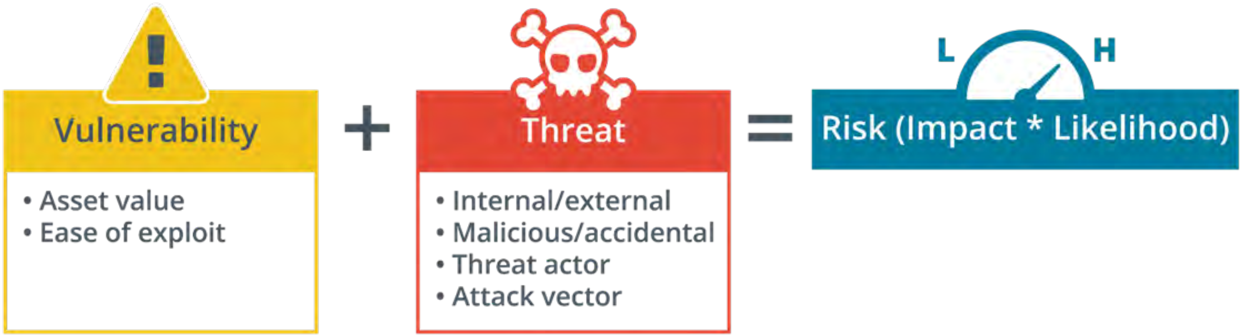
Ch 6: Threats and Security Measures

- Logical Security Concepts
- Threats and Vulnerabilities
- Physical Security Measures

Topic A: Logical Security Concepts



Vulnerability

- Asset value
- Ease of exploit

+

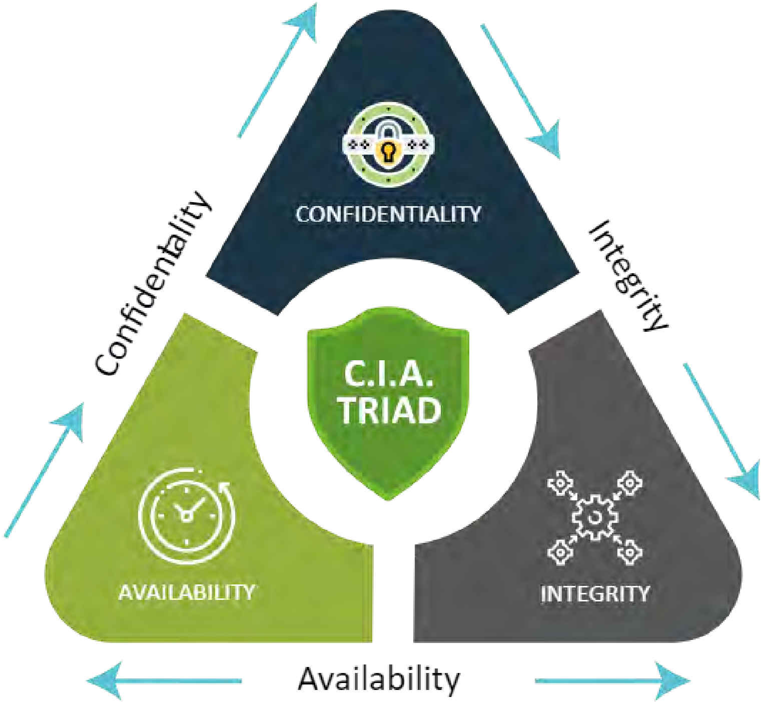
Threat

- Internal/external
- Malicious/accidental
- Threat actor
- Attack vector

=

Risk (Impact * Likelihood)

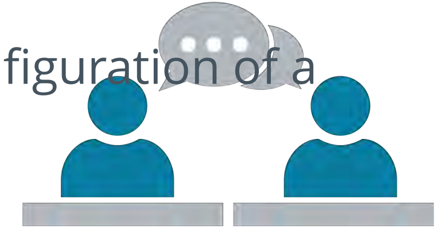
Security Basics



- CIA triad
  - Confidentiality
  - Integrity
  - Availability
- Security policies
  - Harden systems
  - Cover all aspects of computer and network technology from procurement to change to disposal

Security Basics

- **Confidentiality:** The fundamental security goal of keeping information and communications private and protecting them from unauthorized access.
- **Integrity:** The fundamental security goal of ensuring that electronic data is not altered or tampered with.
- **Availability:** The fundamental security goal of ensuring that systems operate continuously and that authorized individuals can access data that they need.
- **Hardening:** A security technique in which the default configuration of a system is altered to protect the system against attacks.



Security Controls

- **Security controls:** A technology or procedure to mitigate vulnerabilities and risk, and to ensure CIA of information.
- **Logical security:** Controls implemented in software to create an access control system. (Firewall)
- **Authentication:** A means for a user to prove their identity to a computer system.
- **Authorization:** In security terms, the process of determining what rights and privileges a particular entity has.
- **Accounting**: In security terms, the process of tracking and recording system activities and resource access. Also known as auditing.

Security Controls

- Physical controls
  - Fences
  - Doors
  - Locks
- Procedural controls
  - Incident response processes
  - Management oversight
  - Security awareness
  - Training

- Logical controls
  - User authentication
  - Software-based access controls
  - Anti-virus software
  - Firewalls
- Legal, regulatory, compliance controls
  - Privacy laws
  - Policies
  - Clauses

Security Controls

text

Logical security controls

Overall operation of access control systems

Implement multiple **CIA** triad functions for more effective security systems

Authentication: means one or more methods of proving that a user is who she/he says she/he is.

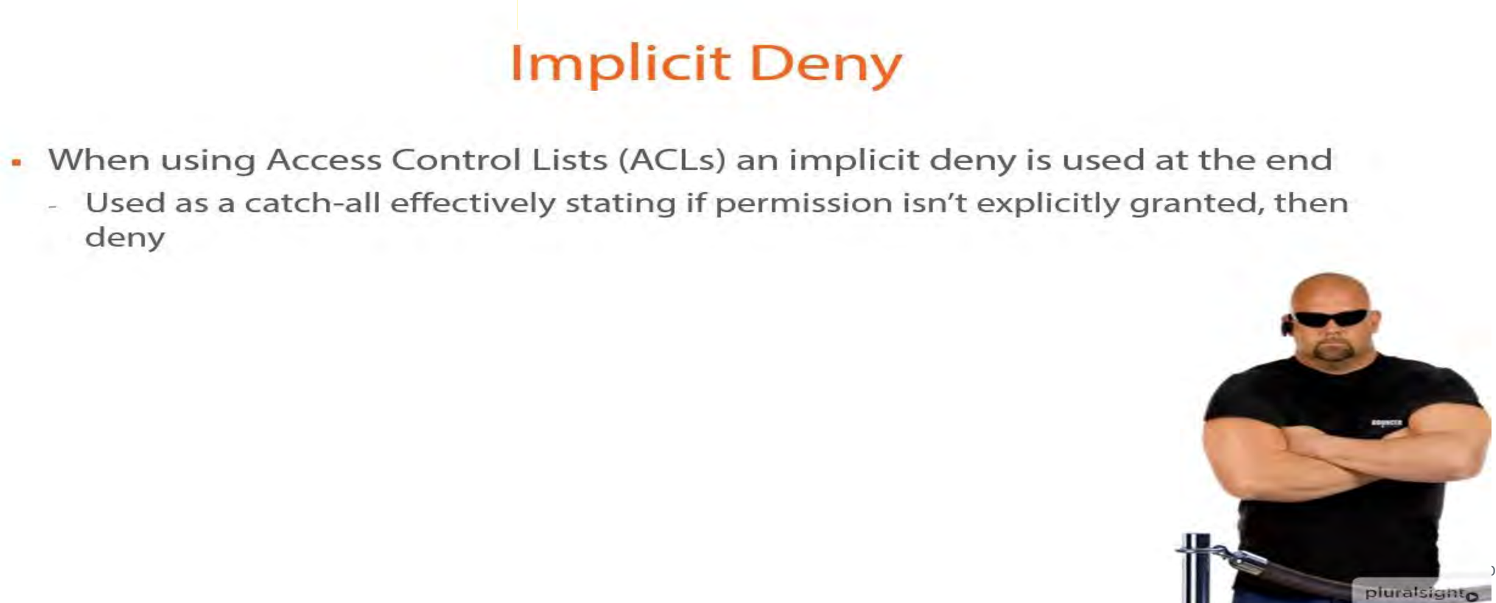
Authorization: means creating one or more barriers around the resource such that only authenticated users can gain access.

