The primary goal is to enable email senders and receivers to determine whether a given message aligns with what the receiver knows about the sender. If not, DMARC provides instructions on how to handle these **discrepancies**.



## File Integrity Monitoring

File Integrity Monitoring (FIM) is a critical security process that involves the **detection** and **alerting** of **changes** to files and directories on a system.

- FIM is used to ensure that files have not been **tampered** with or **altered** by unauthorized parties.
- FIM systems typically work by creating a baseline of file characteristics (like hashes, sizes, and permissions) and then continuously monitoring these files for any changes against this baseline.



CompTIA Security+ 70 Course Notes

## Network Access Control

The primary goal of **NAC** is to **prevent unauthorized access** to network resources and to ensure that all devices and users on the network **comply** with the established security policy.

This helps in **mitigating risks** posed by non-compliant or infected devices.





CompTIA Security+ 70 Course Notes

## Network Access Control

Health Checks: Assessing the **security status** of devices, including the presence of antivirus software, system updates, and security patches.

Compliance with Regulations: Helping organizations comply with security **regulations** by ensuring only compliant devices can access sensitive data.



## CompTIA Security+ 70 Course Notes

# Network Access Control

Pre-Admission Control: Includes device **authentication** and **policy enforcement** before allowing access to the network.

Post-Admission Control: Involves continuous **monitoring** of devices to ensure they remain **compliant** with security policies after gaining network access.





CompTIA Security+ 70 Course Notes

## EDR and XDR

Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) are **advanced** security solutions designed to provide **comprehensive** threat detection, analysis, and response.





CompTIA Security+ 70 Course Notes

## Endpoint Detection and Response (Definition)

EDR is a cybersecurity solution focused on **detecting, investigating, and mitigating** suspicious activities and issues on hosts and endpoints (like laptops, workstations, and mobile devices).





CompTIA Security+ 70 Course Notes

## Endpoint Detection and Response (Key Functions)

Continuous Monitoring: EDR systems **continuously monitor** endpoint data to detect threats.

Threat Detection: Utilizes advanced analytics to **identify** potential security threats.

Response Capabilities: Offers tools to **respond** to identified threats, such as isolating endpoints or removing malware.



## CompTIA Security+ 70 Course Notes

# User Behavior Analytics

UBA refers to the use of analytics to **monitor** and **evaluate** user behavior on IT systems and networks.

UBA involves **collecting and analyzing** data on how users interact with the organization's IT systems and applications.

This data includes user activities, access to systems and data, and network operations.

The primary goal of UBA is to detect **anomalies or deviations** from normal user behavior that could indicate potential security threats, such as insider threats, compromised accounts, or external attacks using stolen credentials.

# Lesson 17 Identity and access management.

---



## Identity Proofing

Identity proofing involves validating that a person is who they claim to be.

It involves **verifying an individual's identity** through various means before granting access to systems and data.

Effective identity proofing is key to maintaining security, ensuring regulatory compliance, and building trust in digital transactions, while also posing challenges in balancing security, user experience, and privacy.





## CompTIA Security+ 70 Course Notes

# Identity Proofing (Key Components)

Verification of Personal Information: This typically involves taking government-issued IDs, biometric data, or other personal information and **checking them against trusted sources** to ensure their authenticity.

Knowledge-Based Authentication (KBA): **Asking personal questions** (like previous addresses or maiden names) that only the legitimate user would likely know.

Document Verification: **Examining documents** such as driver's licenses, passports, or birth certificates for authenticity.

Biometric Verification: Using fingerprint, facial recognition, or other **biometric data** to confirm identity.

Use of Third-Party Services: Employing **external services** or databases to validate the identity of an individual.



CompTIA Security+ 70 Course Notes

## Provisioning User Accounts

Provisioning user accounts refers to the process of creating and setting up new user accounts with **appropriate access rights** in an organization's systems and applications.





## CompTIA Security+ 70 Course Notes

# Provisioning User Accounts (Key Steps)

User Identification: Determining the **identity** of the new user and their role in the organization.

Access Rights Assignment: Assigning appropriate access levels based on the user's **role**, following the principle of least privilege (PoLP), where users are given the **minimum** levels of access necessary to perform their duties.

Account Creation: Setting up the user account in **various systems**, which may include email, file storage, databases, and other applications.

Security Measures: Implementing security measures such as strong password requirements, multi-factor authentication (MFA), and security training.



CompTIA Security+ 70 Course Notes

## De-provisioning User Accounts

De-provisioning involves the process of **removing or disabling** user accounts when they are no longer needed, typically when an employee leaves the organization or changes roles.





CompTIA Security+ 70 Course Notes

## De-provisioning User Accounts (Key Steps)

Access Revocation: Terminating the user's **access** to all systems and applications.

Data Handling: Ensuring any data associated with the user is handled according to organizational and legal requirements.

This may involve **transferring ownership** of files or emails to another employee.

Account Disabling or Deletion: Disabling or permanently deleting the user **account** to prevent future access.



CompTIA Security+ 70 Course Notes

## Permission Assignments

Permission assignments are a core component of identity and access management, involving the allocation of access rights to users.

These assignments must be handled carefully, following principles like least privilege and role-based access, to maintain security and compliance.





CompTIA Security+ 70 Course Notes

## Single Sign-On

Single Sign-On is a common feature where users **log in once** and gain **access to multiple systems** without the need to re-authenticate. This enhances user experience and productivity.





CompTIA Security+ 70 Course Notes

## SSO (Importance)

Reduced Password Fatigue: SSO reduces the number of passwords users must manage, **decreasing the likelihood of weak password practices.**

Centralized Authentication Control: Provides centralized control over user access to multiple systems, making it **easier to enforce security policies.**

Reduced IT Workload: **Simplifies the management of user accounts** and credentials, reducing the workload on IT departments.



## CompTIA Security+ 70 Course Notes

### LDAP

LDAP (Lightweight Directory Access Protocol) is a protocol for accessing and maintaining **distributed directory information services**, like user and group details, over an IP network.

Usage: Primarily used for directory services and information lookup. Commonly utilized for **storing user credentials and groups** in an enterprise environment.

The foundation for Microsoft Active Directory and used as Linux Open LDAP.



## CompTIA Security+ 70 Course Notes

### Federation

Federation in cybersecurity is the process of **linking and managing identities** across different systems and organizational boundaries.

It enables users to use the same identity or set of credentials to **access multiple applications or services**.

It allows for single sign-on and **streamlined access management**, enhancing user experience and operational efficiency.

Federation involves identity providers, service providers, and specific protocols, and is crucial for **centralized authentication** and compliance.



## CompTIA Security+ 70 Course Notes

### SAML

SAML (Security Assertion Markup Language) is an open standard for exchanging authentication and authorization data between parties, specifically **between an identity provider and a service provider**.

Usage: Widely used for SSO to allow users to log in to multiple applications with one set of credentials.

Characteristics: SAML uses XML for data exchange and is focused on both authentication and authorization. It's **particularly useful in enterprise-level SSO**.



CompTIA Security+ 70 Course Notes

## SAML (Key Components)

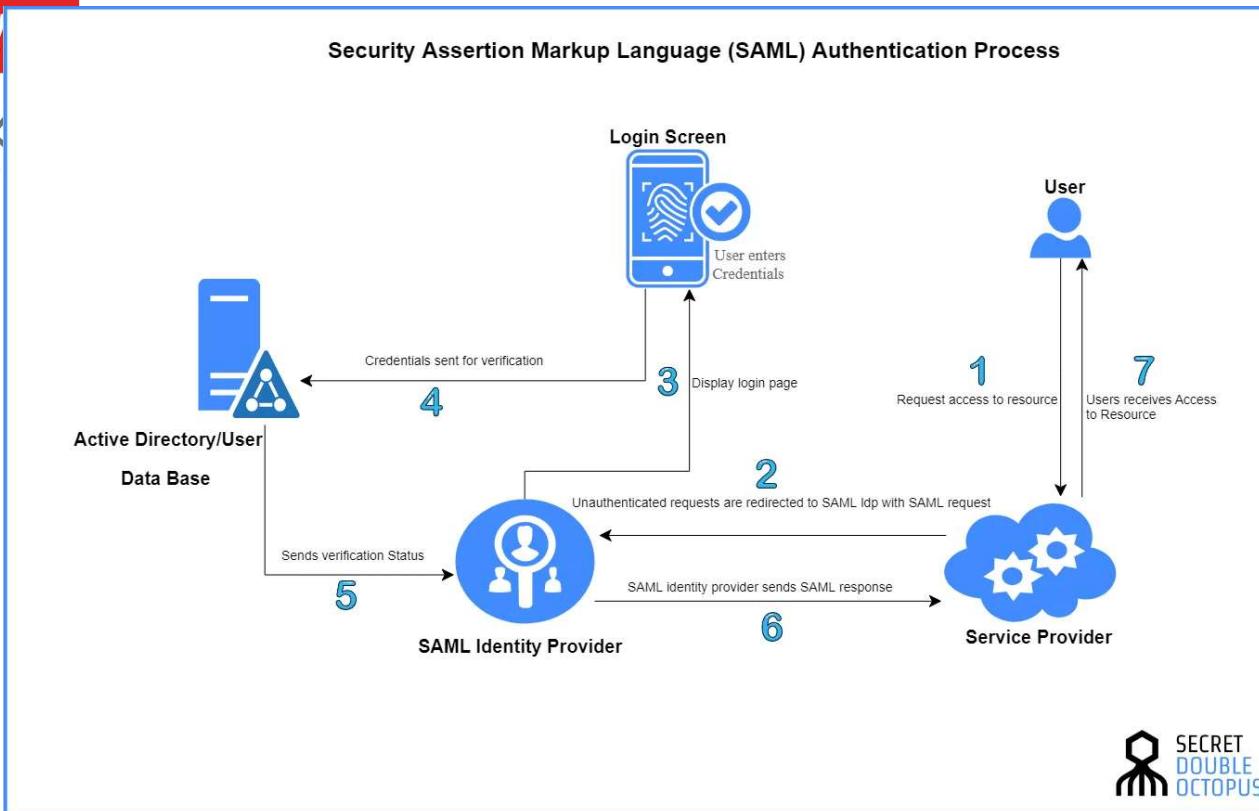
Identity Providers (IdPs): Services that **authenticate users** and provide identity information to service providers. Examples include Okta, Microsoft Azure AD, and Google Identity.

- Attestation (formal verification that something is true), is done by the IdPs. They attest that user is who they claim to be.

Service Providers (SPs): The applications or services that rely on information from the IdP to **provide access** to the user.

## CompTIA Security+ 70 Course Notes

# SAML





## CompTIA Security+ 70 Course Notes

# OAuth

OAuth is an open standard for access delegation.

It is used to grant websites or applications access to their information on other websites but without giving them the passwords.

Usage: Commonly used for authorizing third-party applications to **access a user's data without exposing user credentials**.

Characteristics: OAuth is about **authorization** (not authentication) and is used to grant **limited access to an application** on behalf of the user.



## CompTIA Security+ 70 Course Notes

# OpenID Connect

OpenID Connect is an identity layer on top of OAuth 2.0. It allows clients to verify the identity of the end-user based on the authentication performed by an **authorization server**.

Usage: Primarily used for authentication in **modern web applications** and **mobile applications**.

Characteristics: OpenID Connect extends OAuth 2.0 for use cases involving identity assertion.



CompTIA Security+ 70 Course Notes

## Interoperability

Interoperability in cybersecurity refers to the ability of different systems, devices, applications, and organizations to effectively communicate, exchange, and use information securely and efficiently.

Interoperability **enhances** collaboration, flexibility, and user experience while **posing challenges** in compatibility, security, and compliance.



## CompTIA Security+ 70 Course Notes

# Access Controls

Access controls are mechanisms and policies used to **manage and restrict access to resources in an information system**.

Various types of access controls include DAC, MAC, RBAC, and ABAC, each with its specific **use cases and implications** for security and compliance.

The effective implementation of access controls requires **balancing security, complexity, and usability**, and is a vital part of any comprehensive cybersecurity strategy.





## CompTIA Security+ 70 Course Notes

# Access Controls (DAC and MAC)

### Mandatory Access Control (MAC):

MAC is a security model in which access rights are regulated by a **central authority** based on different levels of security clearance.

Use Case: Common in **government and military** systems where classified information is involved.

Key Aspect: Users cannot change access permissions; they are set and enforced by a system **administrator**.

### Discretionary Access Control (DAC):

In DAC, the **resource owner** decides on access levels. It is the most flexible access control model.

Use Case: Used in environments where **users** need control over the resources they own, like setting file permissions in an operating system.

Key Aspect: Risk of **users granting excessive access**, potentially leading to security breaches.



CompTIA Security+ 70 Course Notes

## Access Controls (RBAC)

**RBAC (Role-Based Access Control):**  
assigns permissions based on a user's **role** within an organization.

Use Case: **Common in corporate environments** where roles define job functions and access needs.

Key Aspect: **Streamlines access management**, especially in organizations with many users and roles.





## CompTIA Security+ 70 Course Notes

# Access Controls

### **Rule-Based Access Control:**

Access decisions are **based on a set of rules defined by the system administrator**.

Use Case: Useful in environments requiring **stringent access control**, like securing network resources.

Key Aspect: Rules can be based on various criteria, such as source/destination IP addresses in firewalls.

### **ABAC (Attribute-Based Access Control):**

uses policies that **evaluate attributes** (or characteristics) of users, the environment, and resources.

Use Case: Effective in **complex environments** with diverse and dynamic user attributes.

Key Aspect: Provides **fine-grained control**, allowing for more nuanced access decisions based on multiple factors.



CompTIA Security+ 70 Course Notes

## Multifactor Authentication

MFA is a security system that requires **more than one method of authentication** from independent categories of credentials to verify the user's identity for a login or other transaction.

This approach combines **two or more distinct authentication factors**, significantly increasing security.





## CompTIA Security+ 70 Course Notes

# MFA (Authentication Factors)

Something You Know: Commonly used but **vulnerable to theft or guessing or brute force.**

Examples: Passwords, PINs, answers to security questions.

Something You Have: Adds a layer of security by **requiring a physical device** in possession of the user.

Examples: Mobile devices with authentication apps, smart cards, security tokens.

Something You Are: **Highly secure**, but implementation can be **complex and costly**.

Examples: Biometric verification methods.

Somewhere You Are (Location-Based Authentication): Adds **contextual security** by restricting access to specific locations.

Examples: Authentication based on the user's geographic location, using GPS or network-based methods.



## CompTIA Security+ 70 Course Notes

# Tokens

### Hard/Soft Authentication Tokens:

- Hard Tokens: **Physical devices** (e.g., key fobs, smart cards) used to generate secure codes.
- Soft Tokens: Software-based approaches that **generate a secure code** on a user's device (like a smartphone).
- Use Case: Both are used to provide a **time-sensitive passcode** as an additional authentication factor.





