Module 1: Understanding Security Threats

These notes are derived from Google Coursera's IT Support Professional courses.

The CIA Triad
A guiding model for designing information security policies.

CIA
Confidentiality - Keeping the data you have hidden safely from unwanted eyes.
Integrity - Keeping our data accurate and untampered with.
Availability - The information we have is readily accessible to those people that should have it.

Risk
The possibility of suffering a loss and the event of an attack on the system.

Vulnerability
A flaw in the system that could be exploited to compromise the system.

0-day Vulnerability (Zero Day)
A vulnerability that is not known to the software developer vendor, but is known to an attacker.

Exploit
Software that is used to take advantage of a security bug or vulnerability.

Threat
The possibility of danger that could exploit a vulnerability.

Hacker
Someone who attempts to break into or exploit a system.
- Black Hat - Try to get into systems to do something malicious.
- White Hat - Attempts to find weaknesses in the system and alert the owners of those systems

Attack
An actual attempt at causing harm to a system.

Malware
A type of malicious software that can be used to obtain your sensitive information or delete or modify files.
- Viruses: Attach themselves to some sort of executable code like a program, and replicates itself on as many files as it can infect.
- Worms: Similar to viruses, but can live on their own and spread through networks.
- Adware: Software that displays advertisements and collects data.
- Spyware: A type of malware that's meant to spy on you.
- Keylogger: Used to record every keystroke you make.
- Ransomware: A type of attack that holds your data or system hostage until you pay some sort of ransom.
- Trojans: Malware that disguises itself as one thing but does something else.
- Rootkits: A collection of software or tools that an admin would use.
- Backdoors: A way to get into a system if the other methods to get in the system aren't allowed.
- Logic Bomb: A type of malware that's intentionally installed. After a certain event or time has triggered, it will run the malicious program.
- Botnets: Designed to utilize the power of the internet-connected machines to perform some distributed function.

Antimalware Protection, Malware Removal

Malware can disrupt, damage, or even destroy a computer. IT teams are often responsible for evaluating and repairing computers that are not running well. If a computer is performing poorly or acting strangely, it might be infected with malware. IT professionals need to know how to isolate, remove, and repair infected devices. This reading covers the steps to take to detect and remove malware.

Gather and verify

If you suspect that the computer is infected, you should gather information from the user. It is helpful to note when the symptoms started and if the user has downloaded any unusual files. If the computer has one or more of the following symptoms it may be infected with malware:

- Running slower than normal
- Restarts on its own multiple times
- Uses all or a higher than normal amount of memory

After you've gathered information, verify that the issues are still occurring by monitoring the computer for a period of time. One way to monitor and verify is to review the activity on the computer's resource manager where you can see open processes running on a system.

When looking at the resource manager, you might see a program with a name you do not recognize, a program that is using a lot of memory, or both. If you see a suspicious program, you should investigate this application by asking the user if it is familiar to them.

Quarantine malware

Some malware communicates with bad actors or sends out sensitive information. Other malware is designed to take part in a distributed botnet. A botnet is a number of Internet-connected devices, each of which runs one or more bots. Because of malware's potential ability to communicate with other bad actors, you should quarantine the infected device.

To quarantine, or separate, the infected device from the rest of the network, you should disconnect from the internet by turning off WiFi and unplugging the ethernet cable. Once the computer is disconnected, the malware can no longer spread to other computers on the network.

You should also disable any automatic system backup. Some malware can reinfect a computer by using automatic backup, because you can restore the system with files infected by the malware.

Remove malware

Once you have confirmed and isolated the malware on a device, you should attempt to remove the malware from the device. First, run an offline malware scan. This scan helps find and remove the malware while the computer is still disconnected from the local network and internet.

All anti-virus/anti-malware programs rely on threat definition files to identify a virus or malware. These files are often updated automatically, but in the case of an infected computer they may be incomplete or unable to update. In this case, you may need to briefly connect to the internet to confirm that your malware program is fully updated.

The scan should successfully identify, quarantine, and remove the malware on the computer. Once the process is complete, monitor the computer again to confirm that there are no further issues.

To help ensure that a malware infection doesn't happen again threat definitions should be set to update automatically, and to automatically scan for and quarantine suspected malware.

After the malware has been removed from the computer, you should turn back on the automatic backup tool and manually create a safe restore point. If the computer needs attention in the future, this new restore point is confirmed safe and clean.

Malware education

One of the most important things an IT professional can do to protect a company and its employees is to educate users about malware. The goal of education is to stop malware from ever gaining access to company systems. Here are a few ways users and IT professionals can protect their computer and the company from malware:

- Keep the computer and software updated
- Use a non-administrator account whenever possible
- Think twice before clicking links or downloading anything
- Be careful about opening email attachments or images
- Don't trust pop-up windows that ask to download software
- Limit your file-sharing
- Use antivirus software

When all employees are on the lookout for suspicious files, it's much easier to prevent malware and viruses from taking hold.

As malware gets more sophisticated, the chance of malware eventually infecting the computers you manage becomes more likely. These steps will help you when and if that time comes.

Key takeaways

Malware can be devastating for a company's computer network. As an IT support professional, you should be familiar with how to detect, isolate, and remove malware from the computers you manage.

- An infected device should be isolated from the local network and internet as soon as possible.
- Antivirus and Anti-Malware software is a key tool for detecting and removing malware.
- Keeping threat protection software updated makes malware removal faster and easier.
- Education is the first and best line of defense against malware.