Accounting: means recording when and by whom a resource was accessed

Implicit Deny and Least Privilege

Implicit deny: Unless something has explicitly been granted access it should be denied access.

Least privilege: Something should be allocated the minimum necessary rights, privileges, or information to perform its role.



Implicit Deny

- When using Access Control Lists (ACLs) an implicit deny is used at the end
  - Used as a catch-all effectively stating if permission isn't explicitly granted, then deny

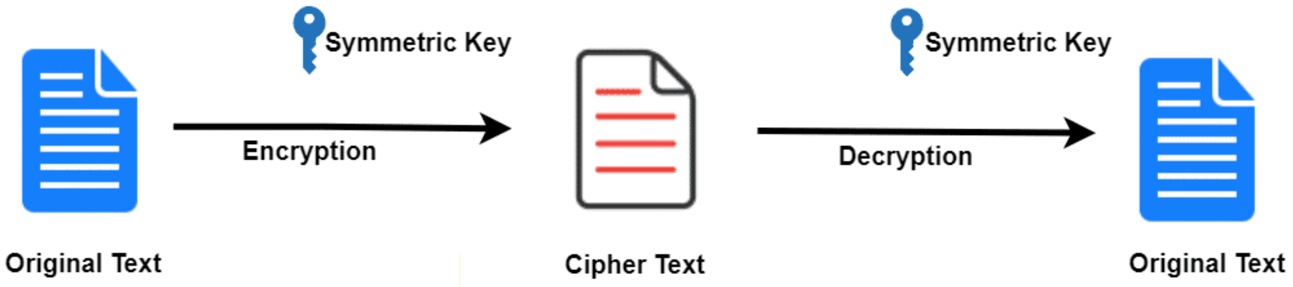
Encryption

Encryption: Scrambling the characters used in a message so that the message can be seen but not understood or modified unless it can be deciphered.

Symmetric encryption

- Single secret key used to encrypt and decrypt data
- Maybe two keys, but one is easy to determine for the other
- Need to securely distribute and store the key
- Faster and less intensive than asymmetric encryption
- Use 1024-bit key encryption
  - Takes more processing to perform encryption and decryption

Encryption


Symmetric Key
Symmetric Key
Encryption
Decryption
Original Text
Cipher Text
Original Text

Encryption

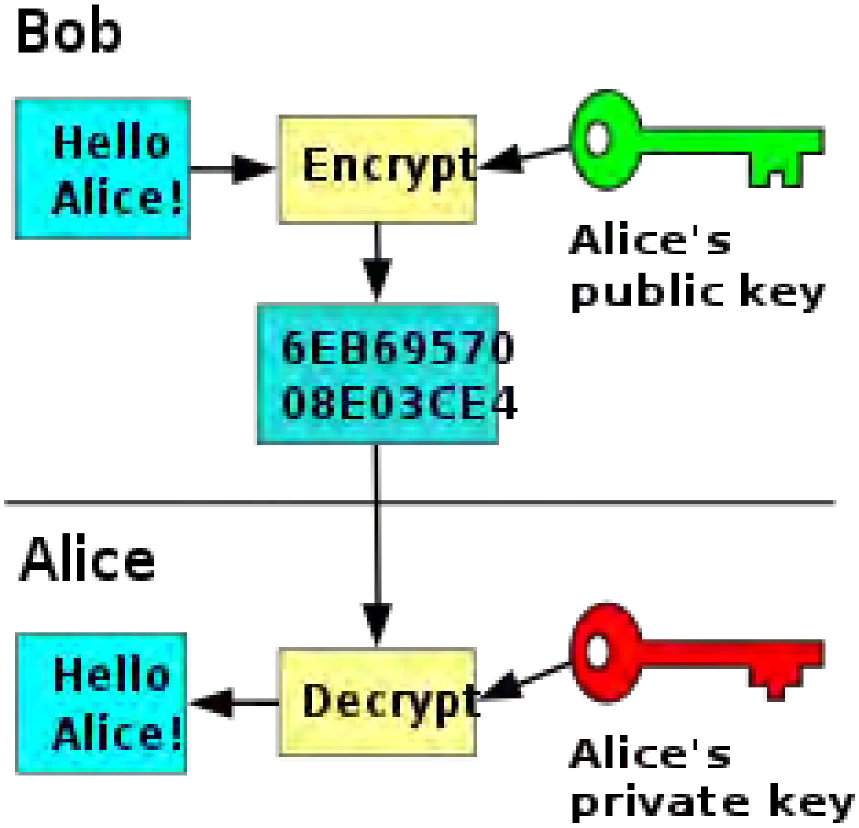
Asymmetric encryption

- Uses a private key to decrypt data
- Mathematically related public key encrypts data
- Often used for digital certificates, digital signatures, and key exchange
- Most often uses RSA cipher

Key exchange: Two hosts need to know the same symmetric encryption key without any other host finding out what it is.

RSA cipher: The first successful algorithm to be designed for public key encryption. It is named for its designers, Rivest, Shamir, and Adelman.

Encryption


Bob
Hello Alice!
Encrypt
Alice's public key
6EB69570 08E03CE4
Alice
Hello Alice!
Decrypt
Alice's private key

Encryption

important

Test

Cryptographic encryption: A hashed value from which it is impossible to recover the original data.

Hash: The value that results from hashing encryption as a short representation of data.

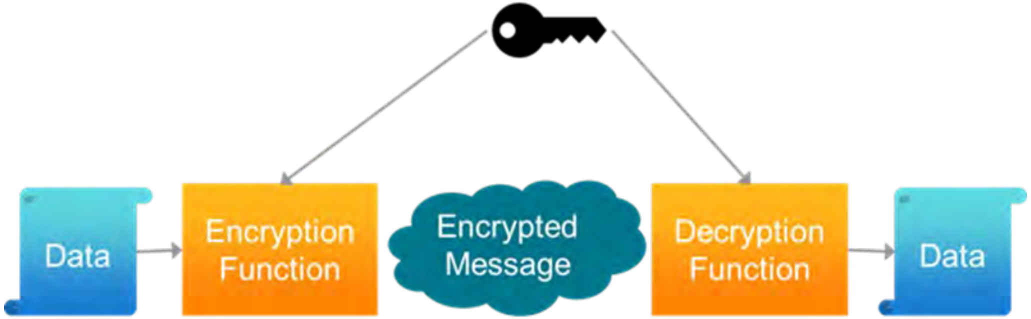
SHA1/2: A cryptographic hashing algorithm created to address possible weaknesses in MDA.

MD5: The Message Digest Algorithm.

Cryptographic encryption

- Provides integrity function in most systems
- Not technically encryption as it is a one-way cryptographic process
- Often uses
  - SHA-1
  - SHA-2
  - MD5

Encryption



- Cryptography - is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.

- An example of basic cryptography is an encrypted message in which letters are replaced with other characters.

Encryption Cryptominers

Cryptominers

- Used both legitimately and illegitimately to mine Cryptocurrencies.

- Cryptominers, when used illegitimately on your computer, it seeks to hijack idle processing power to mine cryptocurrency and make the cybercriminal rich.