## CompTIA Security+ 70 Course Notes

# Security Key

A security key is a **physical hardware device** used for verifying a user's identity. It is also used as a part of multifactor authentication.

Functionality: Unlike hard tokens that generate a passcode, security keys usually **work by being plugged into a computer or connected wirelessly**.

They often support **protocols** like Universal 2nd Factor (U2F) or FIDO2, and they authenticate by **proving possession of the key** (something you have) in response to an authentication request.

Examples: USB security keys (like YubiKey or Google Titan), NFC-enabled keys, or Bluetooth-enabled keys.





## CompTIA Security+ 70 Course Notes

# Biometric

Based on unique physical attributes or behavior

- Biometric authentication is a type of system that relies on the unique biological characteristics of individuals
- Sophisticated but expensive
- Types:
  - **Fingerprints:** Visible patterns on the fingers and thumbs
  - **Face Scans:** Uses geometric patterns of face
  - **Retina Scans:** Focuses on the pattern of blood vessels at the back of the eyes. Most accurate but least acceptable. Can reveal high blood pressure and pregnancy
  - **Iris Scans:** Focused on the colored area around the pupil, second-most accurate, longer authentication life span
  - **Palm Scans:** Scans the palm, uses infrared light to measure vein patterns in the palm

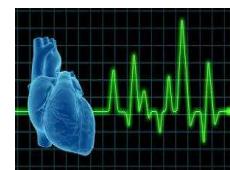




## CompTIA Security+ 70 Course Notes

### Biometric

- **Hand Geometry:** Recognizes the physical dimension of the hand, including width and length of the fingers and hands
- **Heart/Pulse Pattern:** Often employed as a secondary biometric to support another type of authentication
- **Voice Pattern Recognition:** Relies on the characteristics of a person's speaking voice, known as voiceprint
- **Signature Dynamics:** Examines both how a subject performs the act of writing as well as features in a written sample. The success relies on pen pressure, stroke pattern, stroke length, and the point in time when the pen is lifted from the writing surface
- **Keystroke Patterns:** Measure how a subject uses a keyboard by analyzing flight time (how long it takes between key presses) and dwell time (how long a key is pressed)

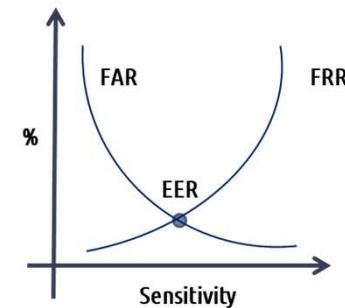




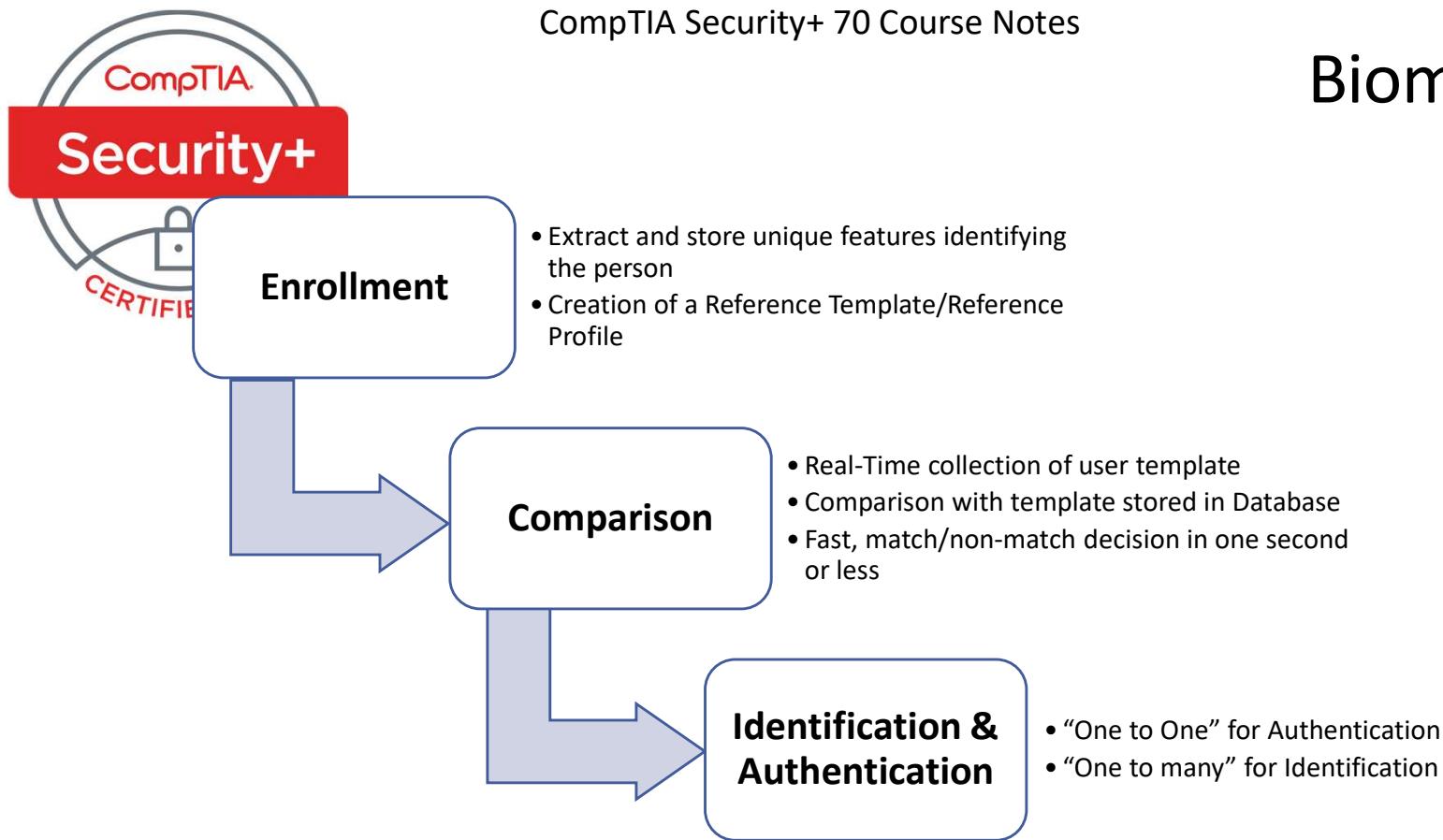
## CompTIA Security+ 70 Course Notes

### Biometric

- **Error Ratings**
- **Type 1 Error:** Occurs when a valid subject is not authenticated
  - More common when the device is too sensitive
  - The ratio of Type 1 errors to valid authentications is **False Rejection Rate (FRR)**
- **Type 2 Error:** Occurs when an invalid subject is authenticated
  - More common when the device is not sensitive enough
  - The ratio of type 2 error to valid authentications is **False Acceptance Rate (FAR)**
- **Crossover Error Rate (CER) / Equal Error Rate (EER):** Point where FRR and FAR percentages are equal
  - The devices with lower CER are more accurate



## Biometric





CompTIA Security+ 70 Course Notes

## Passwords

Passwords are a fundamental component of cybersecurity, serving as the **first line of defense** in many systems.





## CompTIA Security+ 70 Course Notes

# Password Best Practices

Length: The longer the password, the more secure it generally is. A minimum of 8-12 characters is often recommended.

Complexity: Passwords should include a mix of uppercase and lowercase letters, numbers, and special characters to resist common attack methods like brute force.

Reuse: Avoid using the same password across multiple accounts to prevent a single breach from compromising multiple systems.

Expiration: Regularly changing passwords, traditionally every 90 days, though this practice is being reconsidered in light of modern security insights.

Age: Monitoring the age of passwords helps in enforcing timely updates and identifying potentially vulnerable accounts.



CompTIA Security+ 70 Course Notes

## Password Managers

Encouraged for managing a **large number of complex passwords**. Password managers store and encrypt passwords, requiring the user to remember only **one strong master password**.





CompTIA Security+ 70 Course Notes

## Passwordless Authentication

An emerging trend where traditional passwords are **replaced with alternative methods like biometrics**, security keys, or one-time tokens sent to a user's device.

This approach enhances security by **eliminating the risks associated with weak or compromised passwords**.





## CompTIA Security+ 70 Course Notes

# Privileged Access Management Tools

PAM tools are used to **control, manage, and monitor access** to critical systems and resources **within an organization**, particularly focusing on **privileged users** who have elevated access rights.

They help mitigate risks associated with privileged accounts by ensuring that **elevated access is provided securely and managed effectively**.

Key aspects of PAM include Just-in-Time permissions for time-limited access, password vaulting for secure credential management, and ephemeral credentials for temporary access with minimal risk.



## CompTIA Security+ 70 Course Notes

### Just-in-Time

Just-in-Time (JIT) permissions grant privileged access on an as-needed basis, typically for a limited period.

#### Functionality:

Reduces the risk of privilege abuse by ensuring privileges are granted **only when necessary and for the shortest time required.**

Often includes approval workflows to ensure oversight.

Use Case: Ideal for situations where users need **temporary elevated access for specific tasks**, like system maintenance or troubleshooting.



## Password Vaulting

Password vaulting involves securely storing and managing credentials for privileged accounts in a **centralized repository (vault)**.

### Functionality:

Users check out credentials **when needed**, which are then returned to the vault.

The vault **automatically** manages, rotates, and updates passwords, reducing the risk of password reuse or theft.

Use Case: Used for managing a **large number of privileged accounts** to ensure secure and controlled access.



## CompTIA Security+ 70 Course Notes

# Ephemeral Credentials

Ephemeral credentials are temporary credentials that are generated on-demand and **expire after a short duration**.

### Functionality:

Enhances security by ensuring credentials are valid only for a brief period and for a specific purpose.

**Reduces the risk of long-term credential compromise.**

Use Case: Useful in dynamic environments like cloud computing, where **temporary access is needed frequently**.



# Lesson 18 automation and orchestration

---



CompTIA Security+ 70 Course Notes

## Automation and Orchestration

This lesson focuses on **practical applications** of automated processes and scripting to enhance security and operational efficiency.

We will be covering:

- User provisioning
- Resource provisioning
- Guard rails
- Security groups
- Ticket creation
- Escalation
- Enabling/disabling services and access
- Continuous integration and testing
- Integrations and Application programming interfaces (APIs)



CompTIA Security+ 70 Course Notes

## User Provisioning

Automation in user provisioning involves **scripts** or **automated workflows** to create, manage, and deactivate user accounts in various systems.

This can include setting up new accounts, assigning appropriate permissions, and removing access when no longer needed, ensuring consistent adherence to security policies.





CompTIA Security+ 70 Course Notes

## Resource Provisioning

This use case involves automatically **allocating and managing computing resources** such as CPU, memory, and storage based on real-time demand.

**Automation helps in dynamically adjusting resources**, reducing the risk of over-provisioning (which can be expensive) or under-provisioning (which can lead to performance issues).





## CompTIA Security+ 70 Course Notes

# Guard Rails

Implementing guard rails through automation involves setting up scripts or **automated controls to enforce security policies** and operational best practices.

This can include limits on user access, automated compliance checks, and restrictions on the types of actions that can be performed in a system.





CompTIA Security+ 70 Course Notes

## Security Groups

Automation can be used to manage security groups, which are **sets of users or systems that have common security requirements** and permissions.

Scripts or automated tools can ensure these groups are kept up-to-date and that their security settings are consistently applied.





CompTIA Security+ 70 Course Notes

## Ticket Creation

In incident response and service management, automation plays a crucial role in ticket creation.

Automated systems can detect anomalies or issues and generate tickets automatically, **ensuring that potential security incidents are promptly recorded and addressed.**





## CompTIA Security+ 70 Course Notes

### Escalation

Automation in escalation involves using scripts or tools to **identify** high-priority incidents and **escalate** them to the appropriate team or individual.

This **ensures timely response to critical issues**, which is essential in maintaining security.



CompTIA Security+ 70 Course Notes

## Enabling/Disabling Services and Access

Automation can be used to control access to services and systems.

For instance, scripts can automatically disable access for users who no longer need it or enable access for new users, based on **predefined criteria or triggers**.





CompTIA Security+ 70 Course Notes

## Continuous Integration and Testing

In the development pipeline, automation is used for continuous integration and testing, where code changes are **automatically tested for security flaws** and other issues.

This **helps in early detection and remediation** of vulnerabilities, contributing to more secure software development.

```
000100111100001110110101011000101011010  
101001100101111110100000010100100010010  
111001110010010101010100101111010101  
1010100111111000001001010100101010101110  
000011111100101010101010101011110101010  
010100111111000001Error001010100101010101  
1010100110111110101010000101010101010101  
1010101011111010001001111000011110110101  
01001011110101010100000101111110100000010  
0100101010101110011100101010101010101010  
00110110110110101010011111000001001010
```



CompTIA Security+ 70 Course Notes

## Integrations and API

Automation often involves using APIs (Application Programming Interfaces) to integrate various security tools and systems.

This allows for seamless **data exchange and coordination between different components** of the security infrastructure, enhancing overall security posture.





CompTIA Security+ 70 Course Notes

## Benefits of Automation and Orchestration in Secure Operations

Automation and orchestration not only **enhance security** but also contribute to overall **operational efficiency** and effectiveness.

These benefits show how automation is not just a technical improvement but a **strategic enabler** for secure, efficient, and resilient IT operations.





CompTIA Security+ 70 Course Notes

## Efficiency/Time Saving

Automation significantly reduces the time required to perform repetitive or complex tasks.

By automating routine tasks such as patching, monitoring, and reporting, organizations can **free up valuable time** for their IT staff to focus on more strategic initiatives.





CompTIA Security+ 70 Course Notes

## Enforcing Baselines

Automation ensures that security baselines are consistently applied across all systems and applications.

This includes automatically configuring security settings, applying patches, and checking for compliance with security policies, **ensuring a uniform security posture across the organization.**





CompTIA Security+ 70 Course Notes

## Standard Infrastructure Configurations

Automation helps in maintaining standard configurations across the IT infrastructure.

This standardization **reduces the risk of configuration errors**, which can lead to security vulnerabilities, and ensures a predictable, secure environment.



CompTIA Security+ 70 Course Notes

## Scaling in a Secure Manner

Automation enables organizations to scale their IT operations securely.

It ensures that as the system grows, security measures are **consistently applied**, and changes are made **without introducing vulnerabilities**, maintaining security at scale.





CompTIA Security+ 70 Course Notes

## Employee Retention

Automation can lead to higher employee satisfaction and retention by **reducing the burden of repetitive and mundane tasks**.

Employees can focus on more challenging and rewarding work, leading to **better job satisfaction and reduced turnover**.





## CompTIA Security+ 70 Course Notes

### Reaction Time

In the event of a security incident, automation allows for a much **quicker response**.

Automated systems can detect and respond to threats in real-time, **reducing the window of opportunity** for attackers and mitigating potential damage.