Network Attacks

DNS Cache Poisoning Attack

Tricking a DNS server into accepting a fake DNS record that will point you to a compromised DNS server. Can be spread to other DNS servers.

Man-in-the-Middle Attack

An attack that places the attacker in the middle of two hosts that think they're communicating directly with each other.

Rogue AP Attack

An access point that is installed on the network without the network administrator's knowledge.

Evil Twin Attack

An "identical" network used by an attacker to trick people into using it for malicious purposes.

Denial-of-Service (DoS) Attack

An attack that tries to prevent access to a service for legitimate users by overwhelming the network or server.

Distributed Denial-of-Service (DDoS) Attack

A DoS attack using multiple systems

Supplemental Reading for DDoS Attacks

DDoS Attacks

In this reading, you will learn about several high profile Distributed Denial of Service (DDoS) attacks and the consequences of these types of attacks. DDoS attacks are coordinated by cybercriminals who intend to disrupt the internet-based business activities of target organizations. DDoS attacks are designed to overwhelm the targeted online servers, networks, and/or platforms so that customers or end users cannot access them. Cybercriminals tend to use malware to hijack numerous internet-connected systems to repurpose as the sources for the DDoS attack. The hijacked systems are then used to send excessive numbers of requests and/or data packets to target systems. The barrage of incoming activity causes the targets to hang or crash and become temporarily inaccessible to regular internet traffic. DDoS attacks can infiltrate targeted systems through any of the Open Systems Interconnection (OSI) layers. However, the application, presentation, transport, and network layers are attacked more often than other OSI layers.

High profile DDoS attacks

- 2020 AWS: The AWS Shield Threat Landscape Report for Q1 of 2020 described the largest DDoS attack to date. AWS cloud servers were inundated by incoming traffic at a rate of 2.3 terabytes per second (Tbps) over a three day period. The peak of the attack was 44% larger than anything the AWS Shield service has experienced previously. The DDoS attack target was an undisclosed AWS cloud platform customer. Attackers took over Connection-less Lightweight Directory Access Protocol (CLDAP) web servers. CLDAP is a user directory protocol that replaced the outdated protocol, LDAP. In recent years, numerous DDoS assaults have utilized CLDAP.
- 2018 Github: In 2018, the online code management service, Github, was the target of a large-scale DDoS attack. This attack sent 126.9 million packets per second, reaching a throughput of 1.3 Tbps. This DDoS attack used memcaching, which takes advantage of a database caching system for an amplified attack impact. The attackers were able to magnify their attack by a factor of around 50,000x by saturating memcached servers with bogus queries. Github's DDoS security provider successfully alerted the company within 10 minutes of the onset, allowing Github to quickly stop the assault and work to restore operations.
- 2017 Google Cloud: This DDoS attack against Google Cloud services generated a magnitude of 2.54 Tbps. Approximately 180,000 web servers were targeted by the attackers, who used fake packets to send responses to Google. The attack was not an isolated occurrence. During the previous six months, the perpetrators had launched many DDoS attacks against Google's infrastructure.
- 2016 Dyn: A DNS service named Dyn experienced a DDoS attack in 2016. Numerous notable websites, including Netflix, The New York Times, PayPal, Amazon, Airbnb, Reddit, Visa, and GitHub experienced downtime as a result of this destructive attack from malware known as Mirai. Mirai turns infected Internet of Things (IoT) gadgets like cameras, printers, baby monitors, smart TVs, radios, etc into botnets. The malware configured the infected IoT devices to make queries to Dyn in order to generate the attack traffic. Thankfully, Dyn was able to stop the attack in one day, but the attack's purpose was never identified.
- 2015 Github: This DDoS attack was politically motivated and persisted for several days. The attack adapted itself to circumvent Github's DDoS mitigation measures. The DDoS activity came from China and was directed at two GitHub projects that were trying to avoid Chinese government censorship. It is believed that the goal of the attack was to exert pressure on GitHub to terminate such projects. Cybercriminals used Baidu, the most widely used search engine in China, to generate attack traffic by injecting JavaScript code into users' browsers. Websites that used Baidu's web traffic analytics services were used to inject malicious code in place of harmless visitor tracking scripts. The code then prompted the affected browsers to make repeated HTTP requests to the targeted GitHub pages.
- 2013 Spamhaus: Spamhaus, an organization that aids in the fight against spam emails and spam-related behavior, fell victim in 2013 to what was then the largest DDoS attack to-date. People who make money from spam emails commissioned the offense on the spam filtering service. Spamhaus experienced 300 Gbps of incoming internet traffic during the attack. When the assault started, Spamhaus registered for Cloudflare, whose DDoS defense successfully reduced the volume of the bogus incoming traffic. In an effort to take down Cloudflare, the attackers retaliated by targeting specific Internet exchanges and bandwidth suppliers. Although this assault's objective was not met, it did seriously harm LINX, the London Internet exchange. The primary attacker hired to organize this offense turned out to be a British teenager.

Resources for more information

For more information about DDoS attacks how to protect against them, please visit:

- How to Stop DDoS Attacks: Prevention & Response - Article from eSecurity Planet about types of DDoS attacks, motivations for launching DDoS attacks, and how to prevent them.
- What is a DDOS Attack & How to Protect Your Site Against One - AWS article about DDoS attacks and protection techniques.
- DDoS Protection, Mitigation, and Defense: 8 Essential Tips - A list of eight best practice tips to prevent DDoS attacks.

Client-Side Attacks

Coss-Site Scripting (XSS) Attacks

A type of injection attack where the attacker can insert malicious code and target the user of the service.