PKI and Certificates

PKI: Asymmetric encryption for secure key distribution for symmetric encryption.

CA: A server that can issue digital certificates and the associated public/private key pairs.

Digital certificate: X.509 certificate issued by a CA as guarantee that the key belongs to the organization.

- Asymmetric encryption is important part of PKI.
  - PKI authenticates subjects on public networks.
  - Users and servers are validated by a CA.
  - Digital certificate contains public key associated with the subject.
  - Certificate signed by the CA to guarantee validity.
- Client can send data to the server using the public key knowing only the server can decrypt the data.
- Digital certificates also used to secure authentication to networks.

Execution Control

Execution control (Harding) : Logical security technologies designed to prevent malicious software from running on a host and establish a security system that does not entirely depend on the good behavior of individual users.

- Helps prevent malicious software from running on a host.
- Helps establish security system not entirely dependent on good behavior of individual users.

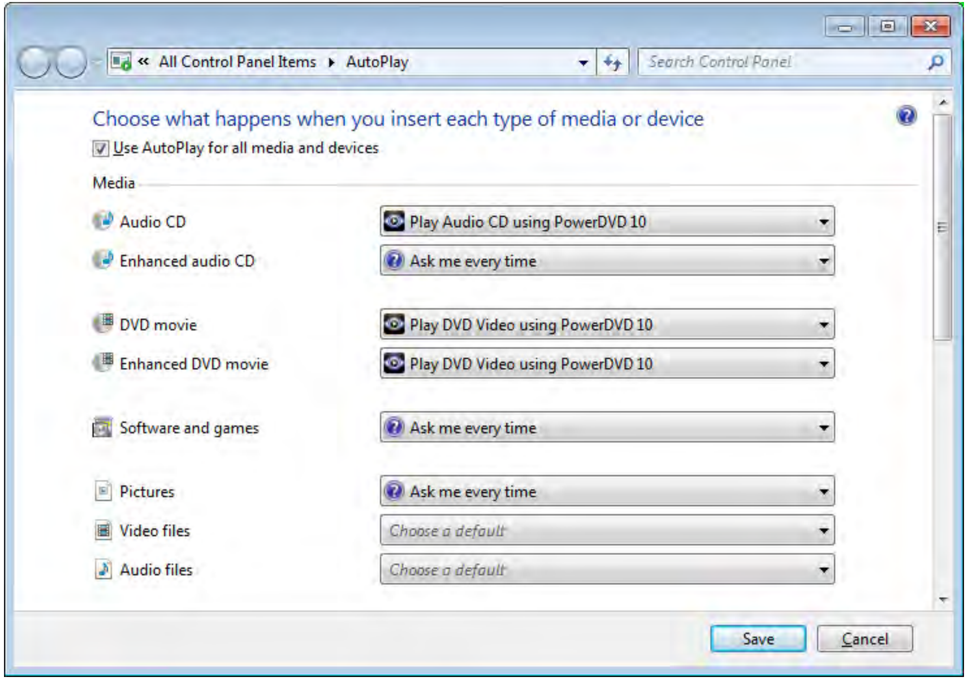
Execution Control

Trusted and Untrusted Software Sources

- Restrict the ability of users to run unapproved program code
  - Administrator and User accounts
  - User Account Control
  - System policies
- App developers should use digital certificates for code signing
  - Proves authenticity and integrity of installer package
- Third-party network management suites enforce application control
  - Blacklist and whitelist software

Execution Control

- Disable AutoRun



Choose what happens when you insert each type of media or device

☑ Use AutoPlay for all media and devices

Media

Audio CD: Play Audio CD using PowerDVD 10

Enhanced audio CD: Ask me every time

DVD movie: Play DVD Video using PowerDVD 10

Enhanced DVD movie: Play DVD Video using PowerDVD 10

Software and games: Ask me every time

Pictures: Ask me every time

Video files: Choose a default

Audio files: Choose a default

Execution Control

- Anti-virus:
  - Detects malware and prevents it from executing
  - Uses database of known patterns
    - Definitions
    - Signatures
  - Uses heuristic identification

- Anti-malware detects threats that are not virus-like:
    - Spyware
    - Trojans
    - Rootkits
    - Ransomware

Heuristic: Monitoring technique that allows dynamic pattern matching based on past experience rather than relying on pre-loaded signatures.

Anti-malware: Software that scans devices for malicious software.

Execution Control

Patch

Patch Management:

Apply

Apply all the latest patches to ensure the system is as secure as possible against attacks against flaws in the software.

Apply

Only apply a patch if it solves a particular problem being experienced.

- Requires more work
- Need to keep abreast of security bulletins
- Updates can cause problems with application compatibility

Test

Test updates on non-production system before rolling out.

NAC

- **Firewalls:** Hardware or software that filters traffic passing into or out of a network.

- **Defense in depth:** Configuring security controls on hosts as well as providing network security, physical security, and administrative controls.

- **NAC:** A means of ensuring endpoint security.

- **Health policy:** Policies or profiles describing a minimum security configuration that devices must meet to be granted network access.

- **MAC filtering:** Applying an access control list to a switch or access point so that only clients with approved MAC addresses can connect to it.

NAC

Port-based NAC: An IEEE 802.1X standard in which the switch (or router) performs some sort of authentication of the attached device before activating the port.

Supplicant: Under 802.1X, the device requesting access.

EAPoL (over land): Framework for negotiating authentication methods, supporting a range of authentication devices.

NAC

Firewalls manage access between networks

Defense in depth monitors security behind the perimeter firewall

Health policy checks for:

- Malware
- Patch levels
- Personal firewall status
- Virus definitions

Physical port security

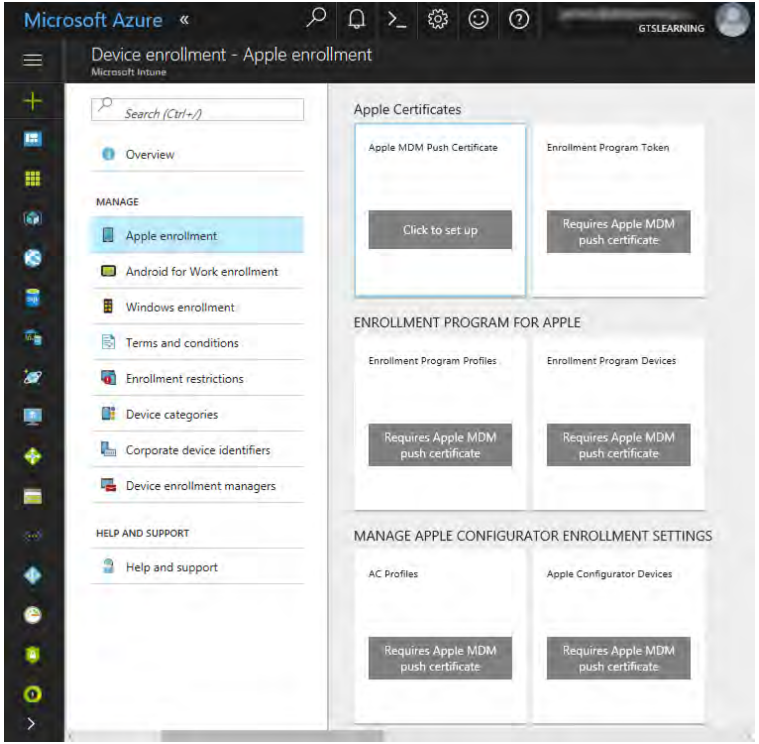
Mac address filtering

Port Security and IEEE 802.1X

MDM

MDM: Software suites designed to manage use of smartphones and tablets within an enterprise.

BYOD: Security framework and tools to facilitate use of personally owned devices to access corporate networks and data.