CompTIA Security+ 70 Course Notes

## Workforce Multiplier

Automation acts as a force multiplier for the cybersecurity workforce.

With automation handling routine tasks, a smaller team can effectively manage a large and complex IT environment, **making the most of limited cybersecurity resources**.





## CompTIA Security+ 70 Course Notes

# Other Considerations

While automation and orchestration has many benefits, it could have the following draw issues:

- Complexity
- Cost
- Single point of failure
- Technical debt
- Ongoing supportability

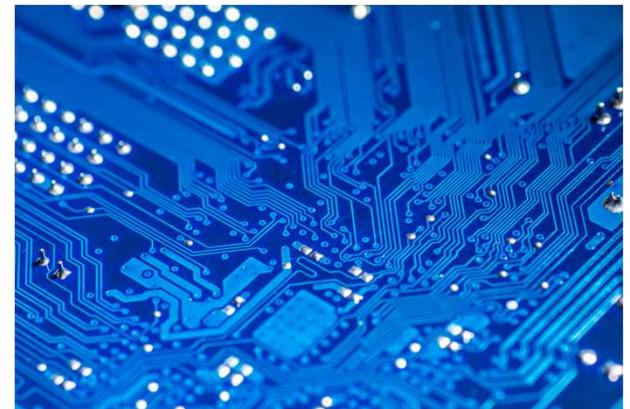


## Complexity

Automation can introduce complexity into IT environments.

While it simplifies certain tasks, setting up and maintaining automated workflows and orchestration tools **requires specialized knowledge**.

There's also the complexity of **integrating various tools and ensuring they work harmoniously**, which can be challenging.





## CompTIA Security+ 70 Course Notes

### Cost

Implementing automation solutions involves costs, including the initial investment in technology, training for staff, and ongoing maintenance expenses.

While automation can lead to **long-term savings and efficiencies**, the **upfront cost** can be significant and should be carefully considered.





## Single Point of Failure

Relying heavily on automated systems can create a single point of failure.

If an automation tool fails, it can impact multiple systems and processes.

Therefore, it's **essential to have redundancy** and failover mechanisms in place to mitigate this risk.





CompTIA Security+ 70 Course Notes

## Technical Debt

Automation can sometimes lead to technical debt if it's implemented without adequate planning or foresight.

Quick fixes and workarounds might solve immediate problems but **can create longer-term issues that are difficult and costly to resolve.**





## CompTIA Security+ 70 Course Notes

# Ongoing Supportability

Automated systems require ongoing support and maintenance.

This includes regular updates, monitoring for issues, and adjustments as organizational needs change.

**Ensuring that there is adequate support for these systems is crucial for their long-term viability.**



# Lesson 19 Incident response

---



## CompTIA Security+ 70 Course Notes

# Incident Response Process

**Security Incident:** an event that compromises the confidentiality, integrity, or availability of information assets.

**Security Incident Process:** process of handling a security incident typically involves several key steps, designed to effectively identify, manage, and mitigate the incident.

Steps:

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Lessons learned



## CompTIA Security+ 70 Course Notes

### Preparation

This is the **foundational** stage where organizations develop incident response plans, establish incident response teams, and set up necessary tools and communication channels.

Preparation includes training personnel, conducting regular security assessments, and ensuring that all necessary resources are in place to handle a security incident.





## CompTIA Security+ 70 Course Notes

### Detection

The detection phase involves **identifying potential security incidents**.

This can be achieved through various means such as network monitoring, intrusion detection systems, and regular security audits.

**Quick and accurate detection is crucial for an effective response.**





## CompTIA Security+ 70 Course Notes

### Analysis

Once a potential incident is detected, it must be analyzed to **understand its nature and scope**.

This involves determining the type of attack, the systems affected, the data compromised, and the attacker's tactics, techniques, and procedures (TTPs).

**Analysis is critical to inform the subsequent steps** in the incident response process.





CompTIA Security+ 70 Course Notes

## Containment

The containment phase aims to limit the scope and magnitude of the incident.

This can involve isolating affected systems, blocking malicious traffic, or temporarily shutting down certain services.

The goal is to **prevent further damage while maintaining critical operations**.



## CompTIA Security+ 70 Course Notes

### Eradication

After containing the incident, the next step is to eradicate the **root cause** of the incident.

This may involve removing malware, closing security gaps, restoring systems, and implementing patches.

The objective is to **eliminate the threat from the environment entirely**.



## CompTIA Security+ 70 Course Notes

### Recovery

In this phase, affected systems and services are **restored to normal operations**.

This includes ensuring that all systems are **cleaned and secure** before bringing them back online.

Recovery also involves **monitoring for any signs of recurrence or fallout** from the incident.





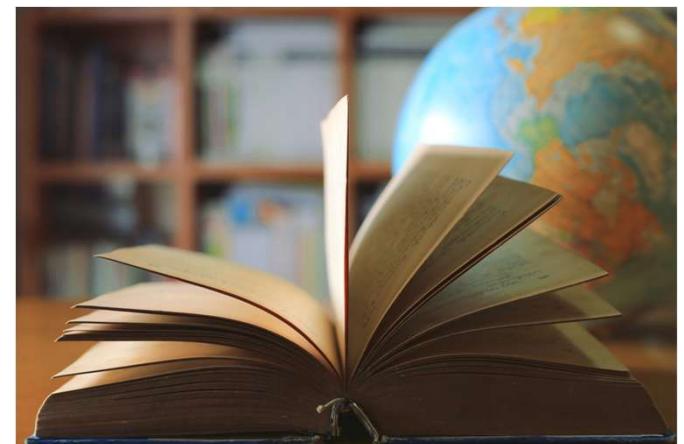
## CompTIA Security+ 70 Course Notes

# Lessons Learned

After the incident is resolved, it's important to conduct a post-incident review.

This involves analyzing what happened, how it was handled, and what could be done better in the future.

Lessons learned are documented and used to **improve the incident response plan and other security measures**.





CompTIA Security+ 70 Course Notes

## Training in Appropriate Incident Response Activities

Training focuses on the educational and skill-building aspects necessary for **preparing individuals** and teams to **effectively respond to cybersecurity incidents**.

Training is a crucial component of the incident response process, encompassing a range of topics and skills.



## CompTIA Security+ 70 Course Notes

### Testing

We will be exploring how organizations test their preparedness and response capabilities to handle cybersecurity incidents.

This testing is crucial for identifying gaps in incident response plans and improving the overall readiness of the response team.

The primary forms of testing in this context are tabletop exercises and simulations.





## CompTIA Security+ 70 Course Notes

# Tabletop Exercise

A tabletop exercise is a discussion-based session where team members walk through various incident scenarios in a structured manner.

It typically involves **key personnel from different departments** who would be involved in incident response.

Purpose: The primary goal of a tabletop exercise is to **assess the effectiveness of the incident response plan** and the team's understanding of their roles and responsibilities during an incident.

It also tests decision-making processes and inter-departmental coordination.



## CompTIA Security+ 70 Course Notes

### Simulation

Simulations are more hands-on and involve **creating a realistic cyber incident environment** where the response team can practice responding to an incident.

This often includes the use of real tools and systems in a controlled setting.

Purpose: The aim is to provide a **realistic experience of handling an incident**, testing both the technical and procedural aspects of the response plan.

Simulations can range from simple scripted scenarios to complex, multi-layered attacks.



CompTIA Security+ 70 Course Notes

## Root Cause Analysis

Involves exploring the systematic process used to identify the **underlying reasons** why a security incident occurred.

RCA is a critical component of incident response, as it **helps prevent future incidents** by addressing the core issues rather than just their symptoms.





## CompTIA Security+ 70 Course Notes

# Threat Hunting

Threat hunting involves exploring the proactive and iterative approach to **detecting and isolating advanced threats** that evade existing security solutions.

It is a crucial component of a robust cybersecurity strategy, particularly in **identifying and mitigating sophisticated cyber threats**.

It highlights a proactive approach to cybersecurity, emphasizing the need for ongoing vigilance, expertise, and advanced tools to identify and mitigate sophisticated cyber threats.





CompTIA Security+ 70 Course Notes

## Digital Forensics

Digital forensics involves **delving into the methodologies and principles applied in the investigation of cyber incidents**, specifically focusing on the identification, collection, examination, and preservation of digital evidence.

It underscores the need for meticulous and ethical handling of digital evidence to ensure its integrity, especially in situations where legal and regulatory factors are involved.





## CompTIA Security+ 70 Course Notes

### Legal Hold

Legal hold is a process in digital forensics where **potentially relevant data is preserved** for legal or investigative purposes.

This involves ensuring that such data is not altered, deleted, or destroyed during the course of an investigation, particularly if the data might be used in a legal proceeding.





CompTIA Security+ 70 Course Notes

## Chain of Custody

Chain of custody refers to the **documentation or paper trail** that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.

It's crucial in maintaining the integrity of the evidence, ensuring it remains admissible in court.

CHAIN OF CUSTODY	
Received from:	_____
By:	_____
Date:	_____ Time: _____ AM/PM
Received from:	_____
By:	_____
Date:	_____ Time: _____ AM/PM
Received from:	_____
By:	_____
Date:	_____ Time: _____ AM/PM
Received from:	_____
By:	_____
Date:	_____ Time: _____ AM/PM
Received from:	_____
By:	_____
Date:	_____ Time: _____ AM/PM
Received from:	_____
By:	_____
Date:	_____ Time: _____ AM/PM



## CompTIA Security+ 70 Course Notes

### Acquisition

Acquisition in digital forensics is the process of **collecting digital evidence** while ensuring that the data is not altered during the process.

This involves creating exact copies of hard drives, memory, or other storage media using specialized tools that ensure the original evidence remains unaltered.



## CompTIA Security+ 70 Course Notes

### Reporting

Reporting involves **documenting the findings** of the forensic investigation.

This includes detailing how the evidence was collected, analyzed, and preserved, as well as the conclusions drawn from the analysis.

**Clear, comprehensive, and precise reporting is essential**, especially if the findings are to be presented in legal contexts.



CompTIA Security+ 70 Course Notes

## Preservation

**Preservation** in digital forensics refers to the process of **protecting and maintaining the integrity of digital evidence**.

This involves storing the evidence in a secure environment and ensuring that it is protected from tampering, alteration, or degradation.





## CompTIA Security+ 70 Course Notes

### E-Discovery

Electronic discovery (e-discovery) is the process of identifying, collecting, and producing electronically stored information (ESI) **in response to a request for production in a legal case or investigation.**

E-discovery can include emails, documents, databases, audio, video files, and more, and involves processes that align with legal standards.

# Lesson 20 Supporting an investigation

---



## CompTIA Security+ 70 Course Notes

# Log Data

Log data is one of the primary data sources in an investigation.

We will be covering:

- Firewall logs
- Application logs
- Endpoint logs
- OS-specific security logs
- IPS/IDS logs
- Network logs
- Metadata



CompTIA Security+ 70 Course Notes

## Firewall Logs

Firewall logs record events related to the **network firewall**, including attempted and blocked connections, allowed traffic, and rule changes.

They are crucial for identifying unauthorized access attempts, potential breaches, and understanding traffic patterns that may indicate malicious activity.





CompTIA Security+ 70 Course Notes

## Application Logs

These logs provide **records of events from specific applications**.

They can include information about application performance, user activities, errors, and security events.

In cybersecurity, they are used to **detect anomalies in application behavior** or unauthorized access to applications.



CompTIA Security+ 70 Course Notes

## Endpoint Logs

Endpoint logs are generated by endpoint devices like laptops, desktops, and mobile devices.

They contain information about the **operations and activities on the device**, including system changes, user activities, and security events like antivirus alerts.

These logs are essential for detecting malware infections, unauthorized access, and other **security incidents at the endpoint level**.



CompTIA Security+ 70 Course Notes

## OS-specific Security Logs

OS security logs provide details about events specific to the **operating system**.

This includes user logon/logoff activities, system errors, policy changes, and security-related changes.

They are key to understanding activities **within the OS** that might indicate a security incident.



CompTIA Security+ 70 Course Notes

## IPS/IDS Logs

Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) logs record information about **network traffic** and potential security threats.

These logs are used to identify suspicious activities, policy violations, and attempted or successful breaches of the **network security**.





CompTIA Security+ 70 Course Notes

## Network Logs

Network logs record data about the activities **within a network**, including traffic flow, device connectivity, and network errors.

They are essential for understanding the **baseline network activity** and identifying deviations that might suggest a security issue.



## CompTIA Security+ 70 Course Notes

### Metadata

**Metadata refers to data that provides information about other data.**

In the context of cybersecurity, this can include details about file creation and modification, sender/recipient information in emails, and location data.

**Metadata can be used to trace activities and establish patterns relevant to an investigation.**



## Data Sources

Data sources provide crucial insights and evidence for understanding the nature of security incidents, their impact, and methods for remediation.

Logs can be obtained from:

- Vulnerability scans
- Automated reports
- Dashboards
- Packet captures



## CompTIA Security+ 70 Course Notes

# Vulnerability Scans

Vulnerability scans are **automated** tools that assess systems, networks, and applications for security weaknesses.

The data from these scans include details about identified vulnerabilities, their severity, and potential impact.

This information is critical for understanding **attack vectors** and potential **entry points** for attackers.





## CompTIA Security+ 70 Course Notes

# Automated Reports

Automated reports are generated by various security tools and systems.

They can include summaries of security events, incidents, and trends observed over a certain period.

These reports are useful for gaining a **high-level overview** of the security posture and **identifying patterns** or anomalies that may require further investigation.



## CompTIA Security+ 70 Course Notes

# Dashboards

Dashboards provide a **real-time** view of an organization's security status, **aggregating data** from multiple sources into a single interface.

They typically display key metrics, alerts, and the status of different systems and defenses.

Dashboards are essential for **ongoing monitoring** and **quick detection** of issues as they arise.





CompTIA Security+ 70 Course Notes

## Packet Captures

Packet captures involve **recording network traffic** and analyzing the packets that travel across the network.

This data source is invaluable for **understanding the nature of network-based attacks**, investigating data exfiltration, and analyzing communication between compromised systems and attackers' command and control servers.

# Lesson 20 5.1

---



CompTIA Security+ 70 Course Notes

## Security Governance

**Security Governance** is the collection of practices related to supporting, evaluating, defining, and directing the security efforts of an organization.

- Establish and sustain a **culture of security** in the organization's conduct
- Establish and maintain a **framework to provide assurance** that information security strategies are aligned with business objectives
- Assure that information security is consistent with applicable **laws and regulations**
- Assess **emerging threats** and provide strong **cyber security leadership**



## CompTIA Security+ 70 Course Notes

# Policies

Policies are a crucial component of security governance, providing a framework for consistent and secure operations across the organization.

They form the foundation for how an organization secures its assets, responds to incidents, and ensures continuity of operations.

Effective security governance relies on the development, implementation, and enforcement of these policies to **create a secure and resilient organizational environment**.