Brute Force Attack

Dictionary Attack

Deceptive Attacks

Social Engineering

An attack method that relies heavily on interactions with humans instead of computers.

- Phishing: A malicious email is sent to a victim disguised as something legitimate.
- Spear Phishing
- Email Spoofing

Tailgating

Gaining access into a restricted area or building by following a real employee in.

Deceptive Attacks

Previously, you learned about the dangers of socially engineered deceptive attacks. In this reading, you will review this topic and learn about a few more types of socially engineered deceptive attacks. Social engineering attacks are unique as compared to other types of attacks. Social engineering requires cybercriminals to use psychology to trick victims into providing information to the cybercriminal. In other types of cyber attacks, the cybercriminals use computers and other digital tools to hack computers and networks without engaging and deceiving individual victims.

Cybercriminals may use deceptive attacks to disguise their identities, intents, and motives. Through social engineering techniques, these cybercriminals attempt to trick victims into revealing private information, such as a credit card number or login credentials. The cybercriminal might disguise their identity by pretending to be from a reputable organization or to be an individual that the victim might trust, like a friend or work colleague. Socially engineered deceptive attacks can happen through websites, email, text messaging, phone calls, in-person interactions, and more. Cybercriminals often find deception through social engineering to be an easy means for hacking a computer system, simply because many technology users are not aware that this type of threat exists. Others may be aware of the potential for a deceptive cybercriminal attack, but are not sure how to recognize the deception and, further, to prevent themselves from being deceived

Social engineering attacks have increased in recent years. These attacks have changed how organizations approach their cybersecurity policies. It is important for organizations to train their employees on how to recognize a deceptive attack. A single employee that is tricked into entering their company login and password into a fake login window could create an opportunity for a catastrophic criminal attack against an organization's network.

Deceptive attacks over the internet

There are many types of social engineering attacks. Some of the more common attacks include:

- **Phishing**: A cybercriminal may use email and text messaging to "fish" or phish for victims that will take the cybercriminal's bait. One basic type of phishing bait may include a convincing story to trick the victim into replying to the email with personal or sensitive information. Another common phishing scam includes using "clickbait" links. These phishing messages entice victims to click on a link by using bait such as popular pet videos, gossip, news scandals, opportunities to win money or prizes, lewd images or videos, etc. If the recipient clicks on the link, they become victim to the next phase of the malicious attack, which could be some type of forced download of malware, ransomware, viruses, keyloggers, trackers, and more.
- **Spoofing**: Cybercriminals use this technique to alter the header on phishing emails in order to appear to originate from a legitimate business or reputable person. For example, a spoofed email might use a fake header that appears to be from a bank. The body of the email might ask the victim to click a given link to log into their bank account to fix a "problem". The link leads to the cybercriminal's fake website that looks identical to the bank website and exists only to collect the bank login credentials from victims. The fake website might even give the victim an error message and forward them to the real bank to try to login again. This technique keeps the victim from immediately recognizing they have been scammed because the second login attempt on the real website is usually successful.
- **Spear phishing**: A cybercriminal might use details about a victim's life to win the victim's trust. For example, the criminal might first purchase data from a social media platform that provides personal information about the platform's users. The cybercriminal then uses this data to target or "spear" specific individuals. The cybercriminal could select a name from a user's friends list and create a spoofed email that appears to be from that friend. The spoofed email may say something as simple as, "look at this photo I found of you online!" The email may also include an attachment or a clickbait link that leads to the next stage of the attack.
- **Whaling**: When a cybercriminal wants to spear phish a big target or "whale," they will spend more time and effort deceiving the victim. A whale target is typically someone in a position of power, such as a wealthy and/or famous person, an executive of a company, or a high-level government employee. The whale is targeted because of the likelihood that they have the ability to pay high ransomware fees, trade valuable information or confidential data, or may be vulnerable to blackmail.
- **Vishing**: Cybercriminals use Voice over IP (VoIP) to make phone calls or leave voice messages pretending to be from reputable companies in order to trick victims into revealing personal information, such as banking details and credit card numbers. Although telephone scams have been running for decades, vishing with VoIP makes it easier for cybercriminals to hide their true identity. VoIP calls are significantly more difficult to trace than landline calls.

Targeted and in-person deceptive attacks

- **Shoulder surfing**: This malicious attack might have a specific victim or organization as their target. Shoulder surfing happens when a person looks over a victim's shoulder to watch them enter login credentials, credit card numbers, or other sensitive information. For example, a temporary contractor for an organization may look over the shoulder of an employee to watch the employee enter their login info. The temporary employee's goal might be to steal credentials in order to illegally obtain confidential company data or plant ransomware.
- **Tailgating**: This in-person attack is a form of social engineering in which an unauthorized party gains physical access to a restricted area by simply following a person or group of persons who have authorized access. For example, a criminal wanting to gain physical access to an organization's computer network might dress in business clothing and follow a group of coworkers coming back from lunch. One member of the group may use their key card to open the door, then hold the door open for the rest of the group, as well as the criminal who is dressed and behaving as though they belong in the building. The criminal may even have a fake ID card to show anyone who questions them.
- **Impersonation**: This attack might happen over email, text messaging, or a phone call. The attacker impersonates someone who should have access to an organization's computer network. For example, the attacker might call the IT Support team to request help with a password reset. Alternatively, the attacker might pretend to be a member of an organization's IT Support team. They may call an employee to ask them to change some settings on their computer to fix a fake problem. These changes are intended to open a door for the cybercriminal to gain access to the organization's network.
- **Dumpster Diving**: This in-person attack involves the attacker literally digging through the trash of an individual or organization to hunt for confidential information, like financial or customer information. Shredding all confidential documents is an easy way to prevent this type of attack.
- **Evil twin**: This type of attack involves the cybercriminal installing Wi-Fi routers that appear to belong to an organization's network. These Wi-Fi access points may not require a password and might appear to offer a stronger signal than the real Wi-Fi router. When victims connect to the fake Wi-Fi access point, the cybercriminal gains access to the victim's wireless transmissions, which can include login credentials and other sensitive information.