Microsoft Azure «
GTSLEARNING
Device enrollment - Apple enrollment
Microsoft Intune
Search (Ctrl+/)
Overview
MANAGE
Apple enrollment
Android for Work enrollment
Windows enrollment
Terms and conditions
Enrollment restrictions
Device categories
Corporate device identifiers
Device enrollment managers
HELP AND SUPPORT
Help and support
Apple Certificates
Apple MDM Push Certificate
Click to set up
Enrollment Program Token
Requires Apple MDM push certificate
ENROLLMENT PROGRAM FOR APPLE
Enrollment Program Profiles
Requires Apple MDM push certificate
Enrollment Program Devices
Requires Apple MDM push certificate
MANAGE APPLE CONFIGURATOR ENROLLMENT SETTINGS
AC Profiles
Requires Apple MDM push certificate
Apple Configurator Devices
Requires Apple MDM push certificate

VPN

- Connects components and resources of two private networks over a public network.
  - Tunnels through the public network
  - Uses IPSec and encryption
  - Communications are encrypted and packaged within another TCP/IP packet stream
- Remote access request granted upon successful user authentication and if the account has been given remote permission.
- Client may be subject to NAC policy checks.

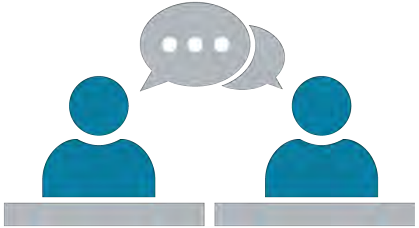
VPN: A secure tunnel created between two endpoints connected via an unsecure network.

IPSec: Layer 3 protocol suite providing security for TCP/IP.

Discussing Logical Security Concepts

- **Confidentiality and integrity are two important properties of information stored in a secure retrieval system. What is the third property?**

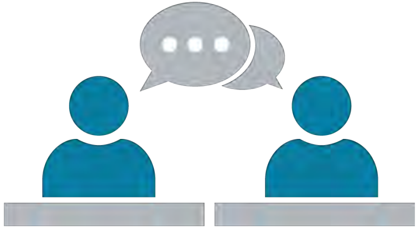
- **ANSWER:**
  - Availability—information that is inaccessible is not of much use to authorized users. For example, a secure system must protect against Denial of Service (DoS) attacks.



Discussing Logical Security Concepts

- While you are assigning privileges to the accounting department in your organization, Cindy, a human resource administrative assistant, insists that she needs access to the employee records database so that she can fulfill change of address requests from employees.
- After checking with her manager and referring to the organization's access control security policy, Cindy's job role does not fall into the authorized category for access to that database. What security concept is being practiced in this scenario?

- ANSWER:
  - The principle of least privilege.

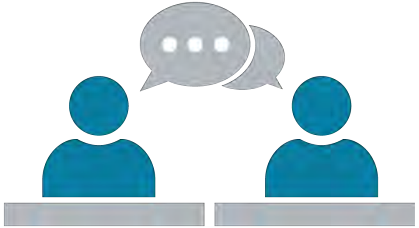


Discussing Logical Security Concepts

- **What distinguishes a cryptographic hash from the output of an encryption algorithm?**

this is thhe test question

- **ANSWER:**
  - An encrypted ciphertext can be decrypted by using the correct key; a cryptographic hash is irreversibly scrambled.



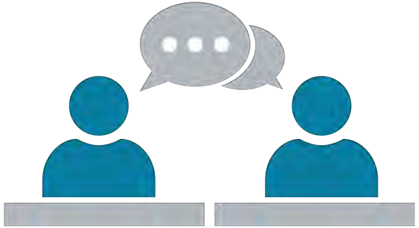
Discussing Logical Security Concepts

- **What type of cryptographic algorithm is AES?**

- **ANSWER:**
  - The Advanced Encryption Standard (AES) is a symmetric encryption cipher.
  - This means that the same key can be used to perform both encryption and decryption operations on a message.

Key

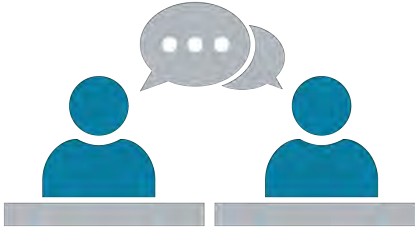
Crypto



Discussing Logical Security Concepts

- **What type of cryptographic key is delivered in a digital certificate?**

- **ANSWER:**
  - A digital certificate is a wrapper for a subject's public key. The public and private keys in an asymmetric cipher are paired. If one key is used to encrypt a message, only the other key can then decrypt it.



Discussing Logical Security Concepts

- **John brought in the new tablet he just purchased and tried to connect to the corporate network. He knows the SSID of the wireless network and the password used to access the wireless network. He was denied access, and a warning message was displayed that he must contact the IT Department immediately. What happened and why did he receive the message?**

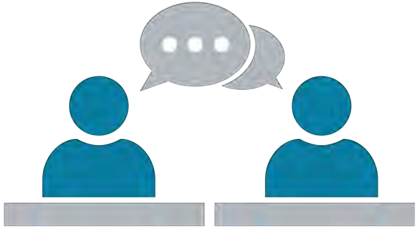
- **ANSWER:**
  - John's new tablet probably does not meet the compliance requirements for network access.
  - Being a new device, it might not have had updates and patches applied, it might not have appropriate virus protection installed, or it does not meet some other compliance requirement.
  - This caused the system to appear as a non-compliant system to the network, and network access was denied.

CompTIA

Discussing Logical Security Concepts

- **What type of network access is facilitated by VPN?**

- **ANSWER:**
  - A Virtual Private Network (VPN) is often deployed to provide remote access to users who cannot otherwise make a physical connection an office network.
  - A remote access VPN means that the user can connect to a private network using a public network for transport. Encryption and authentication are used to make sure the connection is private and only available to authorized users. You might also mention that VPNs can be used to other types of access (such as connecting one network site to another).



Topic B: Threats and Vulnerabilities

Vulnerabilities, Threats, and Risks

Vulnerability: Any weakness that could be triggered accidentally or exploited intentionally to cause a security breach.

Threat: Any potential violation of security policies or procedures.

Threat agent: A person or event that triggers a vulnerability accidentally or exploits it intentionally.

Risk: The likelihood and impact (or consequence) of a threat actor exercising a vulnerability.

Social Engineering Threats

Social engineering: A hacking technique whereby the hacker gains useful information about an organization by deceiving its users or by exploiting their unsecure working practices.

Attacker gains insider knowledge

Attacker often carries out multiple small steps to gain access

Attacks depend on human factors

Attacks come in a variety of ways:

- In person
- Email
- Phone

Often targets non-technical users and users who need assistance

Common Social Engineering Exploits

- Impersonation
- Phishing
- Spoofing
- Spear phishing
- Pharming
- Dumpster diving
- Shoulder surfing
- Tailgating

Mitigation of Social Engineering Attacks

Training

- Only release information using standard procedures
- Identify phishing style attacks
- Not to release work-related information to third-party sites or social networking

Reporting system for suspected attacks

Network Footprinting Threats

- **Footprinting**: An information **gathering threat**, in which the attacker attempts to learn about the configuration of the network and security systems through social engineering attacks or software-based tools.

- **Network mapping**: Tools used to gather information about the way the network is built and configured and the current status of hosts.