Polices should be develop using a **top-down approach**.

- Senior Management supports the policies and their creation.



## CompTIA Security+ 70 Course Notes

# Acceptable Use Policy

An AUP defines the **acceptable ways** in which network, systems, and information can be **used by employees** and other users.

It typically covers the use of organizational resources, internet usage, email, and social media guidelines.

The aim is to **protect** both the organization's **resources and its data** from misuse or malicious activities.



CompTIA Security+ 70 Course Notes

## Information Security Policies

These policies encompass a broad range of guidelines designed to protect the **confidentiality, integrity, and availability of information**.

They cover aspects like data classification, access controls, cryptography, and physical security.

Information security policies are foundational to an organization's overall cybersecurity strategy.



CompTIA Security+ 70 Course Notes

## Business Continuity Policy

Business continuity policies outline procedures and instructions an organization must follow in the face of **major disruptions or disasters**.

This includes **maintaining essential functions and services** during and after a major disruption, such as a natural disaster or a significant cyber attack.



CompTIA Security+ 70 Course Notes

## Disaster Recovery Policy

The disaster recovery policy focuses on **restoring IT systems, data, and infrastructure** to operational status after a disaster.

It includes **detailed plans** on data backups, system recovery processes, and roles and responsibilities during the recovery process.





CompTIA Security+ 70 Course Notes

## Incident Response Policy

This policy provides a structured approach for managing security incidents and breaches.

It defines roles, responsibilities, processes, and communication strategies to be employed during and after an incident.

An effective incident response policy is crucial for minimizing the impact of security incidents.



CompTIA Security+ 70 Course Notes

## Software Development Lifecycle Policy

SDLC policies govern the processes involved in **developing, deploying, and maintaining software**.

These policies ensure that security is **integrated into each stage** of the software development process, from initial design to deployment and maintenance.





CompTIA Security+ 70 Course Notes

## Change Management Policy

Change management policies are critical for ensuring that changes to IT systems and environments are made in a **controlled and secure manner**.

This includes evaluating, approving, and documenting changes to prevent **unauthorized modifications** that could compromise security.



CompTIA Security+ 70 Course Notes

## Standards

Standards are established benchmarks or sets of criteria against which security measures are designed and evaluated.

They guide organizations in implementing organization policies.



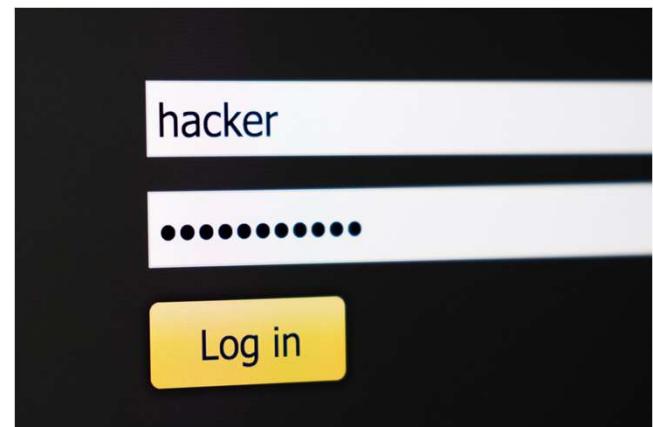


## CompTIA Security+ 70 Course Notes

# Password Standards

Password standards define the **criteria for creating and managing passwords**.

This includes requirements for password complexity (such as length, use of numbers, uppercase and lowercase letters, and special characters), frequency of password changes, and guidelines for storing and transmitting passwords securely.





CompTIA Security+ 70 Course Notes

## Access Control Standards

These standards specify **how access to information systems and data should be controlled and managed**.

They include guidelines for user authentication, authorization levels, role-based access control, and the principle of least privilege.

These standards ensure that users have access **only to the resources necessary** for their roles.





CompTIA Security+ 70 Course Notes

## Physical Security Standards

Physical security standards address the protection of hardware, software, networks, and data from **physical actions and events** that could cause serious loss or damage.

This includes securing facilities, controlling physical access to sensitive areas, and protecting against environmental hazards.





CompTIA Security+ 70 Course Notes

## Encryption Standards

Encryption standards outline the **requirements for encrypting data**, both at rest and in transit.

They cover the use of encryption algorithms, key management, and the implementation of encryption protocols.

These standards are crucial for protecting the confidentiality and integrity of data.



CompTIA Security+ 70 Course Notes

## Guidelines

Guidelines in cybersecurity governance are essentially sets of **recommendations and best practices** that help shape an organization's security posture and decision-making.

They provide the roadmap for organizations to develop, implement, and maintain robust security practices that align with their **business objectives** and **risk tolerance levels**.





## CompTIA Security+ 70 Course Notes

# Procedures

Procedures in cybersecurity governance are detailed, operational-level instructions that guide the day-to-day activities of maintaining security.

They represent the **actionable steps-by-steps** that operationalize security policies and standards, ensuring that security governance is effectively implemented and maintained throughout the organization.





CompTIA Security+ 70 Course Notes

## Change Management Procedures

Change management procedures are critical for ensuring that all changes to IT systems, software, and infrastructure are made in a **controlled, systematic manner**.

This includes steps for requesting, reviewing, approving, implementing, and documenting changes.

The goal is to **minimize the risk of unintended service disruptions and security vulnerabilities**.



CompTIA Security+ 70 Course Notes

## Onboarding/Offboarding Procedures

Onboarding procedures involve steps for integrating new employees into the organization securely.

This includes granting access to systems and networks, providing necessary training, and ensuring compliance with security policies.

Offboarding procedures are equally important.

They ensure that when employees leave the organization, their **access to systems and data is revoked**, and any **sensitive information they handled is secured**.



## CompTIA Security+ 70 Course Notes

# Playbooks

Security playbooks are sets of procedures that detail the steps to be taken in response to specific security incidents or scenarios.

They provide a predefined set of actions to follow, ensuring a consistent and effective response to incidents.

Playbooks can cover a range of scenarios, from responding to a data breach to mitigating a DDoS attack.





## CompTIA Security+ 70 Course Notes

# External Considerations

These considerations shape and often mandate certain aspects of security governance, making them critical components of an organization's overall cybersecurity strategy.

They highlight the need for organizations to be aware of and compliant with a **diverse range of external factors**, from legal and regulatory to technological and societal, which collectively shape effective security governance.



## CompTIA Security+ 70 Course Notes

# National Regulatory and Legal Considerations

Organizations must comply with various **industry-specific and general data protection regulations**.

- Examples include GDPR (General Data Protection Regulation) in Europe, HIPAA (Health Insurance Portability and Accountability Act) in the healthcare sector in the U.S., and PCI DSS (Payment Card Industry Data Security Standard) for handling credit card transactions.

**These regulations often dictate specific security measures and processes.**



## CompTIA Security+ 70 Course Notes

# Local/Regional Considerations

Local and regional regulations and laws can also affect an organization's security governance.

This includes state or regional data protection laws and regulations, which may **vary significantly from one jurisdiction to another.**



## CompTIA Security+ 70 Course Notes

# Global Considerations

For organizations operating internationally, global cybersecurity considerations are critical.

This includes understanding and complying with the cybersecurity **laws and regulations** of all the countries in which they operate.

Global considerations also involve dealing with **cross-border data transfers** and **multinational regulatory compliance**.





## CompTIA Security+ 70 Course Notes

# Industry Considerations

Different industries often have **unique cybersecurity challenges and standards**.

For example, the financial sector might have stringent requirements for data encryption and transaction security, while the healthcare sector has to ensure the confidentiality and integrity of patient records.

Understanding industry-specific security requirements is crucial.



CompTIA Security+ 70 Course Notes

## Monitoring and Revision

Monitoring and revision involves understanding the **ongoing processes** of overseeing security operations and making **necessary adjustments** to enhance and maintain the security posture.

Effective governance requires not only the implementation of robust security measures but also their **ongoing evaluation** and **adaptation** to meet the changing security landscape and organizational needs.





CompTIA Security+ 70 Course Notes

## Types of Governance Structures

Various governance structures can be employed, each with its own advantages and challenges.

We will be covering:

- Boards
- Committees
- Government Entities
- Centralized Governance
- Decentralized Governance



## CompTIA Security+ 70 Course Notes

# Boards

In many organizations, a board of directors or a similar governing body has the ultimate responsibility for cybersecurity governance.

The board **sets the tone at the top**, establishes **strategic priorities**, and ensures that cybersecurity risks are adequately considered in the organization's **overall risk management**.





## CompTIA Security+ 70 Course Notes

### Committees

Cybersecurity committees, often comprised of **cross-functional** members from various departments, are tasked with specific governance roles.

These may include a Cybersecurity Steering Committee, an IT Risk Committee, or a Data Privacy Committee.

Committees typically have more **specialized focus areas** and are responsible for overseeing the implementation of policies, compliance, and risk management strategies.



## CompTIA Security+ 70 Course Notes

# Government Entities

At a **broader** level, government entities and regulatory bodies play a crucial role in cybersecurity governance, especially in defining legal and regulatory frameworks.

These entities set standards and regulations that **organizations must comply** with, such as GDPR in the European Union or the Cybersecurity Framework by NIST in the United States.





## Centralized Governance

In a centralized governance structure, cybersecurity policies and decision-making are consolidated within a **central entity or group within the organization**.

This is usually under the leadership of roles like a Chief Information Security Officer (CISO) or IT Director.

Centralized governance allows for **uniform policy enforcement** and **streamlined decision-making** but may lack the flexibility or specific focus of decentralized systems.



CompTIA Security+ 70 Course Notes

## Decentralized Governance

In a decentralized approach, cybersecurity governance responsibilities are **distributed across various departments** or units within the organization.

This approach can offer **greater specialization** and alignment with specific business needs but may **face challenges in ensuring consistent policy implementation and coordination**.



CompTIA Security+ 70 Course Notes

## Roles and Responsibilities for Systems and Data

Each role has specific duties and responsibilities regarding the protection of information assets.

We will be covering:

- Owners
- Custodians/Stewards
- Controllers
- Processors



## CompTIA Security+ 70 Course Notes

### Owners

Owners are typically **senior management** members or **department heads** who have overall accountability for specific information assets.

They are responsible for ensuring that proper controls are in place to protect the data and for making strategic decisions regarding the data's use, security, and handling.

Owners **define the classification of the data** and approve access controls.



CompTIA Security+ 70 Course Notes

## Custodians/Stewards

Custodians or data stewards are responsible for the **technical management and protection of data**.

They implement and maintain security measures, manage access controls, and ensure the proper operation of systems that store or process the data.

Custodians handle the day-to-day management of data, ensuring its integrity, availability, and confidentiality.



## CompTIA Security+ 70 Course Notes

# Controllers

In the context of data protection regulations like GDPR, controllers are entities that determine the purposes and means of processing personal data.

They are responsible for **making decisions** about data processing activities and ensuring compliance with applicable data protection laws.

Controllers must **implement measures to protect data** and are usually the **primary point of contact** for legal and compliance issues related to the data.



## CompTIA Security+ 70 Course Notes

### Processors

Processors are entities that **process data** on behalf of the controller.

In a cybersecurity context, they might be third-party service providers or internal departments that **handle data as directed by the controller**.

Their responsibilities include **processing data securely** as per the controller's instructions and ensuring that their activities **comply** with the relevant data protection laws and organizational policies.

# Lesson 21 5.2

---



## CompTIA Security+ 70 Course Notes

### Risk

The probability of a threat exploiting a vulnerability

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



## CompTIA Security+ 70 Course Notes

# Risk

### **Asset**

- Anything within an environment that should be protected.

### **Asset Valuation**

- A dollar value assigned to an asset based on actual cost and nonmonetary expenses.

### **Threats**

- Any potential occurrence that may harm the asset.

### **Threat Agent / Actors**

- People, programs, hardware, or systems that use threats to cause harm

### **Threat Events**

- Threat events are occurrences that lead to the exploitations of vulnerabilities.

### **Threat Vector**

- A threat vector or attack vector is the path or means by which an attack or attacker can gain access to a target in order to cause harm



## CompTIA Security+ 70 Course Notes

# Risk

### **Vulnerabilities**

- The weakness in an asset or the absence or the weakness of a safeguard or countermeasure that could be exploited.

### **Exposure**

- Actual or anticipated damage from a threat.

### **Safeguards**

- Anything that removes or reduces a risk

### **Attack**

- The threat exploiting the vulnerability

### **Breach**

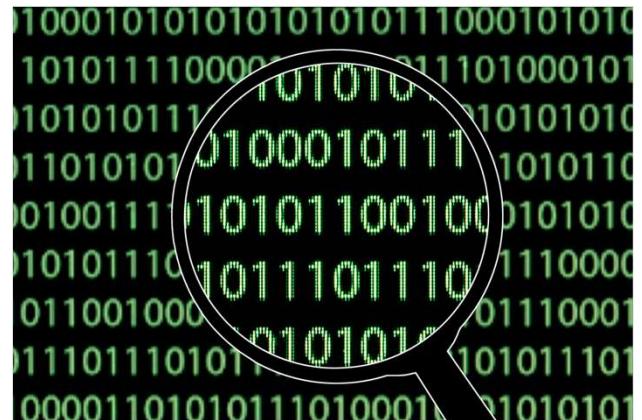
- The occurrence of a security mechanism being bypassed or thwarted by a threat agent.



## Risk Identification

Risk Identification involves understanding the **initial phase** of the risk management process where potential security risks are **recognized** and **described**.

This stage is critical for establishing a baseline from which risk analysis, assessment, and mitigation strategies are developed.





CompTIA Security+ 70 Course Notes

## Ad Hoc Risk Assessment

Ad hoc risk assessments are performed as needed, often **in response** to specific events or changes in the environment.

For example, an ad hoc assessment might be conducted after a major security breach in the industry or the release of a new threat.

These assessments are useful for addressing **immediate and emerging risks**.





CompTIA Security+ 70 Course Notes

## Recurring Risk Assessment

This type of risk assessment is conducted at **regular intervals**, such as quarterly or annually.

Recurring risk assessments are part of a **systematic** approach to risk management and ensure that changes in the organization's environment, assets, and threat landscape are **consistently accounted for and addressed**.



CompTIA Security+ 70 Course Notes

## One-Time Risk Assessment

One-time risk assessments are conducted for **specific scenarios**, such as before launching a new product, implementing a new IT system, or entering a new market.

They are **focused** and are typically not repeated unless there are significant changes to the initial conditions.



CompTIA Security+ 70 Course Notes

## Continuous Risk Assessment

Continuous risk assessment involves **ongoing monitoring and analysis** of the risk landscape.

This approach uses **real-time data** and **automated tools** to constantly evaluate risk levels.

Continuous assessments are becoming **increasingly important** and feasible due to advancements in technology and the **dynamic nature** of cyber threats.