As an IT Support professional, it is important to train the people and organizations you support on how to identify and protect from socially engineered attacks. These training sessions should be offered to all new employees, contractors, and anyone else who may have access to the organization's network. Additionally, the training sessions should be repeated on a frequent schedule as new, more sophisticated cybercrime techniques emerge. One best practice method for keeping network users always on alert for attacks, is for IT Support staff to periodically stage harmless attacks that target network users. This method is used to test how effective the training classes have been and how long the users are able to recall how to protect themselves against an attack. Instead of stealing the user's private information, the harmless attack makes users aware that they fell for a scam, and provides reminders on how to protect themselves against real cybercriminal attacks in the future.

Physical Security

Physical security measures protect technical assets and data from unauthorized physical access. This reading covers common physical security methods.

Physical security measures

Physical security measures make it harder for intruders to gain access, steal, or damage IT equipment and data. Here are some common methods:

- **Guards** monitor controlled access points throughout a facility to prevent unauthorized access.
- **Door locks** allow an area to be restricted. Only people with an authorized unlocking mechanism, like a key or security badge, can gain access to the restricted area.
- **Equipment locks** can restrict the movement of sensitive equipment, like servers, storage media, or terminals, by anchoring them to a less mobile structure. Only people with an authorized unlocking mechanism, like a key or security badge, can release the controlled equipment from its anchored location.
- **Video surveillance**: Video cameras allow continuous observation and recorded activity playback within controlled areas. Video surveillance can document who accesses a controlled area, how they access it, and what they do there.
- **Alarm systems** notify security by sounding an alarm or sending a message when a controlled area is accessed.
- **Motion sensors** are devices that detect movement within a controlled area. Motion sensors can trigger alarm systems or video surveillance.

Protecting the entry points of a building

- **Access control vestibules** create a space between two sets of interlocking doors or gateways to prevent unauthorized individuals from following authorized individuals into controlled facilities.
- **Badge readers** are devices that read information encoded into a plastic card. They identify each user by the badge they present to the device. Badge readers can be used to control electrically operated door locks and can be built into computer terminals to control access to information.

Protecting the outside of a building

- **Bollards** are sturdy, short, vertical posts placed to restrict access of vehicles to a controlled area.
- **Fences** are physical barriers, with many different designs, that enclose controlled areas to establish a perimeter and keep out external threats.

New technologies for physical security continue to evolve. Your IT security planning should include reviewing the newest methods for securing your organization's assets and information.

Key takeaways

It's essential to ensure that an organization's technical assets and data are protected physically and virtually.

- Physical security includes measures that help protect technical assets and data from unauthorized physical access.
- You should stay current with the newest methods for physically securing your organization's assets and information.

Module 2: Pelcgbybtl (Cryptology)

Cryptography
Hiding messages from potential enemies. The overarching discipline that covers the practice of coding and hiding messages from third parties. The study of this practice is referred to as **cryptology**.

Encryption
The act of taking a message, called a plaintext, and applying an operation to it, called a cipher, so that you receive a garbled, unreadable message as the output, called ciphertext.

Decryption
The reverse process of Encryption.

Encryption Algorithm
The underlying logic or process that's used to convert the paintext into ciphertext.

Cryptosystem
A collection of algorithms for key generation and encryption and decryption operations that comprise a cryptographic service should remain secure - even if everything about the system is known, except the key.

Cryptanalysis
Looking for hidden messages or trying to decipher coded messages.

Frequency Analysis
The practice of studying the frequency with which letters appear in a ciphertext.

Steganography
The practice of hiding information from observers, but not encoding it.

Supplemental Reading for The Future of Cryptanalysis

Data security is one of the top issues for companies. Being familiar with how data is protected and the attacks that can occur within a company to get sensitive information is a crucial aspect of an IT professionals role. This reading covers the definitions of cryptography and cryptanalysis as well as the five types of attacks and their outcomes.

Cryptography

Cryptography is a method of protecting information and communications using codes so that only the intended person can read and process them. Cryptography has mainly stemmed from the manual encoding of messages and information using a formula to convert any given letter or number to a new value. Encryption is the process that encodes the data making it harder to decode. The goal of encrypting data is to keep internal information secure.

Cryptanalysis

Cryptanalysis uses technology to improve the process of encrypting data and innovates new ways to defend companies from attacks that can access and decode their data.

Impact of technology

Many modern encryption algorithms are based on large prime number factorization. This factorization is difficult to do by hand since there are millions of options for these algorithms. Once the information has been encrypted using the algorithm, it is called ciphertext. Technology has evolved to create harder algorithms but also makes it easier to crack algorithms. Modern quantum computers can crack encryption keys significantly faster using factorization and brute-force attacks. An encryption key is typically a random string of bits generated specifically to scramble and unscramble data. The encryption key is then used to convert the ciphertext to plaintext, which is not encoded.