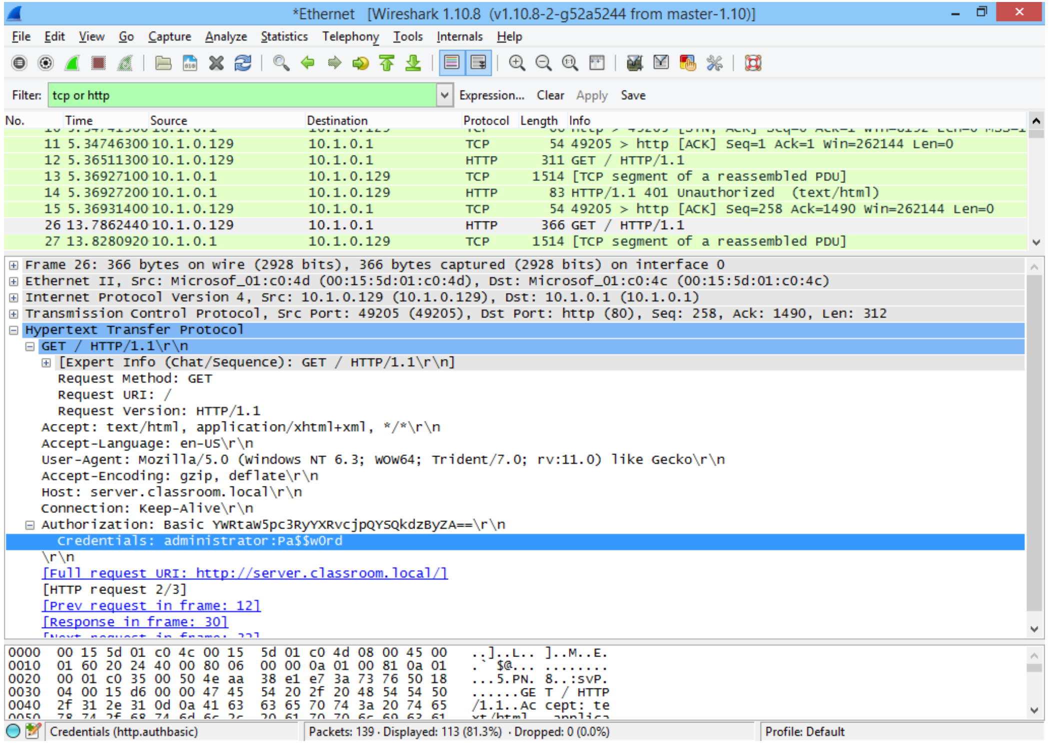
- **Port scanning:** Software that enumerates the status of TCP and UDP ports on a target system. Port scanning can be blocked by some firewalls and IDS.

Eavesdropping Threats

Eavesdropping: Listening in to communications sent over media.

MAC flooding: Overloading the switch's MAC cache to prevent genuine devices from connecting.

ARP poisoning: Maps IP addresses to NIC MAC address.


*Ethernet [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: tcp or http

```
No.  Time        Source      Destination  Protocol Length Info
 11  5.34746300  10.1.0.129  10.1.0.1     TCP        54 49205 > http [ACK] Seq=1 Ack=1 Win=262144 Len=0
 12  5.36511300  10.1.0.129  10.1.0.1     HTTP      311 GET / HTTP/1.1
 13  5.36927100  10.1.0.1    10.1.0.129   TCP      1514 [TCP segment of a reassembled PDU]
 14  5.36927200  10.1.0.1    10.1.0.129   HTTP       83 HTTP/1.1 401 Unauthorized  (text/html)
 15  5.36931400  10.1.0.129  10.1.0.1     TCP        54 49205 > http [ACK] Seq=258 Ack=1490 Win=262144 Len=0
 26 13.7862440   10.1.0.129  10.1.0.1     HTTP      366 GET / HTTP/1.1
 27 13.8280920   10.1.0.1    10.1.0.129   TCP      1514 [TCP segment of a reassembled PDU]
```

```
⊞ Frame 26: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits) on interface 0
⊞ Ethernet II, Src: Microsof_01:c0:4d (00:15:5d:01:c0:4d), Dst: Microsof_01:c0:4c (00:15:5d:01:c0:4c)
⊞ Internet Protocol Version 4, Src: 10.1.0.129 (10.1.0.129), Dst: 10.1.0.1 (10.1.0.1)
⊞ Transmission Control Protocol, Src Port: 49205 (49205), Dst Port: http (80), Seq: 258, Ack: 1490, Len: 312
⊟ Hypertext Transfer Protocol
  ⊟ GET / HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Accept: text/html, application/xhtml+xml, */*\r\n
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: server.classroom.local\r\n
    Connection: Keep-Alive\r\n
  ⊟ Authorization: Basic YWRtaW5pc3RyYXRvcjpQYSQkdzByZA==\r\n
      Credentials: administrator:Pa$$w0rd
    \r\n
    [Full request URI: http://server.classroom.local/]
    [HTTP request 2/3]
    [Prev request in frame: 12]
    [Response in frame: 30]
```

```
0000  00 15 5d 01 c0 4c 00 15  5d 01 c0 4d 08 00 45 00   ..]..L.. ]..M..E.
0010  01 60 20 24 40 00 80 06  00 00 0a 01 00 81 0a 01   .` $@... ........
0020  00 01 c0 35 00 50 4e aa  38 e1 e7 3a 73 76 50 18   ...5.PN. 8..:svP.
0030  04 00 15 d6 00 00 47 45  54 20 2f 20 48 54 54 50   ......GE T / HTTP
0040  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 74 65   /1.1..Ac cept: te
```

Credentials (http.authbasic) | Packets: 139 · Displayed: 113 (81.3%) · Dropped: 0 (0.0%) | Profile: Default

CompTIA

Spoofing and MITM Threats

man in the middle threasts

- **Spoofing:** Attacker disguises their identity. Wireless AP MAC
- **Replay attack:** Attacker intercepts some authentication data and reuses it to try to re-establish a session.
- **MITM:** Attacker intercepts communications between two hosts.
- **Mutual authentication:** A client authenticates to the server and the server authenticates to the client.

Types of Password Attacks

Rainbow tables: Tool for speeding up attacks against Windows passwords by precomputing possible hashes.

- Dictionary
- Brute force
- Rainbow table

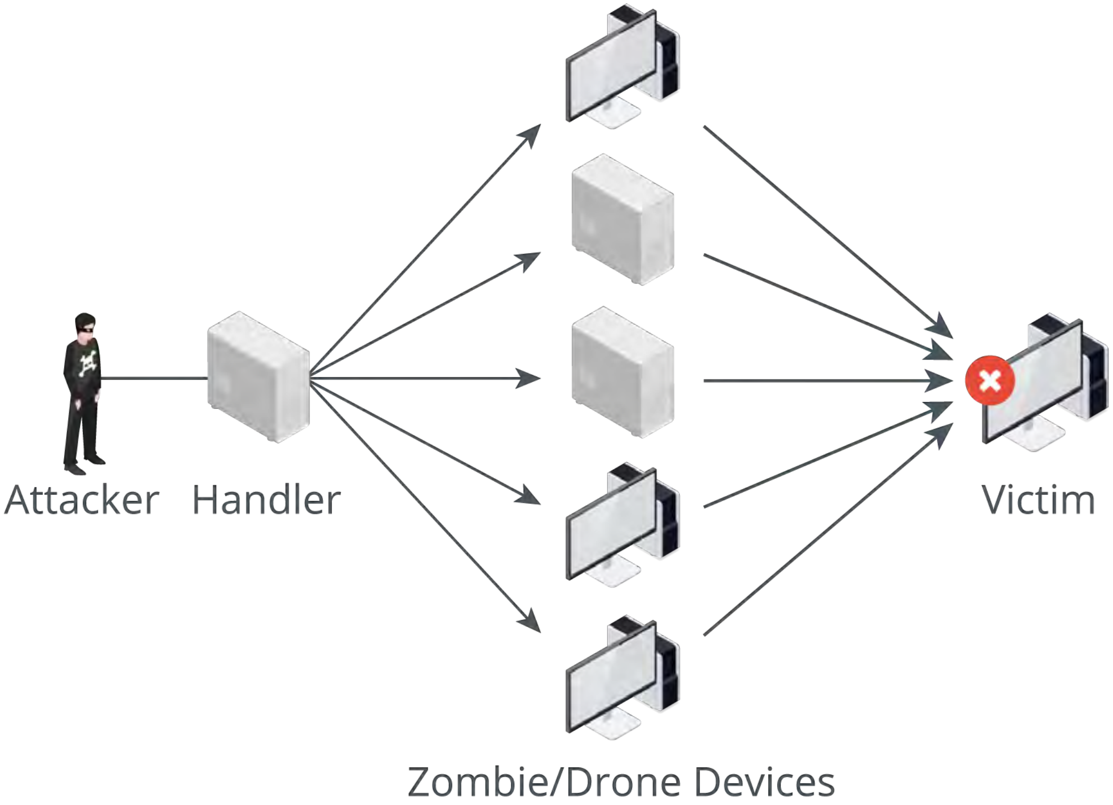
Denial of Service Attacks

- DoS attack:
  - Causes service to fail or be unavailable to legitimate users
  - Overload a service
  - Exploit design failures
  - Physical DoS attack could be cutting cables
  - Can be precursor to DNS spoofing attack