## CompTIA Security+ 70 Course Notes

# Quantitative Risk Analysis

**Quantitative** risk assessment comes into play when we can map a monetary amount to an identified risk.

**Asset Value (AV)**: Dollar value of an asset

**Exposure Factor (EF)**: The percentage of loss that an org would experience if a specific asset were violated

**Single Loss Expectancy (SLE)**: Cost associated with a single realized risk against a specific asset

$$\circ \text{ SLE} = \text{AV} * \text{EF}$$

**Annualized Rate of Occurrence (ARO)**: The expected frequency with which a specific threat or risk will occur within a single year

**Annualized Loss Expectancy (ALE)**: The possible yearly cost of all instances of a specific realized threat against a specific asset

$$\circ \text{ ALE} = \text{SLE} * \text{ARO} \text{ or } \text{AV} * \text{EF} * \text{ARO}$$

**Annual Cost of Safeguard (ACS)**: The cost of safeguard should be lower than ALE to a worthwhile investment

$$\circ \text{ Value} = \text{ALE before safeguard} - \text{ALE after safeguard} - \text{ACS}$$



## CompTIA Security+ 70 Course Notes

# Qualitative Risk Analysis

**Qualitative risk analysis** involves assessing risks based on subjective criteria, such as expert opinions, scenario analysis, and industry best practices.

It typically categorizes risks into levels such as low, medium, or high based on their perceived severity and likelihood.

This approach is useful for understanding the general magnitude of risks when precise data is not available.



CompTIA Security+ 70 Course Notes

# Risk Register

A risk register is an essential component of effective risk management, serving as a **centralized repository** for information about

- identified risks
  - their assessment
  - and actions taken to mitigate them

SIMPLE SAFETY RISK REGISTER TEMPLATE

RISK DESCRIPTION	IMPACT DESCRIPTION	IMPACT LEVEL	PROBABILITY LEVEL	PRIORITY LEVEL	MITIGATION NOTES	OWNER
Brief summary of the risk.	What will happen if the risk is not mitigated or eliminated.	Rate 1 (LOW) to 5 (HIGH)	Rate 1 (LOW) to 5 (HIGH)	(IMPACT X PROBABILITY) Additive, highest first.	What can be done to lower or eliminate the impact or probability.	Who's responsible?
Leaks from roof during rain make the floor slippery	Slips and falls	3	5	15	- Order 'slippery when wet' signs - Have mops on hand - Fix roof	Allen
Shortage of eye protection	Increase in injuries Production delayed Increased Insurance premiums	5	1	5	- Increase supply - Low inventory warnings - Find alternative suppliers	Linda
		4	5	20		
		5	5	25		
		2	1	2		
		3	4	12		
		1	1	1		
		2	4	8		
		4	4	16		

<https://www.smartsheet.com/risk-register-templates>



# **Technical Institute of America**



## CompTIA Security+ 70 Course Notes

# Description of Risks

The risk register begins with a detailed description of each identified risk.

This includes:

- the **nature** of the risk
- the assets or **areas affected**
- and the potential **consequences** if the risk were to materialize.



## Key Risk Indicators (KRI)

KRIs are metrics used to measure and monitor the **likelihood and impact of risks**.

They provide **early warning signs** that a risk may be increasing or decreasing in severity.

For example, a high number of failed login attempts might be a KRI for **unauthorized access risks**.





## CompTIA Security+ 70 Course Notes

### Risk Owners

Each risk is assigned a risk owner, who is **responsible** for managing and mitigating that specific risk.

The risk owner is typically someone in a **management role** who has the **authority** and **knowledge** to implement risk responses.



## CompTIA Security+ 70 Course Notes

# Risk Threshold

Risk threshold refers to the **level of risk** that the organization is willing to **accept**.

Risks that fall **below** the threshold might be accepted or monitored, while those **above** it will require active mitigation.



## Risk Appetite

Risk appetite refers to the **risk** that an organization is prepared to pursue, retain, or take in its operations.

It reflects the organization's attitude towards risk and is shaped by factors like

- organizational culture
- business goals
- market conditions
- and regulatory environment

Risk tolerance is the amount of risk the organization is willing to take.



CompTIA Security+ 70 Course Notes

## Expansionary Risk Appetite

An expansionary risk appetite indicates a willingness to take on **higher levels of risk** in pursuit of **greater rewards**.

Organizations with an expansionary appetite are often in **growth phases**, seeking **competitive advantage** and willing to invest in opportunities that may carry higher risk, including **adopting new and potentially less tested technologies**.



CompTIA Security+ 70 Course Notes

## Conservative Risk Appetite

A conservative risk appetite implies a preference for lower risk and a focus on **stability and predictability**.

Organizations with a conservative appetite prioritize **protecting assets** and **minimizing potential losses** over seeking out high-risk opportunities.

They tend to invest heavily in **robust** cybersecurity measures and may be **cautious** in adopting new technologies.



## CompTIA Security+ 70 Course Notes

# Neutral Risk Appetite

A neutral risk appetite strikes a balance between expansionary and conservative approaches.

Organizations with a neutral appetite are willing to **accept some level of risk** for reasonable returns but are not inclined to pursue high-risk opportunities.

Their cybersecurity strategies aim to **balance** risk mitigation with the pursuit of business objectives.





CompTIA Security+ 70 Course Notes

## Risk Management Strategies

Risk Management Strategies refer to the **systematic approach** an organization takes to handle potential risks associated with its information systems and data.

These strategies are designed to **minimize the impact of risks** on organizational operations and objectives.

In cybersecurity, risk management strategies are particularly important due to the **evolving nature of threats** and the **critical importance** of protecting digital assets.



## Risk Avoidance

Avoiding risk involves **changing plans or procedures** to eliminate the risk or to remove the organization's exposure to it.

This might mean **not implementing** a certain system or technology that introduces high risk.





## Risk Mitigation

Mitigation refers to taking steps to **reduce the likelihood or impact** of a risk.

In cybersecurity, this often involves

- implementing security controls,
- updating software,
- improving user training,
- and enhancing monitoring and detection capabilities.



## CompTIA Security+ 70 Course Notes

### Risk Transfer

Transferring risk means **shifting the impact** of a risk to a third party.

This is often done through insurance policies, where a company transfers the **financial risk** to an insurance provider, or through outsourcing, where certain IT services or processes are **managed by external vendors**.



## Risk Acceptance

Accepting risk is a **conscious decision** to not take any action against a particular risk.

This strategy is chosen when the cost of mitigating the risk is **greater** than the potential loss from the risk itself, or when the likelihood of the risk materializing is **acceptably low**.

Exemption: Sometimes, specific risks might be exempted from mitigation due to their **nature** or the **context** in which they exist.

Exception: In some cases, an exception might be made for a risk, **usually temporarily**, until it can be **properly addressed** at a later time.



## Risk Exploitation

Exploiting a risk involves **taking advantage of the potential positive impacts** of a risk.

While this is **less common in cybersecurity**, it could involve leveraging a risky technological innovation that could place the organization at a **competitive advantage**.



CompTIA Security+ 70 Course Notes

## Risk Reporting

Risk Reporting involves understanding the process of **communicating information** about identified risks, their analysis, and mitigation strategies to relevant stakeholders.

Risk reporting is a crucial element in cybersecurity risk management as it ensures transparency, informs decision-making, and aids in the **ongoing management** of cybersecurity risks.



CompTIA Security+ 70 Course Notes

## Business Impact Analysis

BIA is a fundamental component in cybersecurity and business continuity planning, as it helps in **identifying** and **evaluating** the potential effects of **interruptions to critical business operations**.

BIA is a **proactive** measure that aids in crafting effective business **continuity and disaster recovery strategies**, ensuring business resilience in the face of cyber threats.



## CompTIA Security+ 70 Course Notes

# Recovery Time

### **Maximum Tolerable Downtime (MTD):**

Defines the amount of time a business function can be inoperable without causing irreparable harm to the business. Also known as the Maximum Tolerable Outage (MTO)

**Recovery Time Objective (RTO):** Amount of time to recover the function in the event of a disaster

**Recovery Point Objective (RPO):** Defines the point in time before the data loss during the outage will leave the business function unrecoverable.

**RTO should be less than MTD**



## Failure Time

### Mean Time to Repair

- MTTR is the average time taken to repair a failed component, system, or function and **return it to operational status**.

### Mean Time Between Failures

- MTBF is a measure of the reliability and stability of IT systems, indicating the **average time between inherent failures of a system** or component in normal operating conditions.

22 5.3

---



## CompTIA Security+ 70 Course Notes

# Vendor Assessment

Vendor assessment in a cybersecurity context is the process of **evaluating** and monitoring the **security risks** associated with **third-party service providers** or suppliers.

It involves **scrutinizing the vendor's cybersecurity practices, policies, and compliance** with relevant standards through methods such as penetration testing, reviewing audit reports, and assessing their data handling and privacy measures.

The goal is to ensure that the vendor's **security posture aligns with the organization's security requirements** and risk management strategies, minimizing potential risks to data and systems.



## CompTIA Security+ 70 Course Notes

# Penetration Testing

Penetration testing involves **simulating cyberattacks** against a vendor's systems to assess the security of their systems and services.

This is particularly important for vendors handling **sensitive data** or providing **critical IT services**.

Results from penetration testing can **reveal vulnerabilities** that might pose a risk to the contracting organization.



## CompTIA Security+ 70 Course Notes

# Right-to-Audit Clause

A right-to-audit clause in vendor contracts grants the organization the **right to conduct**, or have conducted on its behalf, an audit of the vendor's security practices.

This can include reviewing

- security policies
- control mechanisms
- and compliance with agreed-upon security standards





CompTIA Security+ 70 Course Notes

## Evidence of Internal Audits

Vendors should provide evidence of regular internal audits of their security processes and controls.

This evidence can include

- audit reports
- summaries of findings
- and documentation of remedial actions taken in response to audit findings



CompTIA Security+ 70 Course Notes

## Independent Assessments

Independent assessments by third parties, such as security certifications (e.g., ISO 27001, SOC 2 Type II), provide an **objective evaluation** of the vendor's security posture.

These assessments are crucial for **verifying that the vendor adheres to industry best practices and standards** in cybersecurity.



CompTIA Security+ 70 Course Notes

## Supply Chain Analysis

This involves **examining the security** of the vendor's supply chain, as vulnerabilities in the supply chain can directly impact the security of the products or services they provide.

This analysis should **assess the security practices** of not only the primary vendor but also their subcontractors and suppliers.





CompTIA Security+ 70 Course Notes

## Questionnaires

Questionnaires are a critical tool used for **gathering essential information** about a vendor's security practices, policies, and compliance status.

These questionnaires are an integral part of the vendor evaluation and monitoring process, allowing organizations to **assess the cybersecurity risks associated with third-party service providers**.





CompTIA Security+ 70 Course Notes

## Rules of Engagement

Rules of Engagement refer to the set of guidelines or protocols that outline **how an organization interacts and cooperates with third-party vendors**, especially regarding cybersecurity matters.

These rules are crucial for establishing clear expectations, responsibilities, and boundaries in the relationship between an organization and its external partners.



CompTIA Security+ 70 Course Notes

## Vendor Selection

Vendor selection is the process of **evaluating and choosing** third-party service providers based on their **ability to meet specified cybersecurity standards** and requirements.



## CompTIA Security+ 70 Course Notes

# Due Diligence

Due diligence is a **comprehensive appraisal** of a vendor's business practices, focusing on their cybersecurity policies, procedures, and controls.

It includes assessing the vendor's security measures, **compliance** with industry standards (like ISO 27001, SOC 2), and **past performance** or reputation in terms of handling cybersecurity risks.

Due diligence aims to **uncover any potential security vulnerabilities** or weaknesses in the vendor's offerings.



## CompTIA Security+ 70 Course Notes

# Conflict of Interest

Identifying and managing any potential conflicts of interest is crucial in vendor selection.

A conflict of interest may arise when a vendor has **competing interests** that could influence their ability to **objectively** and **securely** provide services.

Ensuring **transparency** and **impartiality** in the selection process is key to avoiding biases or decisions that could compromise security.





## CompTIA Security+ 70 Course Notes

### Vendor Monitoring

Vendor Monitoring is the continuous process of **assessing and overseeing third-party vendors** to ensure they comply with established security standards and contractual agreements.

This involves **regular evaluations** of the vendor's security practices, incident response capabilities, and adherence to relevant regulatory and industry compliance standards.

The objective is to **proactively identify and mitigate potential security risks** that vendors may pose to an organization's information systems and data.



## Contractual Agreements

The selection process must consider how well the vendor's contractual terms (Service Level Agreements, or SLAs) align with the organization's security expectations.

This includes provisions for

- data protection,
- incident response,
- regular security audits,
- and the right-to-audit clauses.



CompTIA Security+ 70 Course Notes

## Service-Level Agreement

An SLA is a contract between a service provider and a client that specifies the level of service expected during the term of the agreement.

In cybersecurity, this includes aspects like **system uptime**, **response times** for support requests, and **security measures**.

SLAs are crucial for establishing **performance benchmarks** and **consequences** for not meeting agreed standards.





CompTIA Security+ 70 Course Notes

## Memorandum of Agreement

An MOA is a formal document outlining an **agreement between two or more parties**.

It's often used to **establish cooperative relationships**, detailing the terms and scope of the arrangement.

In cybersecurity, an MOA can set out joint initiatives for **information sharing, collaborative development** of security protocols, etc.



CompTIA Security+ 70 Course Notes

## Memorandum of Understanding

An MOU is **less formal** than an MOA and is typically used to outline a mutual agreement on a shared goal or project, **without legal obligations**.

In cybersecurity, MOUs can **facilitate partnerships** for information sharing, research collaborations, or joint responses to security incidents.



CompTIA Security+ 70 Course Notes

## Master Service Agreement

An MSA is a **comprehensive contract** that sets the general terms governing future transactions or agreements.

It can **streamline future agreements** and often includes clauses on confidentiality, dispute resolution, and data security standards.





CompTIA Security+ 70 Course Notes

## Work Order/ Statement of Work

A WO or SOW is a **document that provides specific details about the work to be performed under a contract.**

It outlines the

- deliverables
- timelines
- specific tasks
- and responsibilities

In cybersecurity, this could detail specific security projects, audits, or implementation of security solutions.



CompTIA Security+ 70 Course Notes

## Non-disclosure Agreement

An NDA is a **legally binding contract** that establishes a confidential relationship.

Parties agree **not to disclose information covered by the agreement**, which is crucial in protecting sensitive data, proprietary methodologies, and security practices.





CompTIA Security+ 70 Course Notes

## Business Partners Agreement

A BPA outlines the terms and conditions of the relationship between business partners.

In a cybersecurity context, it can specify roles, responsibilities, and security requirements when **sharing resources, joint ventures, or collaborative projects**.