Types of cryptanalysis attack

There are several types of attacks that hackers or security professionals employ to get data from a network using cryptanalysis. The attacks all use a different way into the network to gain encoded information and translate it from the encoded form into information that can be easily read.
The following are the most common cryptanalytic attacks:

- **Known-Plaintext Analysis (KPA)** requires access to some or all of the plaintext of the encrypted information. The plaintext is not computationally tagged, specially formatted, or written in code. The analyst's goal is to examine the known plaintext to determine the key used to encrypt the message. Then they use the key to decrypt the encoded information.
- **Chosen-Plaintext Analysis (CPA)** requires that the attacker knows the encryption algorithm or has access to the device used to do the encryption. The analyst can encrypt one block of chosen plaintext with the targeted algorithm to get information about the key. Once the analyst obtains the key, they can decrypt and use sensitive information.
- **Ciphertext-Only Analysis (COA)** requires access to one or more encrypted messages. No information is needed about the plaintext data, the algorithm, or data about the cryptographic key. Intelligence agencies face this challenge when intercepting encrypted communications with no key.
- **Adaptive Chosen-Plaintext Attack (ACPA)** is similar to a chosen-plaintext attack. Unlike a CPA, it can use smaller lines of plaintext to receive its encrypted ciphertext and then crack the encryption code using the ciphertext.
- **Meddler-in-the-Middle (MITM)** uses cryptanalysts to insert a meddler between two communication devices or applications to exchange their keys for secure communication. The meddler replies as the user and then performs a key exchange with each party. The users or systems think they communicate with each other, not the meddler. These attacks allow the meddler to obtain login credentials and other sensitive information.

Results from a cryptanalysis attack

There are various results of a cryptanalysis attack. Some attacks result in a total break in the encryption and some result in more information that can help the attacker cause other damage or get closer to the goal of a total break. Common results from a cryptanalysis attack include:

- **Instance deduction** where the attacker discovers additional plain or cipher text. While the key isn’t found to break the code, the additional plaintext or ciphertext can be used to cause problems or continue attacks.
- **Information deduction** where the attacker obtains some information about plain or cipher text not previously known. The additional information can lead to more information about the encryption key.
- **Distinguishing algorithm** where the attacker can distinguish the encryption algorithm from a random alteration. This information reveals clues about the encryption algorithm and can lead to more significant breaks.
- **Global deduction** where the attacker finds an algorithm that is functionally equivalent to the one used in the key. This algorithm is then used to decrypt all information and messages.
- **Total break** where the attacker can gain the entire key. With the entire key, the attacker can decrypt all messages and information.

Key takeaways

Many companies use encryption to protect the sensitive information on their network

- Technology has advanced cryptanalysis, using more complex algorithms to encrypt data. Modern quantum computers also make it easier to use cryptanalysis to break a company’s encryption.
- The different types of attacks that focus on plaintext and ciphertext are Known-Plaintext Analysis, Chosen-Plaintext Analysis, Ciphertext-Only Analysis, and Adaptive Chosen-Plaintext Attack. The meddler in the middle attack is another cryptanalysis attack that gets the key from intercepting a key exchange.

- There are various results of a cryptanalysis attack including Instance deduction, Information deduction, Distinguishing algorithm, Global deduction, and Total break.

More resources

- For more information on large prime number factorization, see Integer Factorization.
- To read more about cryptanalysis techniques and attacks, see Cryptanalysis explained.

Symmetric Cryptography

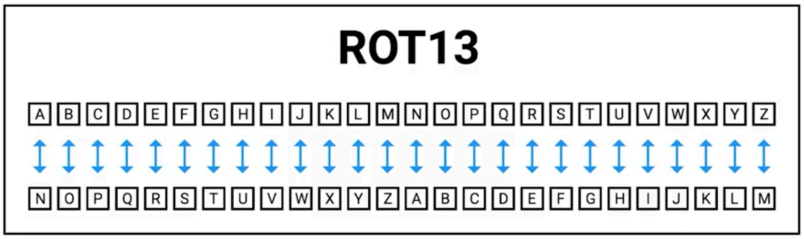
Symmetric algorithms use the same key to encrypt and decrypt a message.

Substitution Cipher

An encryption mechanism that replaces parts of your plaintext with ciphertext.

ROT13

Moves letters by 13 places



URYYB JBEYQ

Stream Cipher

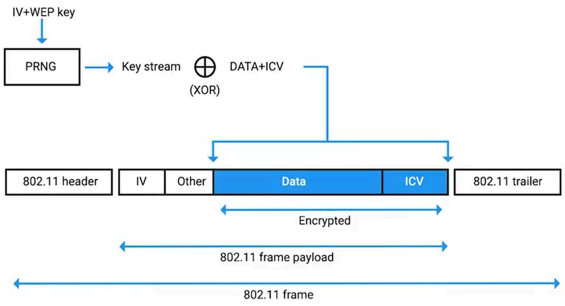
Takes a stream of input and encrypts the stream one character or one digit at a time, outputting one encrypted character or digit at a time.

Block Cipher

The cipher takes data in, places it into a bucket or block of data that's a fixed size, then encodes that entire block as one unit.

Initialization Vector (IV)

If the same key is used to encrypt data two or more times, it's possible to break the cipher, and to recover the plaintext. To avoid key reuse, **initialization vector** or **IV** is used. That's a bit of random data that's integrated into the encryption key, and the resulting combined key is then used to encrypt the data. The idea behind this is, if you have one shared master key, then generate a one time encryption key. That encryption key is used only once by generating a new key using the master one and the IV. In order for the encrypted message to be decoded, the IV must be sent in plain text along with the encrypted message. A good example of this can be seen when inspecting the 802.11 frame of a web encrypted wireless packet.