Denial of Service Attacks

- **Distributed DoS (DDoS):** A DoS attack that uses multiple compromised computers (a "botnet" of "zombies") to launch the attack.
- **Botnet:** A network of Zombies attack that aims to disrupt a service, usually by overloading it.
- **Zombie:** Unauthorized software that directs the devices to launch a DDoS attack.
- **Cyber warfare:** The use of IT services and devices to disrupt national, state, or organization activities, especially when used for military purposes.
- **Hacker collectives:** A group of hackers, working together, to target an organization as part of a cyber warfare campaign.

Denial of Service Attacks



Vulnerabilities and Zero-Day Exploits

Vulnerability: Any weakness that could be triggered accidentally or exploited intentionally to cause a security breach.

Zero

Zero-day exploit: An attack that exploits a vulnerability in software that is unknown to the software vendor and users.

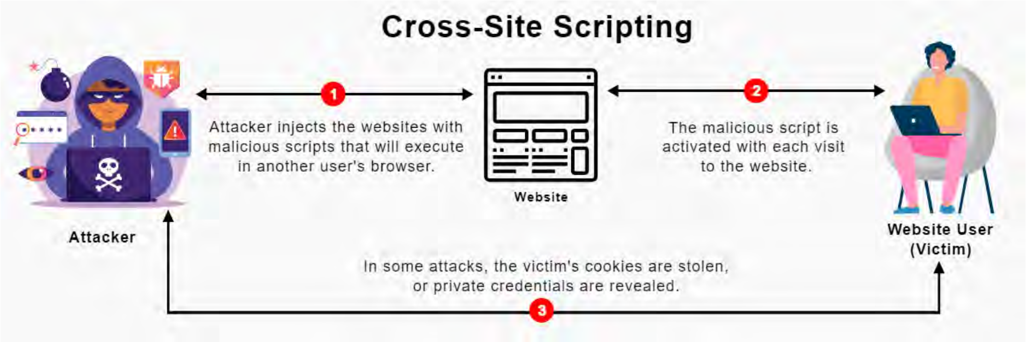
Legacy: A computer system that is no longer supported by its vendor and so is no longer provided with security updates and patches.

Cross-site Scripting Attacks

Important

- Web application vulnerabilities
  - Server-side versus client-side code
  - Input validation

- Cross-site scripting (XSS)
  - Attacker exploits input validation vulnerability to inject code into trusted site/web app
  - Non-persistent versus persistent
  - Arbitrary code could deface site, steal cookies, intercept form data, or install malware



Cross-Site Scripting

1 Attacker injects the websites with malicious scripts that will execute in another user's browser.

2 The malicious script is activated with each visit to the website.

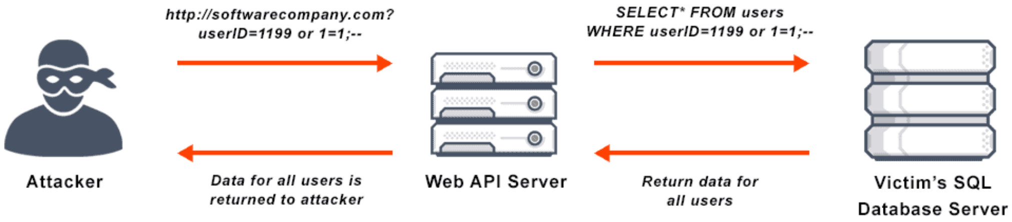
3 In some attacks, the victim's cookies are stolen, or private credentials are revealed.

SQL Injection Attacks

- Structured Query Language (SQL)
  - Statements to update and retrieve database records
  - SELECT, INSERT, DELETE, UPDATE

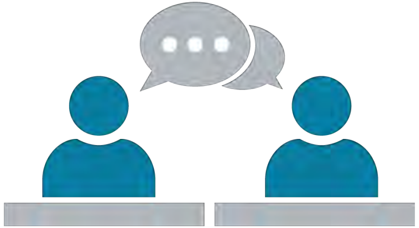
- Threat actor exploits faulty input validation to run arbitrary SQL statements
  - SELECT … FROM … WHERE

- Add or return information in the database without authorization



Discussing Threats and Vulnerabilities

- **What do all types of social engineering attack have in common?**
- **ANSWER:**
  - Many different of attacks can be classed as a type of social engineering, but they all exploit some weakness in the way people behave (through manipulation and deception).
  - These weaknesses might arise from politeness and cultural norms, from habitual behavior, or from respect for authority and rank.



CompTIA

Discussing Threats and Vulnerabilities

- **An attacker crafts an email addressed to a senior support technician inviting him to register for free football coaching advice. The website contains password-stealing malware. What is the name of this type of attack?**

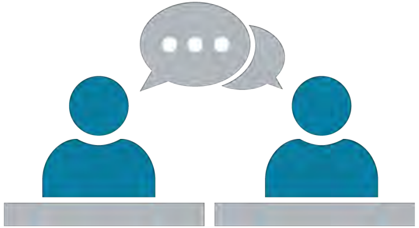
- **ANSWER:**
  - A phishing attack tries to make users authenticate with a fake resource, such as a website that appears to be a genuine online banking portal.
  - Phishing emails are often sent in mass as spam. This is a variant of phishing called spear phishing, because it is specifically targeted at a single person, using personal information known about the subject (such as his or her hobbies).

Discussing Threats and Vulnerabilities

- **What is the difference between tailgating and shoulder surfing?**

- **ANSWER:**
  - Tailgating means following someone else through a door or gateway to enter premises without authorization.

  - Shoulder surfing means observing someone type a PIN or password or other confidential data.

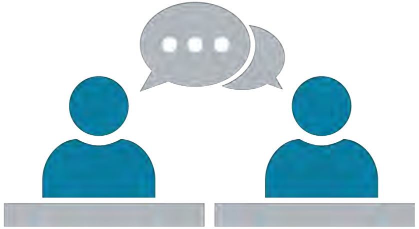


CompTIA

Discussing Threats and Vulnerabilities

- **What type of software is typically used to perform eavesdropping on an Ethernet network?**

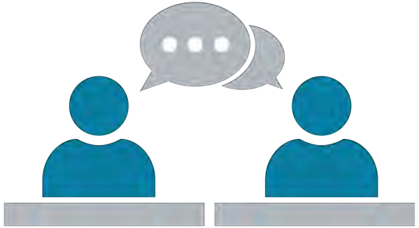
- **ANSWER:**
  - A **packet sniffer** or packet capture utility. When combined with software to decode the frames, these can also be called packet analyzers or network monitors.