23 5.4

---



CompTIA Security+ 70 Course Notes

## Compliance Reporting

Compliance reporting refers to the process of **documenting and conveying an organization's adherence** to various cybersecurity regulations, standards, and internal policies.



CompTIA Security+ 70 Course Notes

## Internal Compliance Reporting

Internal reporting involves generating reports for use **within the organization**, typically for management, internal audit teams, or IT security departments.

They serve as a tool for self-evaluation, helping to **identify areas of improvement** and ensure that internal security practices align with the organization's cybersecurity objectives.



CompTIA Security+ 70 Course Notes

## External Compliance Reporting

External reporting is prepared for outside entities, such as regulatory bodies, clients, or third-party auditors.

This type of reporting demonstrates compliance with external cybersecurity standards (like ISO/IEC 27001, NIST, GDPR, HIPAA) and any industry-specific regulations.

External reports might be required **periodically or in response to specific compliance audits**, and are crucial for maintaining legal and regulatory compliance, as well as for building trust with clients and partners.



## CompTIA Security+ 70 Course Notes

# Consequences of Non-Compliance

Consequences of non-compliance refers to the adverse effects an organization faces when it fails to adhere to relevant cybersecurity laws, regulations, standards, or contractual obligations.

We will be covering:

- Fines
- Sanctions
- Reputational damage
- Loss of license
- Contractual impacts
- Operational Disruptions
- Increased Scrutiny and Ongoing Monitoring
- Market and Competitive Disadvantages



## CompTIA Security+ 70 Course Notes

### Fines

**Non-compliance with cybersecurity regulations and standards can result in **substantial financial penalties**.**

Regulatory bodies across various jurisdictions can impose fines, which can be **particularly hefty in cases of severe breaches** or non-compliance with major regulations like GDPR, HIPAA, or PCI DSS.



## CompTIA Security+ 70 Course Notes

# Sanctions

Sanctions are formal penalties or restrictions imposed by regulatory authorities or governing bodies.

These can include

- **restrictions** on business operations
- **suspension of certain activities**
- or even **legal actions** against the organization or its executives





CompTIA Security+ 70 Course Notes

## Reputational Damage

Non-compliance can lead to significant reputational damage.

The public disclosure of a compliance failure, especially those that compromise customer data, can **erode trust and confidence among clients, partners, and the public**, potentially leading to loss of business and damaged stakeholder relationships.



## CompTIA Security+ 70 Course Notes

### Loss of License

In some industries, continual non-compliance can result in the revocation of licenses or certifications necessary to operate legally.

This is **particularly relevant in heavily regulated sectors** like finance, healthcare, or legal services.



## CompTIA Security+ 70 Course Notes

# Contractual Impacts

Failure to comply with cybersecurity clauses in contracts can lead to contractual breaches, resulting in

- legal disputes,
- termination of contracts,
- or financial liabilities.

This is especially significant in B2B relationships where **cybersecurity compliance is a key contractual requirement.**





CompTIA Security+ 70 Course Notes

## Compliance Monitoring

**Compliance Monitoring** refers to the **ongoing process** of ensuring that an organization **consistently meets the required standards and regulations for cybersecurity**.

This process is vital for maintaining security integrity and **avoiding the negative consequences of non-compliance**.





## CompTIA Security+ 70 Course Notes

# Due Diligence/Care

Due diligence in compliance monitoring involves the **continuous effort** to ensure that all cybersecurity practices, policies, and controls are **in line with the latest legal and regulatory requirements**.

Due care refers to the **ongoing management and upkeep of these practices**, demonstrating that the organization is actively maintaining its cybersecurity posture.



CompTIA Security+ 70 Course Notes

## Attestation and Acknowledgement

Attestation involves **formal verification**, confirming that an organization's **cybersecurity controls meet certain standards or regulations**.

Acknowledgement typically refers to the organization's **recognition and acceptance of its cybersecurity responsibilities**, often documented through policies or agreements.



CompTIA Security+ 70 Course Notes

## Internal and External Monitoring

Internal monitoring consists of **activities conducted within the organization to ensure compliance**, such as regular audits, reviews, and assessments of security policies and controls.

External monitoring may involve **assessments or audits by external parties**, regulatory compliance checks, or industry certification processes.



CompTIA Security+ 70 Course Notes

## Automation

Automation in compliance monitoring includes the use of software tools and technologies to **continuously monitor compliance status**.

Automated systems can **track changes** in regulatory requirements, monitor security controls in real-time, and **provide alerts** when potential non-compliance issues are detected.





## CompTIA Security+ 70 Course Notes

### Privacy

**Privacy** refers to the **practices, policies, and legal requirements surrounding the protection of personal and sensitive data.**

Privacy in cybersecurity is a critical aspect, encompassing various dimensions from legal compliance to ethical data handling.

It is integral to effective security compliance and requires a comprehensive approach that encompasses

- legal adherence
- technical controls
- and organizational processes



CompTIA Security+ 70 Course Notes

## Legal Implications

**Privacy** is heavily regulated, with implications varying across local, regional, national, and global jurisdictions.

Laws like the GDPR in Europe, CCPA in California, and various other data protection regulations globally, impose **specific requirements on how organizations should handle personal data**.

**Non-compliance** can result in significant legal penalties, including fines and sanctions.





CompTIA Security+ 70 Course Notes

## Local/Regional Legal Implications:

Local or regional laws typically address **specific issues** pertinent to a smaller geographic area or community.

These laws can be **more detailed** or stricter in certain areas, depending on the local context and specific concerns.

For instance, a city or state might have specific laws regarding the use of surveillance technology or the protection of consumer data.



## CompTIA Security+ 70 Course Notes

# National Legal Implications

National laws are **broader in scope**, impacting how organizations operate across an entire country.

They typically include **comprehensive data protection laws** (like the Health Insurance Portability and Accountability Act (HIPAA) in the U.S.), cybersecurity regulations, and industry-specific requirements.

National laws can **set the baseline** for security and privacy standards, often influencing local or regional legislation.



CompTIA Security+ 70 Course Notes

## Global Legal Implications

Global legal implications come into play for organizations **operating internationally or dealing with data across national borders.**

They must navigate various international laws and regulations, such as the General Data Protection Regulation (GDPR) in the European Union, which has extraterritorial reach.

Global compliance is **complex** due to the **variation** in laws across different countries and regions.



## CompTIA Security+ 70 Course Notes

# Data Subject

The data subject is an individual whose personal data is processed by an organization.

Protecting the rights and privacy of data subjects is a central focus of most privacy regulations.

This includes **ensuring consent** for data processing and **allowing data subjects to access their data**.



## CompTIA Security+ 70 Course Notes

# Controller vs. Processor

In privacy terminology, a controller is an entity that determines the **purposes and means of processing personal data**,

A processor is an entity that **processes the data on behalf of the controller**.



## CompTIA Security+ 70 Course Notes

# Ownership

Data ownership refers to **the rights and control over data**.

In the context of privacy, it typically relates to the **ownership of personal data** by data subjects and the organization's responsibilities in managing this data.





CompTIA Security+ 70 Course Notes

## Data Inventory and Retention

Maintaining a data inventory is essential for privacy compliance.

It involves **keeping a record** of

- what data is held
- where it is stored
- how it is used
- and how long it is retained

Data retention policies **must align with legal requirements and best practices for data minimization.**

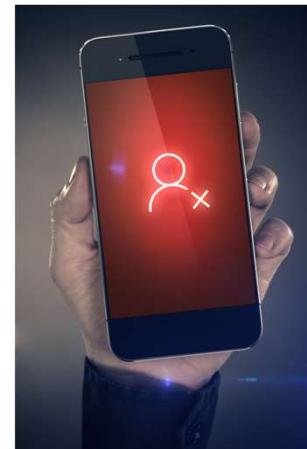


CompTIA Security+ 70 Course Notes

## Right to Be Forgotten

Also known as the right to erasure, it is a principle that allows individuals to **request the deletion of their personal data** when there is no compelling reason for its continued processing.

This concept is a cornerstone of GDPR and is being adopted in various forms in other privacy regulations.



24 5.5

---



CompTIA Security+ 70 Course Notes

## Internal Assessments

Audits, assessments, and procedures **conducted within an organization** by its own employees or a designated internal audit team.

These internal activities are crucial for maintaining and improving cybersecurity measures, ensuring compliance, and preparing for external audits.





## CompTIA Security+ 70 Course Notes

# Compliance

Internal audits play a critical role in ensuring that the organization complies with relevant cybersecurity **regulations and standards**.

This includes laws like GDPR, HIPAA, or industry-specific regulations like PCI-DSS for payment card security.

By regularly reviewing and assessing internal processes and controls, the organization can **identify and rectify compliance gaps** before they become a legal or security issue.



CompTIA Security+ 70 Course Notes

## Audit Committee

An internal audit committee typically oversees the internal audit function.

They ensure that audits are conducted objectively, thoroughly, and in alignment with the organization's strategic goals.

The audit committee also plays a key role in **evaluating the findings of internal audits** and ensuring that appropriate actions are taken in response to any identified issues.



CompTIA Security+ 70 Course Notes

## Self-Assessments

They involve the organization's IT and security teams regularly evaluating their own cybersecurity measures and controls.

This **proactive** approach allows for continuous monitoring and improvement of cybersecurity practices.

Self-assessments help

- **identify** vulnerabilities and gaps in security controls
- **assess** the effectiveness of current security measures
- and **guide** the allocation of resources towards areas that need strengthening



## CompTIA Security+ 70 Course Notes

# External Assessments

Audits, examinations, assessments, and reviews conducted by entities **outside of the organization** being evaluated.

These external processes are essential for

- providing an **objective view** of an organization's cybersecurity posture,
- **ensuring compliance** with regulations,
- and **validating internal controls and practices**.





CompTIA Security+ 70 Course Notes

## Regulatory Examinations

External regulatory examinations are typically mandated by government bodies or industry regulators.

They focus on ensuring that an organization **complies with specific cybersecurity laws**, regulations, and standards (such as GDPR, HIPAA, or PCI-DSS).

These examinations are crucial for

- maintaining public trust,
- avoiding legal penalties,
- and ensuring that sensitive data is protected according to legal requirements.



CompTIA Security+ 70 Course Notes

## Independent Third-Party Audit

This refers to a **comprehensive review conducted by an independent entity** (not affiliated with the organization).

The purpose of these audits is to **validate the accuracy** of an organization's cybersecurity claims and to ensure that its security controls are **effective and in line with industry best practices**.

This type of audit is **crucial for building trust with stakeholders**, including customers, partners, and investors.



## CompTIA Security+ 70 Course Notes

# Penetration Testing

Penetration testing is a specialized, proactive method used to evaluate the security of an IT infrastructure by **safely trying to exploit vulnerabilities**.

This type of testing can be conducted in various environments and approaches, each offering unique insights into an organization's security posture.

By **simulating various types of attack scenarios**, it provides a realistic assessment of how well an organization can protect against and respond to real cyber threats.



## CompTIA Security+ 70 Course Notes

# Purpose

Penetration testing serves several purposes in a cybersecurity context:

- **Identifying vulnerabilities** that could be exploited by attackers.
- **Testing the effectiveness** of security measures and incident response procedures.
- **Providing insights** into potential security gaps in both physical and digital defenses.
- **Offering recommendations** for strengthening security postures based on real-world attack simulations.
- **Helping meet compliance requirements** that often mandate regular penetration testing.



## CompTIA Security+ 70 Course Notes

### Physical

Involves testing physical security controls to assess how well they protect assets and data.

This can include

- attempts to bypass locks,
- enter secure areas unauthorized,
- or access computer systems through physical means.





## CompTIA Security+ 70 Course Notes

### Offensive

This is a more aggressive approach where testers **actively attempt to exploit vulnerabilities** in the system, simulating the actions of a potential attacker.

**The goal is to identify and exploit weaknesses** before malicious attackers can.



## CompTIA Security+ 70 Course Notes

### Defensive

Focuses on how well an organization can **defend against and respond to attacks.**

This includes

- testing incident response procedures,
- monitoring capabilities,
- and the effectiveness of defensive mechanisms like intrusion detection systems.





CompTIA Security+ 70 Course Notes

## Integrated

**Combines various types of tests** (physical, offensive, defensive) to provide a comprehensive assessment of an organization's overall security posture.



CompTIA Security+ 70 Course Notes

## Known Environment

In this scenario, the penetration testers have **full knowledge** of the network and system infrastructure they are testing.

This allows for a **thorough and focused assessment** of specific components.



CompTIA Security+ 70 Course Notes

## Partially Known Environment

Testers have **some knowledge** of the environment, mimicking an attacker who has conducted preliminary information gathering but doesn't have complete knowledge of the target.

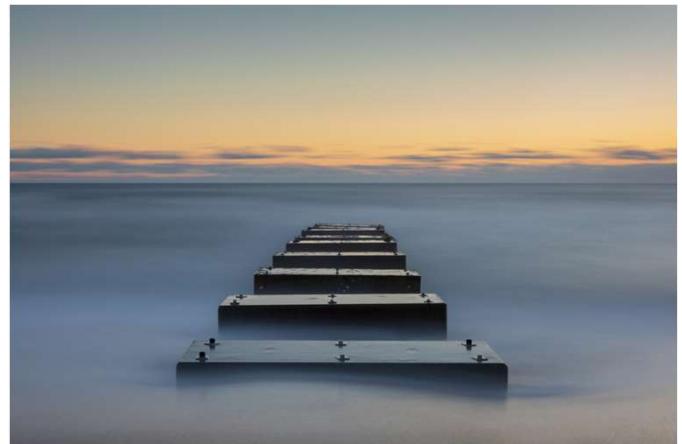


CompTIA Security+ 70 Course Notes

## Unknown Environment

Testers have **no prior knowledge** of the systems they are testing, simulating an external attacker's perspective.

This is often **considered the most realistic test** of an organization's external defenses.





## CompTIA Security+ 70 Course Notes

# Reconnaissance

Passive: Involves gathering information **without directly interacting** with the target systems.

This can include collecting publicly available information or using indirect methods to learn about the target.

Active: **Directly interacts** with the target systems to gather information.

This can include scanning for open ports, identifying running services, or attempting to elicit responses from the system to learn more about its configuration and vulnerabilities.

# Lesson 26 5.6

---



CompTIA Security+ 70 Course Notes

## Phishing

Phishing is a type of social engineering attack where attackers **deceive individuals** into providing sensitive information, such as login credentials or financial details, by **masquerading as a trustworthy entity** in digital communication.





## CompTIA Security+ 70 Course Notes

### Campaigns

Phishing campaigns involve sending **fraudulent communications**, often emails, that appear to come from legitimate sources to users.

These campaigns are usually **mass-distributed**, targeting a large number of recipients in the hope that some will respond.

Campaigns often **mimic the look and feel of legitimate emails** from well-known companies, banks, or government agencies.



## CompTIA Security+ 70 Course Notes

# Recognizing a Phishing Attempt

Key to security awareness is teaching individuals how to recognize phishing attempts.