The IV is included in plain text right before the encrypted data payload.

Symmetric Encryption Algorithms

Data Encryption Standard (DES)
Designed in the 1970s by IBM, with some input from the US National Security Agency
- A symmetric block cipher that uses 64-bit key sizes and operates on blocks 64-bits in size.
- While the key size is 64-bits in length, 8 bits are used only for parity checking (error checking).
    - The real world length for DES is only 56-bits

FIPS
Federal Information Processing Standard

Advanced Encryption Standard (AES)
Adopted by the **National Institute of Standards and Technology (NIST)** in 2001.
- Replaced the **DES**
- Uses 128-bit blocks
- Supports key lengths of 128-bit, 192-bit, or 256-bit.

Rivest Cipher 4 (RC4)
A symmetric stream cipher that gained widespread adoption because of its simplicity and speed.
- Supports key sizes from 40-bits to 2048-bits.
- Supported until 2015 when all versions of TLS dropped RC4 because of inherent weaknesses.

Galois/Counter Mode (GCM)
Takes randomized seed value, incrementing this, and encrypting the value, creating a sequentially numbered blocks of ciphertext.
- The ciphertexts are then incorporated into the plain text to be encrypted.
- TLS 1.2 with AES GCM Is ideal security configuration as of the video recording date, likely 2020.

Supplemental Reading for Symmetric Encryptions

For more information about symmetric encryptions, check out the following link hee.

Asymmetric Cryptography

Asymmetric Ciphers (Public Key Ciphers)
Different keys are used to encrypt and decrypt a message.

- Confidentiality: Granted through the encryption-decryption mechanism.
- Authenticity: Granted by the digital signature mechanism, as the message can be authenticated or verified that it wasn't tampered with.
- Non-repudiation: The author of the message isn't able to dispute the origin of the message.

Asymmetric vs. Symmetric Cryptography

MAC
A bit of information that allows authentication of a received message, ensuring that the message came from the alleged sender and not a third party masquerading as them.

HMAC
A keyed-hash message authentication code.

CMACs
Cipher-Based Message Authentication Codes

CBC-MAC
Cipher block chaining message authentication codes.

Asymmetric Encryption Algorithms

RSA
Patented in 1983 and released to the public domain by RSA Security in 2000
- Named after Ron Rivest, Adi Shamir, and Leonard Alderman

Digital Signature Algorithm (DSA)
Used for signing and verifying data.
- Patented in 1991 and is part of the US government's federal information processing standard.

Diffie-Hellman (DH)
Another popular key exchange algorithm. Often used for a PKI (Public Key Infrastructure) System.
1. First, Suzanne and Darryl agree on the starting number, that would be random and will be a very large integer. This number should be different for every session and doesn't need to be secret.
2. Next, each person chooses another randomized large number, but this one is kept secret. Then, they combine their shared number with their respective secret number and send the resulting mixed number to each other.
3. Next, each person combines their secret number with the combined value they received from the previous step.
4. The result is a new value that's the same on both sides without disclosing enough information to any potential eavesdroppers to figure out the shared secret.

Elliptic Curve Cryptography (ECC)
A public-key encryption system that uses the algebraic structure of elliptic curves over finite fields to generate secure keys.
- Both Diffie-Hellmen and DSA have elliptic curve variants, referred to as ECDH and ECDSA, respectively.

Hashing

Hashing (or a hash function)
A type of function or operation that takes in an arbitrary data input and maps it to an output of fixed size, called a hash or digest.
- The user feeds in any amount of data into a hash function and the resulting output will always be the same size, but the output should be unique to the input, such that two different inputs should never yield the same output.
- Ideal for identifying duplicate data sets in databases to reduce duplicates and save space.

Cryptographic hashing is distinctly different from encryption because cryptographic hash functions should be one directional.

Hash Collisions
Two different inputs mapping to the same output.

Hashing Algorithms

MD5
Popular and widely used hash function designed in 1992 as a cryptographic hashing function.
- Operates on a 512-bit blocks and generates 128-bit hash digest.
- A flaw was detected in 1996, cryptographers recommended using SHA1 after.

SHA1
Part of the Secure Hash Algorithm suite of functions designed by the NSA and published in 1995.
- Operates on a 512-bit blocks and generates 160-bit hash digest.
- Used in popular protocols like TLS/SSL, PGP/SSH, and IPSec.

Message Integrity Check (MIC)
Essentially a hash digest of the message in question. It works like a checksum for the message, ensuring that the contents of the message weren't modified in transit.

Hashing Algorithms (continued)

Brute Force Attacks
Eventually, with enough time and resources, all passwords can be hacked.

Rainbow Table Attacks
Pre-computed tables of passwords

Password Salt
Additional randomized data that's added into the hashing function to generate a hash that's unique to the password and salt combination.

Public Key Infrastructure

PKI is a system that defines the creation, storage, and distribution of digital certificates.

A digital certificate is a file that proves that an entity owns a certain public key.
- Info on Public Key
- Registered Owner
- Digital Signature

Certificate Authority (CA)
The official authoritative body that hands out digital certificates.

Registration Authority (RA)
Responsible for verifying the identities of any entities requesting certificates to be signed and stored with the CA.