CompTIA

Discussing Threats and Vulnerabilities

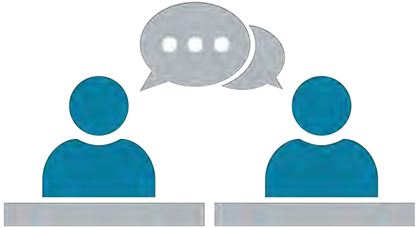
- **What attack might be launched to eavesdrop on all communications passing over a local network segment?**
- **ANSWER:**
  - Address Resolution Protocol (ARP) poisoning or spoofing. This is a type of **Man-in-the-Middle attack.**



Discussing Threats and Vulnerabilities

- **An attacker learns that a system policy causes passwords to be configured with a random mix of different characters but that are only five characters in length. What type of password cracking attack would work best here?**

- **ANSWER:**
  - **Brute force** attacks are effective against short passwords (under seven characters).
  - Dictionary attacks depend on users choosing ordinary words or phrases in a password.

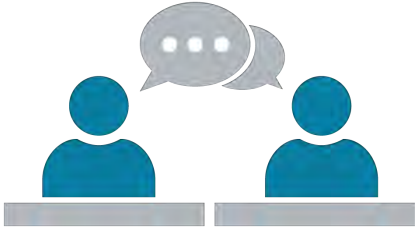


Discussing Threats and Vulnerabilities

- **What is the difference between a DoS and a DDoS attack?**

- **ANSWER:**
  - Denial of Service (DoS) is any type of attack that halts or disrupts a network application or resource.

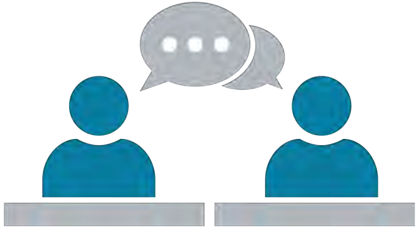
  - A Distributed Denial of Service (DDoS) is a specific class of DoS attack. It means that the attacker uses multiple hosts to launch the attack. The distributed hosts are usually PCs and other devices (zombies) compromised by malware (bots) controlled by the attacker.



Discussing Threats and Vulnerabilities

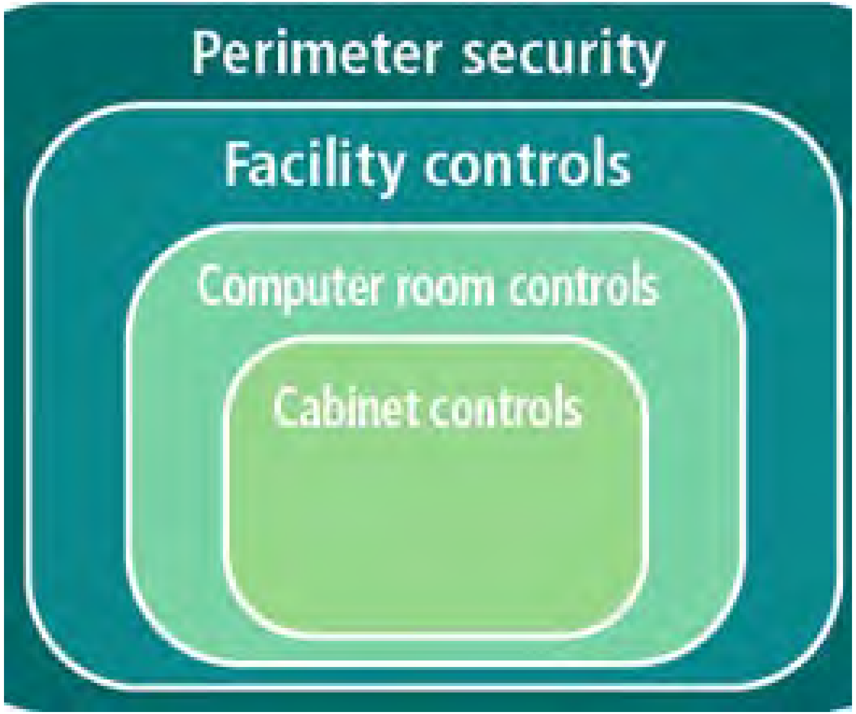
- **With what type of threat is a "zero day" associated?**

- **ANSWER:**
  - A zero day is a type of **software exploit**. You could also say that it is associated with hacking and malware threats.
  - The term arises because an attacker has found a means of exploiting a vulnerability in the software before the software developer has been able to create a patch or fix for the vulnerability.



Topic C: Physical Security Controls

- Who can access:
  - Building
  - Secure area
- Examples:
  - Wall with a door
  - Fence with a gate
- Need lock or access system



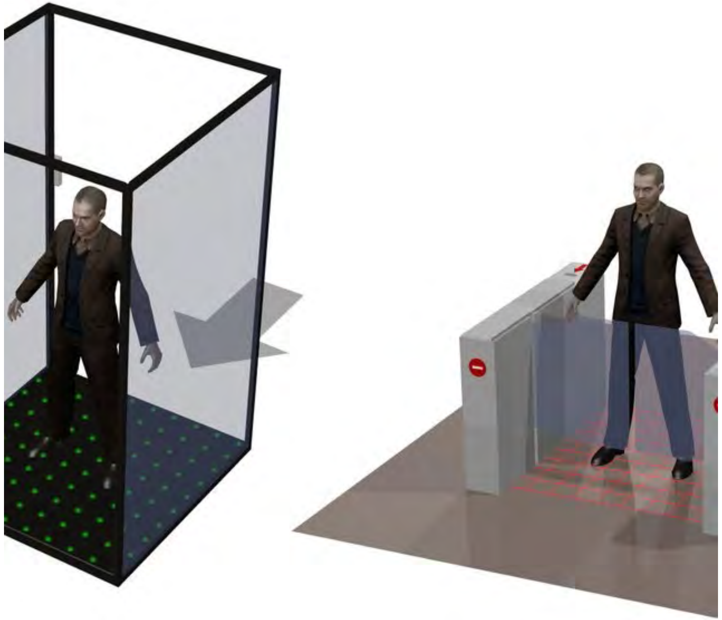
Lock Types

- Conventional
- Deadbolt
- Electronic
- Token-based
- Biometric
- Multifactor

Turnstiles and Mantraps

- **Tailgating:** Social engineering technique to gain access to a building by following someone else (or persuading them to "hold the door").

- **Mantrap:** A secure entry system with two gateways, only one of which is open at any one time.



Security Guards

- Humans:
  - Armed
  - Unarmed
  - At critical checkpoints
- Verify authentication:
  - Allow or deny access
  - Log physical entry
- Visual deterrent
- Apply knowledge and intuition to potential security breaches

ID Badges and Smart Cards

RFID badge: An ID badge containing a chip allowing data to be read wirelessly.

Common Access Card: An identity and authentication smart card produced for Department of Defense employees and contractors in response to a Homeland Security Directive.

Personal Identification Verification Card: Smart card standard for access control to US Federal government premises and computer networks.

Entry Control Rosters

Entry control roster: Sign-in sheet for managing access to premises.

Logging requirements should include:

- Name and company
- Date, time of entry, time of departure
- Reason for visiting
- Contact within the organization

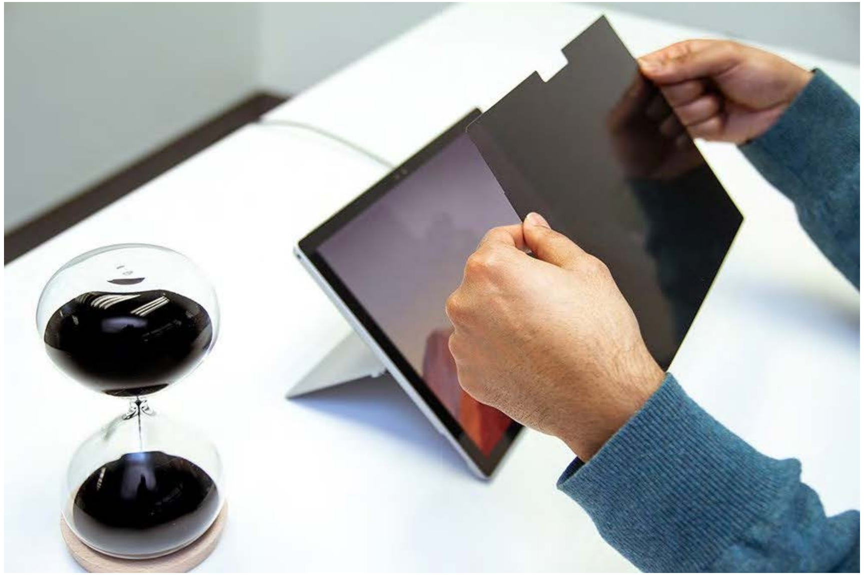
When possible, have a single entry point for visitors

- Decreases risk of unauthorized entry through tailgating

Physical Security Controls for Devices

Privacy screen: A filter to fit over a display screen so that it can only be viewed straight-on.