Common indicators include:

- **Unsolicited** requests for sensitive information.
- Emails with poor grammar, spelling mistakes, or an unusual tone.
- Suspicious links or **email addresses that don't match the supposed sender's organization**.
- **Urgent or threatening language** urging immediate action.
- Offers that seem **too good to be true**.
- Unexpected **attachments**.



CompTIA Security+ 70 Course Notes

## Responding to Reported Suspicious Messages

It's crucial for organizations to have a **clear process for handling reported phishing attempts.**

This often involves:

- **Educating employees** on how to report suspected phishing emails.
- Having a **dedicated team** or channel for analyzing reported emails.
- **Taking immediate action** if a phishing attempt is confirmed, such as
  - blocking the sender's email address,
  - alerting other employees,
  - and securing potentially compromised accounts.
- **Conducting a follow-up investigation** to understand the scope of the attack and to improve defenses.



CompTIA Security+ 70 Course Notes

## Anomalous Behavior Recognition

Anomalous behavior refers to activities or actions within an organization's network or systems that deviate from the norm or expected patterns.

Recognizing such behavior is crucial for early detection of potential security incidents, including those that are risky, unexpected, or unintentional.





## Risky Behavior

This involves actions that significantly increase the likelihood of a security breach or data loss.

Risky behaviors might include:

- employees bypassing security protocols
- using unauthorized devices or software
- accessing sensitive data without a legitimate need.

Awareness programs should **educate employees** on what constitutes risky behavior and the **consequences** it may have for the organization's security.



CompTIA Security+ 70 Course Notes

## Unexpected Behavior

This category includes activities that are out of the ordinary for a particular user or system but may not immediately appear malicious.

Security awareness training should emphasize the **importance of reporting unexpected behaviors**, as they could be indicators of a compromised account or an ongoing attack.



## CompTIA Security+ 70 Course Notes

# Unintentional Behavior

Often, security incidents occur due to **unintentional actions by employees**, such as falling for phishing scams, misconfiguring systems, or accidentally sharing sensitive information.

Training should focus on helping employees recognize how their actions can inadvertently lead to security vulnerabilities and **educate them on best practices** to avoid such situations.



CompTIA Security+ 70 Course Notes

## User Guidance and Training

**Equipping users with the knowledge** and skills needed to recognize, respond to, and prevent potential cybersecurity threats.

**Effective user training covers a wide range of topics and practices**, ensuring that users understand their role in maintaining the organization's cybersecurity posture.

**Acts as a first line of defense** against cyber threats, thereby enhancing the overall security posture of the organization.



CompTIA Security+ 70 Course Notes

## Policy/Handbooks

These are **comprehensive guides** that outline the organization's cybersecurity policies, procedures, and expectations from its employees.

They **serve as a reference point** for users to understand the dos and don'ts related to cybersecurity.

**Training should include familiarizing employees with these handbooks** and ensuring they understand the importance of adhering to these policies.





CompTIA Security+ 70 Course Notes

## Situational Awareness

Training should focus on developing users' ability to **recognize potential cybersecurity threats in their daily activities**.

This includes identifying suspicious emails, unusual system behavior, and understanding the implications of their actions in a digital environment.



CompTIA Security+ 70 Course Notes

## Insider Threat

Users should be educated about the risks posed by insider threats — both **intentional** and **unintentional**.

Training should cover how to **recognize signs** of potential insider threats and the protocols for **reporting such activities**.





CompTIA Security+ 70 Course Notes

## Password Management

**Strong password practices** are fundamental in cybersecurity.

Training should cover creating strong passwords, the importance of not reusing passwords across different platforms, and using password management tools.





CompTIA Security+ 70 Course Notes

## Removable Media and Cables

Users often overlook the risks posed by removable media (like USB drives) and cables.

Training should **highlight the dangers of using non-trusted media** and the potential for data leakage or malware introduction.

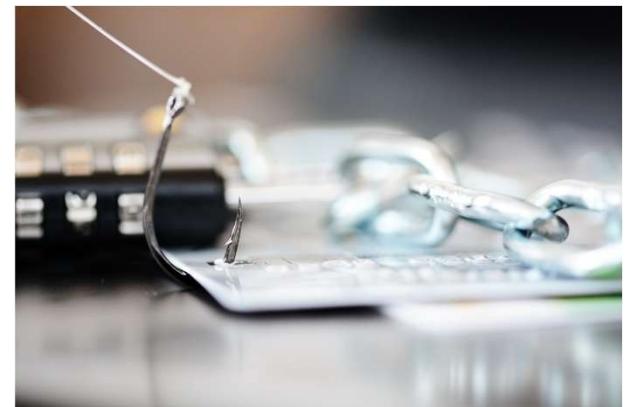


CompTIA Security+ 70 Course Notes

## Social Engineering

One of the **most common attack vectors**, social engineering involves manipulating individuals into breaking normal security procedures.

Training should teach users how to **recognize and resist social engineering** tactics, such as phishing, pretexting, baiting, and tailgating.





CompTIA Security+ 70 Course Notes

## Operational Security

This includes best practices for maintaining the confidentiality, integrity, and availability of data.

Training should cover topics like secure document handling, secure disposal of sensitive information, and the importance of regular data backups.



CompTIA Security+ 70 Course Notes

## Hybrid/Remote Work Environments

With the rise of remote and hybrid work models, training should address the **unique cybersecurity challenges** these environments present.

This includes

- secure home networking
- the use of VPNs
- the importance of maintaining physical security at home
- and the risks associated with using public Wi-Fi networks



CompTIA Security+ 70 Course Notes

## Reporting and Monitoring

These practices involve the **continuous observation of network and system activities** and the structured reporting of potential security issues.

They enable organizations to **quickly detect and respond to threats**, ensure ongoing compliance with security policies and regulations, and **continuously improve their security measures** based on real-world data and insights.





## CompTIA Security+ 70 Course Notes

# Initial Reporting

This refers to the **immediate action** taken by users or automated systems when a potential security threat or incident is identified.

**User Reporting:** Educating all employees on how to recognize and report security incidents or suspicious activities.

This could be reporting phishing attempts, unusual system behavior, or unauthorized access.

**Automated Alerts:** Setting up systems that automatically detect and report anomalies in network traffic, system performance, or user activities.

These alerts often serve as the first line of defense in identifying potential breaches.



## CompTIA Security+ 70 Course Notes

# Recurring Monitoring and Reporting

Regular Security Audits: Conducting **periodic reviews** of the organization's cybersecurity measures and practices to **identify and address potential vulnerabilities**.

Continuous Monitoring: Implementing tools and processes for **real-time monitoring** of network and system activities.

This helps in detecting and mitigating threats **as they occur**.

Performance Reports: Regularly reviewing and analyzing security logs and reports to understand the **overall health** of the organization's cybersecurity posture.

This can help in identifying trends, patterns, and areas of concern that need attention.

Compliance Reporting: Ensuring that the organization adheres to **regulatory and legal requirements** related to cybersecurity.

Regular reporting on compliance status is often **mandatory** in regulated industries.



## CompTIA Security+ 70 Course Notes

### Development

The **ongoing process** of creating, enhancing, and maintaining an effective cybersecurity awareness program.

This process is crucial for ensuring that the program stays relevant, effective, and aligned with the **evolving cybersecurity landscape and organizational needs**.

Utilizes a **dynamic** and effective security awareness program that **educates and engages employees**, stays current with the evolving threat landscape, and is deeply **integrated into the fabric of the organization's culture and operations**.



## CompTIA Security+ 70 Course Notes

### Execution

**Execution** refers to the **practical application** and **enactment of the designed** cybersecurity awareness program.

Execution is a critical phase where plans and **strategies are put into action** to educate and engage employees in maintaining and enhancing the organization's cybersecurity posture.



# Lesson 27 Physical Security

---



## CompTIA Security+ 70 Course Notes

# Physical Security

Physical security is a critical aspect that focuses on **protecting an organization's assets**, including buildings, equipment, and personnel, from physical actions and events that could cause serious loss or damage.

This includes protection from

- fire
- flood
- natural disasters
- burglary
- theft
- vandalism
- and terrorism

**Even the most sophisticated cybersecurity measures can be rendered ineffective if physical security is compromised.**



## CompTIA Security+ 70 Course Notes

### Bollards

These are **sturdy, vertical posts** designed to **prevent car-based attacks on buildings** or to control access to sensitive areas.





CompTIA Security+ 70 Course Notes

## Access Control Vestibule

This is a **secured area between two sets of doors** used to manage and control access into a secure area.

It can be equipped with biometric scanners, metal detectors, and other security measures to ensure that **only authorized individuals gain entry**.





## CompTIA Security+ 70 Course Notes

### Fencing

Fences are used to **secure the perimeter of a property.**

High-security fences are often topped with barbed wire or other deterrents to prevent unauthorized entry.





CompTIA Security+ 70 Course Notes

## Video Surveillance

The use of cameras to **monitor activities in and around a facility**.

Video surveillance acts as a deterrent to unauthorized actions and can provide valuable evidence in the event of a security breach.





## CompTIA Security+ 70 Course Notes

# Security Guard

Human security presence is a critical component of physical security.

Guards can

- monitor surveillance equipment
- conduct patrols
- respond to incidents
- and control access to facilities





CompTIA Security+ 70 Course Notes

## Access Badge

Badges are used to identify authorized personnel and often contain magnetic strips or RFID chips to allow access to secured areas.

They are a key part of an access control system.





## CompTIA Security+ 70 Course Notes

### Lighting

Adequate lighting is important for security, especially in outdoor areas.

It enhances visibility, acting as a deterrent to trespassers and aiding in the effectiveness of video surveillance.





## CompTIA Security+ 70 Course Notes

# Sensors

### Infrared Sensors:

**Detect heat and movement**, often used in intrusion detection systems.

### Pressure Sensors:

**Detect changes in pressure** (like weight) on a surface, used for securing floors or windows.

### Microwave Sensors:

**Use microwave pulses to detect movement**, useful for perimeter security.

### Ultrasonic Sensors:

**Emit ultrasonic waves and measure the reflection off a moving object**, commonly used in motion detection systems.



CompTIA Security+ 70 Course Notes

## Deception and Disruption Technology

Deception and Disruption Technology refers to a set of cybersecurity strategies and tools designed to **mislead, confuse, or disrupt the actions of malicious actors**.

These technologies are used to **create traps or illusions** that protect real network assets by diverting attackers to **decoy systems or files**.



## CompTIA Security+ 70 Course Notes

### Honeypot

A honeypot is a security mechanism set up to **detect, deflect, or study hacking attempts.**

It acts as a decoy, imitating a real computer system, network, or information system, but is **isolated and monitored.**

Attackers engaging with a honeypot provide **valuable information** about their techniques and intentions without endangering the actual network.





## CompTIA Security+ 70 Course Notes

### Honeynet

A honeynet is essentially a network of honeypots.

It simulates a network environment to attract attackers.

This setup is **more complex** and can provide **deeper insights** into how attackers interact with networks, what strategies they use, and how they move laterally within a network.



## CompTIA Security+ 70 Course Notes

### Honeyfile

These are **decoy files** placed within a network's file system.

Honeyfiles are designed to **appear legitimate and contain attractive data**, but they are monitored for access.

Unauthorized access to a honeyfile can **alert security personnel** to a potential breach or insider threat.



## CompTIA Security+ 70 Course Notes

### Honeytoken

Similar to a honeyfile, a honeytoken is a broader term that refers to **any decoy data or token inserted into a system**.

This could be a fake user account, database record, or any other type of digital bait that, if interacted with, indicates a compromise or unauthorized access.

# Lesson 28

---



CompTIA Security+ 70 Course Notes

## Change management

in cybersecurity is a **structured approach** to transitioning individuals, teams, and organizations from a current state to a **desired future state**, while ensuring the security, confidentiality, integrity, and availability of information.



CompTIA Security+ 70 Course Notes

## Business Processes Impacting Security Operation

Understanding business processes impacting security operations involves **knowing how these processes work together** to manage changes in a way that minimizes risk and ensures the security and stability of IT environments.



CompTIA Security+ 70 Course Notes

## Approval Process

A structured approval process ensures that any changes, especially those affecting IT systems and security infrastructure, are **reviewed and approved by authorized personnel before implementation**.

This step helps in mitigating risks associated with unauthorized or poorly planned changes.





## CompTIA Security+ 70 Course Notes

### Ownership

Ownership refers to identifying **who is responsible for overseeing the change process**.

This includes **responsibility for planning, execution, and follow-up**.

Clear ownership ensures **accountability** and that appropriate security considerations are integrated into the change process.



## Stakeholders

Stakeholders in a change management process include **anyone who may be affected by the change** or who has influence over the process.

In terms of security, this typically includes

- IT staff,
- security teams,
- management,
- and users.

Effective **communication** with and **involvement** of stakeholders are key for the successful implementation of changes.



## CompTIA Security+ 70 Course Notes

# Impact Analysis

Before implementing a change, it's crucial to analyze its potential impact on the organization's security posture.

This involves evaluating the risks and benefits of the change, **how it might affect existing security controls**, and what new risks it might introduce.



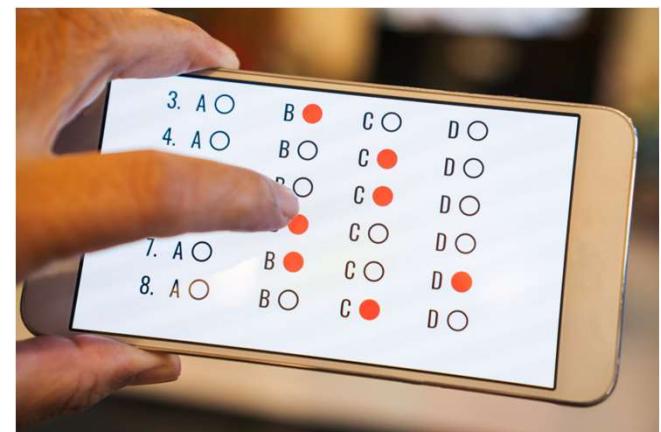
## CompTIA Security+ 70 Course Notes

# Test Results

Testing changes in a controlled environment before full implementation is essential.

This helps in **identifying any unforeseen security issues**.

Documenting test results allows organizations to use them to **refine the change further enhances security**.





## CompTIA Security+ 70 Course Notes

# Backout Plan

A backout plan is a **contingency plan** that can be activated if the change **introduces unacceptable risks or causes unforeseen issues**.

It **outlines the steps to revert the systems** to their state before the change, minimizing the impact on security and operations.



CompTIA Security+ 70 Course Notes

## Maintenance Window

This is a **predefined period** during which changes are implemented.

Scheduling changes in maintenance windows helps in **reducing the impact on users** and allows for more **controlled and secure implementation**.