Certificates

X.509 Standard
Defines the format of digital certificates, as well as certificate revocation lists, or CRL.
- First issued in 1988, the current version is Version 3.
    - Version
    - Serial Number: Assigned by the CA, lets the CA manage and identify individual certificates.
    - Certificate Signature Algorithm: Indicates the algorithm for the public key and the hashing algorithm used to sign the certificate.
    - Issuer Name: Info on the authority that signed the certification.
    - Validity: "Not Before" and "Not After" dates of validation.
    - Subject: Identifying information about the entity the certificate was issued to.

- Subject Public Key Info: Two subfields that define the algorithm of the public key, along with the public key itself
- Certificate Signature Algorithm: The same as the subject public key and field, and must match.
- Certificate Signature Value: The digital signature data itself.

Web of Trust
Where individuals, instead of certificate authorities, sign other individuals' public keys.

Supplemental Reading for the X.509 Standard

For more information about this topic from this Video Lecture, check out the following link. The X.5029 standard is what defines the format of digital certificates.

Cryptography in Action

TLS Grants the following:

1. A secure communication line, which means data being transmitted is protected from potential eavesdroppers.
2. The ability to authenticate both parties communicating, though typically only the server is authenticated by the client.
3. The integrity of communications, meaning there are checks to ensure that messages aren't lost or altered in transit.

The session key is the shared symmetric encryption key used in TLS sessions to encrypt data being sent back and forth.

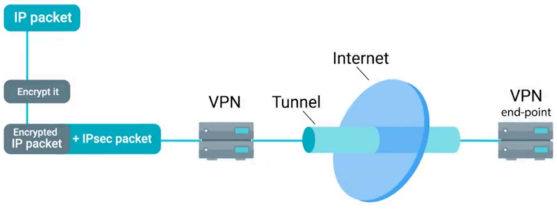
Forward Secrecy
This is a property of a cryptographic system so that even in the event that the private key is compromised, the session keys are still safe.

Pretty Good Privacy (PGP)
An encryption application that allows authentication of data, along with privacy from third parties, relying upon asymmetric encryption to achieve this.
- Most commonly used for encrypted email communication, but also available as a full disk encryption solution or for encrypting arbitrary files, documents, or folders.
- Developed in 1991 by Phil Zimmermann, and was freely available for anyone to use.
- Widely regarded as very secure, with no known mechanisms to break the encryption via cryptographic or computational means.
- It's been compared to military grade encryption.

Securing Network Traffic

VPN
The encrypted tunnel.

IPSec (Internet Protocol Security)
IPsec works by encrypting an IP packet and encapsulating the encrypted packet inside an IPsec packet. This encrypted packet then gets routed to the VPN end-point where the packet is de-encapsulated and decrypted then sent to the final destination.



- **Transport mode**: Where only the payload of the IP packet is encrypted, leaving the IP headers untouched.
- **Tunnel Mode**: The entire IP packet, header and payload and all, is encrypted and encapsulated inside a new IP packet with new headers.

- **L2TP (Layer 2 Tunneling Protocol)**: Typically used to support VPNs, allows for encapsulation of different protocols or traffic over a network that may not support the type of traffic being sent.

Supplemental Reading for Securing Network Traffic

The combination of L2TP and IPsec is referred to as L2TP/IPsec and was officially standardized in IETF RFC 3193.

An example of this is OpenVPN, which uses the OpenSSL library to handle key exchange and encryption of data along with control channels.

Cryptographic Hardware

TPM Chips

A TPM has a unique secret RSA key burned into the hardware at the time of manufacture, which allows a TPM to perform things like hardware authentication.

- Secure generation of keys
- Random number generation
- Remote Attestation: The idea of a system authenticating its software and hardware configuration to a remote system, allowing the remote system to determine the integrity of the remote system.
- Data Binding: Involves using the secret key to derive a unique key that's then used for encryption of data.
- Data Sealing: Where data is encrypted using the hardware backed encryption key.

Secure Element

A tamper resistant chip often embedded in the microprocessor or integrated into the mainboard of a mobile device.

- Provides secure storage of cryptographic keys, and provides a secure environment for applications.

Trusted Execution Environment (TEE)

It provides a full-blown isolated execution environment that runs alongside the main OS.

- Provides isolation of the applications from the main OS and other applications installed there.
- Isolates secure processes from each other when running in the TEE.

Full Disk Encryption (FDE)

- PGP
- Bitlocker
- Filevault 2
- dm-crypt

Supplemental Reading for TPM Attacks

There's been one report of a physical attack on a TPM which allowed a security researcher to view and access the entire contents of a TPM.

Module 3: The 3 A's of Cybersecurity: Authentication, Authorization, Accounting

Best Practices for Authentication

Multifactor Authentication

OTP: One-time password
TOTP: Time-based Token

Windows Hello

U2F: Universal 2nd Factor
- Incorporates a challenge response mechanism along with a public key cryptography.
- Referred to as "Security Keys"

Physical Privacy and Security Components

In this reading, you will learn more about physical privacy and security, including biometric and Near Field Communication authentication. You will also revisit the "confidentiality" aspect of the CIA Principle (Confidentiality, Integrity, Availability), which was introduced previously in this certificate program.

CIA Principle: Confidentiality

Preventing unauthorized access to an organization's data and networks is imperative in protecting a company's information systems. Regulations, standards, and laws may also require that certain information be kept confidential, like health records. Failing to ensure the confidentiality of specific types of data could result in damage to reputation, loss of customers, liability lawsuits, financial losses, penalty fines, criminal charges, and more. It is vital for IT Support specialists to take all measures possible to protect confidential information.