- Cable locks
- Locking cabinets
- Privacy screens



Data Disposal Methods

Remnant removal: Data that has nominally been deleted from a disk by the user can often be recovered using special tools.

The best way to shred data without physically destroying a disk is to ensure that each writable location has been overwritten in a random pattern.

- Physical security measures for media where data is stored
- Remnant removal critical because:
  - Organization’s confidential data could be compromised
  - Third-party data the organization possesses could be compromised
  - Software licensing could be compromised

Data Disposal Methods

Shredding: Grinding a disk into little pieces.

Incineration: Exposing the disk to high heat to melt its components.

imp On test

Degaussing: Exposing the disk to a powerful electromagnet to disrupt the magnetic pattern that stores data on the disk surface.

- Physical destruction prevents the media from being recycled or repurposed.

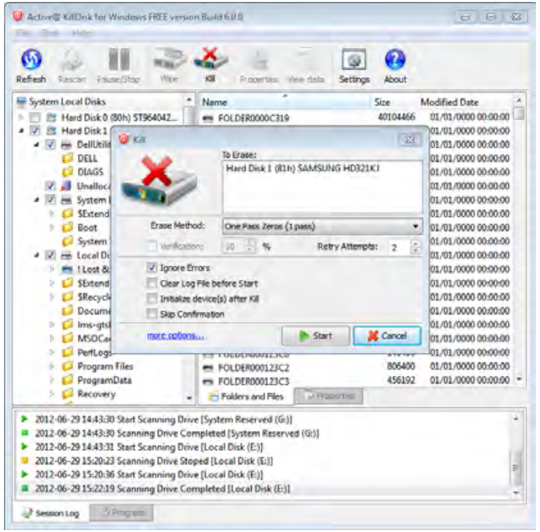
CompTIA

Data Disposal Methods

Disk wiping: Overwriting each disk location using zeroes or in a random pattern, leaving the disk in a clean state for reuse.

Low level format: Creates cylinders and sectors on the disk.

- Overwrite data
- Wipe disk
- Low level formatting
  - Wipes software



Active@ KillDisk for Windows FREE version Build 6.1.0

Kill

To Erase: Hard Disk 1 (81h) SAMSUNG HD321KJ

Erase Method: One Pass Zeros (1 pass)

□ Verification: 10 %   Retry Attempts: 2

☑ Ignore Errors
□ Clear Log File before Start
□ Initialize device(s) after Kill
□ Skip Confirmation

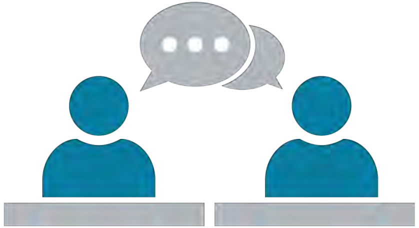
Name	Size	Modified Date
FOLDER0000C319	40104466	01/01/0000 00:00:00
FOLDER000123C2	806400	01/01/0000 00:00:00
FOLDER000123C3	456192	01/01/0000 00:00:00

```
2012-06-29 14:43:30 Start Scanning Drive [System Reserved (G:)]
2012-06-29 14:43:30 Scanning Drive Completed [System Reserved (G:)]
2012-06-29 14:43:31 Start Scanning Drive [Local Disk (E:)]
2012-06-29 15:20:23 Scanning Drive Stoped [Local Disk (E:)]
2012-06-29 15:20:36 Start Scanning Drive [Local Disk (E:)]
2012-06-29 15:22:19 Scanning Drive Completed [Local Disk (E:)]
```

Discussing Physical Security Measures

- **Katie works in a high-security government facility. When she comes to work in the morning, she places her hand on a scanning device in her building's lobby, which reads her hand print and compares it to a master record of her hand print in a database to verify her identity. What type of security control is this?**

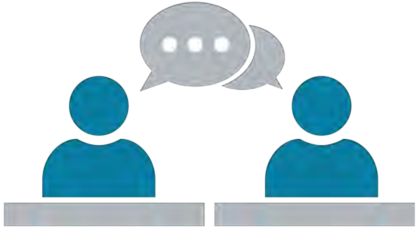
- **ANSWER:**
  - Biometric authentication deployed as part of a building's entry control system.



Discussing Physical Security Measures

- **Why might an ID badge not be restricted to use at doors and gateways?**

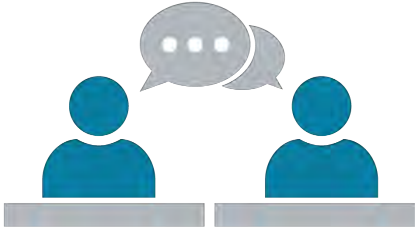
- **ANSWER:**
  - A visible ID badge shows that someone is authorized to move around a particular zone. This means that even if they are able to slip through a door using tailgating or some other method, they can be identified and challenged for not wearing visible ID.



Discussing Physical Security Measures

- **What sort of information should be recorded on an entry control roster?**

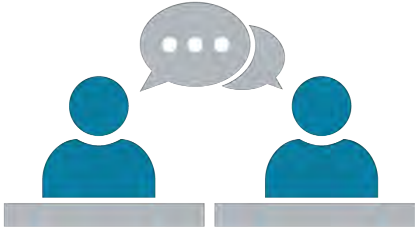
- **ANSWER:**
  - Name and company being represented, date, time of entry, and time of departure, reason for visiting, and contact within the organization.



Discussing Physical Security Measures

- **What is a server lock?**

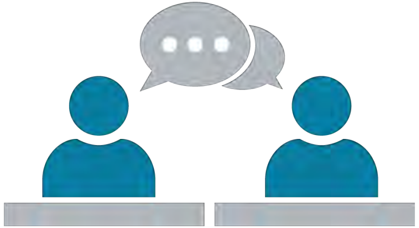
- **ANSWER:**
  - A computer in which the chassis can be locked shut, preventing access to physical components.



Discussing Physical Security Measures

- **What type of device would a privacy screen be used to protect?**

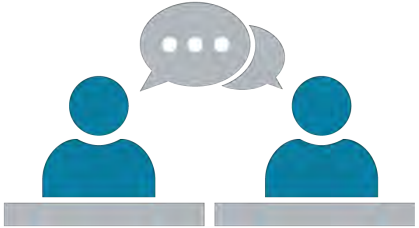
- **ANSWER:**
  - A display device such as a monitor. A privacy screen prevents the display from being observed at any angle other than directly in front of the screen.



Discussing Physical Security Measures

- **What three methods of mechanically destroying a hard disk are most effective?**

- **ANSWER:**
  - Incineration, degaussing, and shredding.
  - Making the disk unusable by damaging it with a drill or hammer is likely to leave remnants that could in theory be analyzed. Note that degaussing is not effective against SSDs.



Reflective Questions

1. What physical security controls have been employed at organizations where you have worked?

2. What steps has your organization taken to ensure the security of mobile devices? Have you planned ahead in case the devices are lost or stolen? If so, how?