CompTIA Security+ 70 Course Notes

## Standard Operating Procedure

**SOPs** are **detailed, written instructions to achieve uniformity** in the performance of specific functions.

In the context of change management, **SOPs ensure that changes are implemented consistently and securely**, adhering to best practices and compliance requirements.



CompTIA Security+ 70 Course Notes

## Technical Implications

Technical implications refer to the **direct effects** that changes in an IT environment can have on system security, functionality, and performance.

It's essential to recognize **how various technical aspects are influenced** by changes and **how to mitigate potential risks**.





## CompTIA Security+ 70 Course Notes

# Allow Lists/Deny Lists

**Changes in security configurations**, such as updating firewall rules or access control lists, can have significant implications.

Allow lists (whitelists) and deny lists (blacklists) need to be carefully managed to ensure that **only authorized entities have access** while blocking malicious or unwanted traffic.

**Incorrect changes can lead to vulnerabilities** or unintended access restrictions.



## CompTIA Security+ 70 Course Notes

# Restricted Activities

Changes in system configurations or policies might impose **new restrictions on user activities**.

This can include **limiting access** to certain resources or **disabling certain functions**.

These restrictions, while enhancing security, **can impact user productivity** and need to be communicated effectively to avoid confusion.



## CompTIA Security+ 70 Course Notes

# Downtime

Many changes, especially significant system updates or hardware replacements, can result in downtime.

Planning for downtime involves **understanding its impact** on business operations and ensuring that it's minimized.

**Security risks can arise if downtime is not properly managed**, such as increased vulnerability during system reboots or updates.





## CompTIA Security+ 70 Course Notes

### Service Restart

Restarting services or servers as part of a change can **temporarily expose security vulnerabilities**, especially if services come back online before security controls are fully re-engaged.

Planning for service restarts involves **ensuring that security measures are promptly reinstated**.



CompTIA Security+ 70 Course Notes

## Application Restart

Similar to service restarts, restarting applications as part of a change might **disrupt security settings or controls**.

Ensuring that applications maintain their security configurations upon restart is crucial.





CompTIA Security+ 70 Course Notes

## Legacy Applications

Changes in the IT environment can  
**particularly impact** legacy applications.

These older applications might not be  
**compatible** with new systems or security  
protocols, potentially creating **security gaps**.

Understanding how changes affect legacy  
systems and planning for their security is  
important.



## CompTIA Security+ 70 Course Notes

# Dependencies

IT systems often have a complex web of dependencies.

A change in one component (like an update in software) can **affect other dependent systems**.

Understanding and managing these dependencies is crucial to **prevent security issues**, such as exposed vulnerabilities or system incompatibilities.

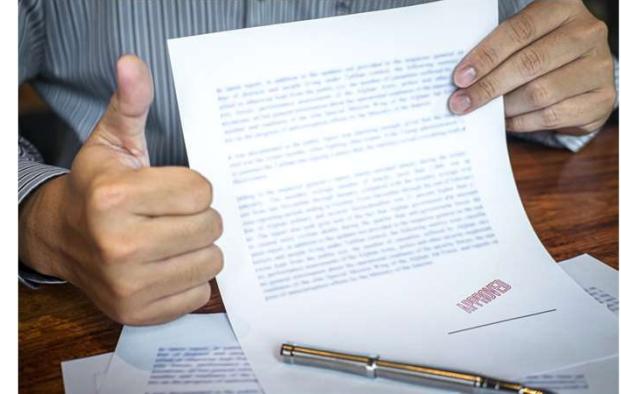


CompTIA Security+ 70 Course Notes

## Documentation

Proper documentation is essential for maintaining a **clear record of all changes**, their reasons, and their impacts on systems and security.

Understanding the **importance and scope of documentation in change management** is vital.





CompTIA Security+ 70 Course Notes

## Updating Diagrams

Network and System Diagrams: Changes in the IT infrastructure need to be **accurately reflected** in network and system diagrams.

These diagrams are crucial for **assessing the potential impacts of changes on various parts of the system**.



CompTIA Security+ 70 Course Notes

## Updating Policies/Procedures

Security Policies: Any change in the IT environment might require **updates to security policies**.

Change Management Procedures:  
**Documenting the change management process itself is critical.**



## Version Control

Version control refers to the practice of **managing changes** to software code, configurations, and other data, usually in a collaborative environment.

It is an essential tool for

- tracking changes,
- maintaining historical versions,
- and ensuring the integrity and security of software and system configurations.

# Lesson 29 resilience and recovery

---



## CompTIA Security+ 70 Course Notes

### High Availability

High Availability is about ensuring that systems, applications, and services are **available** to users over a desired period, typically aiming for **near-continuous availability**.

It involves designing systems that can **prevent or quickly recover from failures**, thereby minimizing downtime.



## Load Balancing

Load balancing is a technique used to **distribute workloads evenly across multiple servers or resources**.

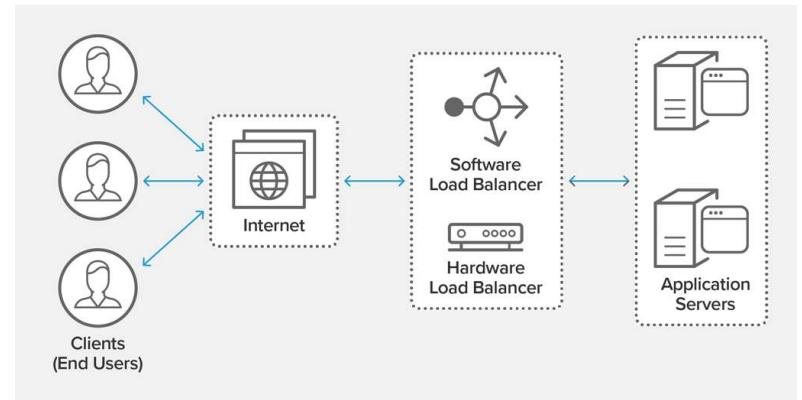
In the event one server becomes unavailable (due to hardware failure, maintenance, or a cyberattack), the load balancer can redirect traffic to other operational servers, thus maintaining the availability of services.





CompTIA Security+ 70 Course Notes

# Load Balancing





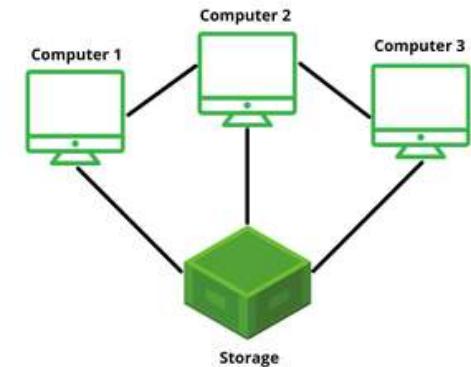
## Clustering

Clustering refers to a group of interconnected computers or servers that **work together as a single system**.

Clusters are often used for High Availability as they can provide **automatic failover**.

If one node in the cluster fails, another node can take over, ensuring that there is no interruption in service.

Clustering **can be used for various purposes**, including storage, computation, and service availability.





## CompTIA Security+ 70 Course Notes

# Site Considerations

Site considerations like hot, cold, and warm sites, along with geographic dispersion, play a critical role in this process, ensuring that organizations can **maintain continuity and protect their assets** in the face of disruptions.



## Hot Sites

A hot site is a **fully functional and equipped data center** that can be switched to immediately in case the primary site fails.

It mirrors the critical data and applications of the organization. Hot sites provide immediate failover capability.

They ensure minimal or no downtime, making them **essential for operations requiring high availability**.





## CompTIA Security+ 70 Course Notes

### Cold Sites

A cold site is a location equipped with the necessary infrastructure to support IT operations but without computers, data and applications.

It requires time and effort to become operational. Cold sites are a cost-effective solution for less critical operations.

They offer a backup option for recovery but with longer restoration times compared to hot sites.





## CompTIA Security+ 70 Course Notes

### Warm Sites

A warm site is a **middle ground between hot and cold sites**.

It contains **some pre-installed and configured equipment**, requiring less time to become operational than a cold site. Warm sites provide a **balance between cost and speed** of recovery.

They are suitable for applications that can **tolerate a short period of downtime**.



CompTIA Security+ 70 Course Notes

## Geographic Dispersion

This involves distributing IT resources and sites **across different geographic locations**.

Helps in mitigating risks associated with **local disasters or threats**.

By spreading out resources, it ensures that **an incident in one location doesn't incapacitate the entire operation**.





## CompTIA Security+ 70 Course Notes

### Platform Diversity

It involves **balancing** the benefits of diverse technology platforms with the challenges of managing a more complex IT environment.

Understanding the nuances of platform diversity and its application in real-world scenarios is crucial.





CompTIA Security+ 70 Course Notes

## Multi-cloud Systems

This refers to the use of cloud computing services from multiple providers.

Instead of relying on a single cloud service provider (CSP), organizations use a **mix of public and private clouds** to distribute their resources and services.





CompTIA Security+ 70 Course Notes

## Continuity of Operations

Continuity of Operations refers to an organization's **ability to continue its essential functions, even in the face of a major disruption or disaster.**

It ensures that key business processes and IT services **remain available and functional** during and after a cyber incident.

This resilience **minimizes downtime** and reduces the impact on business operations.



CompTIA Security+ 70 Course Notes

## Capacity Planning

Involves forecasting and **preparing** for the future **resources needed to manage information security effectively**.

It encompasses the **assessment of current capabilities** and the **anticipation of future needs**.

Proper capacity planning ensures that an organization has **adequate resources** to handle current and future cybersecurity challenges **without overextending or underutilizing its assets**.



CompTIA Security+ 70 Course Notes

## People

**Ensuring an organization has enough skilled cybersecurity professionals** to handle various tasks, including incident response, risk assessment, and system maintenance.



CompTIA Security+ 70 Course Notes

## Technology

Implementing security technologies that can **scale with the organization's growth** and evolving threat landscape.

Keeping abreast of and **investing in emerging technologies**, such as AI and machine learning, which can enhance cybersecurity capabilities.



CompTIA Security+ 70 Course Notes

## Infrastructure

Ensuring the IT infrastructure can support both **current and anticipated future cybersecurity needs.**



CompTIA Security+ 70 Course Notes

## Testing

Each plays a vital role in ensuring that an organization's security architecture is resilient and capable of recovering from disruptions.





## CompTIA Security+ 70 Course Notes

# Tabletop Exercises

Tabletop exercises are **discussion-based** sessions where team members gather to **walk through various cybersecurity scenarios**.

The primary goal is to **assess the team's understanding and preparedness** for handling different types of cyber incidents.

These exercises typically involve key personnel **discussing the response to a hypothetical cybersecurity incident**, such as a data breach or ransomware attack.



CompTIA Security+ 70 Course Notes

## Failover Testing

**Failover testing is critical for verifying the reliability and effectiveness of backup systems and processes.**

This involves **intentionally causing a system's primary processing capabilities to fail** to test whether the failover process to a secondary system occurs **smoothly and without significant disruption**.

It ensures **business continuity and data integrity** during unexpected failures, providing confidence in disaster recovery strategies.



## CompTIA Security+ 70 Course Notes

### Simulation

Simulations are realistic, controlled tests designed to **mimic the conditions of a genuine cyber-attack**.

These tests involve **creating an attack scenario** and **assessing how well the systems and the team respond to it**, typically without the knowledge of most of the organization to gauge real responses.



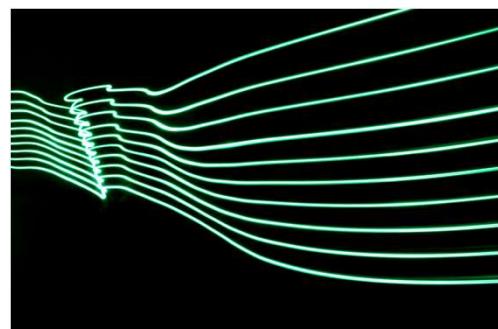


CompTIA Security+ 70 Course Notes

## Parallel Processing

Parallel processing tests the ability of an organization to handle operations on **multiple systems simultaneously**.

It involves running the primary system **alongside a secondary system** (often a backup or new system) to ensure they can operate in parallel without issues.





## CompTIA Security+ 70 Course Notes

### Backups

**Backups are copies of data and systems that are stored separately from the original, designed to be used for restoring the original in case of data loss, corruption, or a disaster.**

They can be maintained in various forms, including onsite, offsite, and in cloud environments, and are **essential for ensuring data integrity and continuity in cybersecurity**.





## CompTIA Security+ 70 Course Notes

# Onsite and Offsite

### Onsite Backups:

These are backups stored at the **same physical location** as the primary data source.

They offer **quick and easy** access for data restoration.

### Offsite Backups:

Stored at a **different location**, these backups provide additional security against disasters that could **affect the primary site**.

They are essential for **comprehensive** disaster recovery plans.



## CompTIA Security+ 70 Course Notes

### Frequency

The frequency of backups should be determined **based on the criticality** of the data and the rate at which it changes.

Critical data might require daily or even real-time backups, while less critical data may be backed up less frequently.



## CompTIA Security+ 70 Course Notes

# Encryption

Encrypting backup data is crucial for maintaining its **confidentiality and integrity**, especially for sensitive or regulated data.

Encryption should be applied both **during transmission and while the data is at rest** in the backup storage.



## CompTIA Security+ 70 Course Notes

# Snapshots

Snapshots are a method of capturing the state of a system at a **particular point in time**.

They are typically used for systems that require **regular backups with minimal disruption**, such as databases or virtual machines.





## CompTIA Security+ 70 Course Notes

### Recovery

The ability to recover data from backups is a fundamental aspect of a robust cybersecurity strategy.

It involves **processes and plans** to restore data and systems from backups **efficiently** and **effectively** after a data loss incident.



CompTIA Security+ 70 Course Notes

## Replication

Replication involves copying data to a secondary location in **real-time or near-real-time**.

Unlike traditional backups, **replication aims to keep a mirror image of the data**, which can be quickly switched to in case of primary data failure.





## CompTIA Security+ 70 Course Notes

### Journaling

Journaling is a method that keeps track of changes made to the data **since the last full backup.**

Used on databases to restore to a point in time.

It allows for **faster recovery** by only applying the changes recorded in the journal to the **last stable state.**



CompTIA Security+ 70 Course Notes

## Power

Ensuring **consistent and reliable power supply** is vital for maintaining the availability and functionality of IT systems, especially in the face of power disruptions or failures.





## CompTIA Security+ 70 Course Notes

# Generators

### Purpose:

Generators provide an **alternative power source** in case of a power outage.

They are **essential for long-term power failures** where the main supply is interrupted.

Ensure that critical systems, such as servers and data centers, **remain operational during extended power outages**.





CompTIA Security+ 70 Course Notes

## Uninterruptible Power Supply

A UPS provides **immediate power backup** in the event of a power failure, allowing for a safe shutdown of systems or bridging the gap until a generator kicks in.

A UPS is crucial for **preventing data loss and system corruption** that can occur from sudden power outages.