In a previous video, you learned about three types of authentication methods:
- **Something you know** - password or pin number
- **Something you have** - bank card, USB device, key fob, or OTP (one-time password)
- **Something you are** - biometric data, like a fingerprint, voice signature, facial recognition, or retinal scan

You will learn more about biometrics in this reading, along with two additional categories of authentication methods:
- **Somewhere you are** - geofencing, GPS, Indoor Positioning Systems (IPS)
- **Something you do** - gestures, swipe patterns, CAPTCHA, or patterns of behavior

Some authentication technologies inherently require two factors:
- **Somewhere you are + Something you have** - Near Field Communication (NFC) uses both proximity to an NFC scanner and a device like an NFC-enabled smartphone or an RFID chip on an employee ID or bank card.

Something you are: Biometrics

Biometric authentication occurs in two steps: enrollment and authentication. **Enrollment** happens when the user provides their biometric data for the first time through a hardware scanner. Specific features of that biometric data are extracted, encrypted, and stored, often in a database or on a personal mobile device. **Authentication**, as the second step, happens when a user presents their biometric data again to the scanner to gain access to the secured item. This new scan is compared against the original stored biometric data to authenticate the person's identity.

Fingerprint scanning

Fingerprint scanners use small capacitive cells that are engineered to detect fingerprint ridges. Dirt and moisture can interfere with the scanner's ability to do its job. As an IT Support specialist, you may need to replace damaged fingerprint scanners on customer devices.

Facial recognition

Many smartphone models provide the hardware and software to use facial recognition as a biometric authentication method. This often requires two cameras. The first camera uses normal color photography. The second camera uses infrared technology to measure depth and ensure your face is 3-dimensional. This prevents hackers from using photographs of the authorized users to unlock mobile devices.

Iris and Retinal scanning

Iris scanning is not a secure form of biometric authentication because a photograph of the user's iris can be used to gain access. In contrast, retinal scanning is one of the more secure forms of biometric authentication. It is exceedingly difficult to impersonate the retinal features of a person's eye. Our retinas have unique and complex patterns in how our blood vessels are arranged. These fingerprint-like patterns can be scanned by shining a beam of infrared light into the eye. Note that eye injuries and medical problems with the eyes can change retinal blood vessel patterns and cause users to be denied access to their devices. Although retinal scanning is secure, the technology can be expensive and difficult to implement.

Somewhere you are: Geolocation

The geographical location of a user can serve as one part of a multi-factor authentication policy or to deny access to users based on their locations. Geolocation services can use GPS, IP ranges, WiFi access points, cell phone towers, and/or Bluetooth beacons to estimate a mobile user's location.

Geofencing

Geofencing is used to authenticate users who are physically within a certain radius of a specific location. For example, if you order food using McDonald's smartphone app, the restaurant will not process your order until your smartphone is within a certain radius of the restaurant. You cannot send someone else to pick up your order either, as that person cannot authenticate without your smartphone being within the geofencing radius.

Global Positioning Systems (GPS)

Global Positioning Systems (GPS) use satellites orbiting Earth to map a device's longitude and latitude. The mobile device needs to be equipped with GPS sensors and have GPS services enabled to take advantage of GPS-based authentication technologies. GPS could be used to authenticate a device based on the physical location of the user. Insurance companies use GPS data to verify the authenticity of disaster claims filed through mobile apps.

Indoor Positioning Systems (IPS)

Indoor Positioning Systems (IPS) triangulate a device's location by using WiFi access points, cell phone towers, and/or Bluetooth beacons. Users must grant permission to apps to use this technology. IPS locations might be used to deny network access when the user has entered a restricted area.

Near-field communication (NFC) and scanners

You may have interacted with a near-field communication (NFC) scanner by using contactless payments with a credit card, bank card, or smartphone. NFC technology can also be used for authentication and access to physical buildings through school or employment ID cards.

NFC transmits on the same frequency as high frequency RFID (13.56 MHz) and has a short distance range of 10 centimeters. The short distance range provides some protection from hackers attempting to intercept the connection to obtain your credit card information. However, NFC is not fully secure. An innocuous looking NFC scanner sitting next to an NFC-enabled payment device could record all NFC transactions that occur within the 10 cm of the device in a "man in the middle" security breach.

Something you do: Gestures and Behaviors

You may already be familiar with using gestures like swipe patterns to unlock a smartphone. Another gesture-based authentication method is the Picture Password, which requires the user to touch specific, secret points on a photograph to unlock the device.
Patterns of people's behaviors can be used to authenticate identity. For example, an organization might keep track of computer system login and logout times of employees. These patterns could be monitored for any unusual changes in employee behavior, which may indicate that the "employee" is instead an imposter.
Turing tests are used to determine if an unknown entity is a human or a machine. You have probably responded to a **CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)** to authenticate that you are indeed a human and not a bot. This is accomplished by asking the user to identify items within a set of photographs. Photos are used for this test because images are more difficult for bots to identify than text.

Key takeaways

There are a variety of MFA protocols that can be implemented to protect the confidentiality, privacy, and security of data and networks. The 5 types of authentication can be categorized as:

1. Something you know - password or pin number
2. Something you have - bank card, USB device, key fob, or OTP (one-time password)
3. Something you are - biometric data, like a fingerprint, voice signature, facial recognition, or retinal scan
4. Somewhere you are - geolocation, geofencing, GPS, Indoor Positioning Systems (IPS), NFC scanning
5. Something you do - gestures, swipe patterns, CAPTCHA, or patterns of behavior

Resources for more information

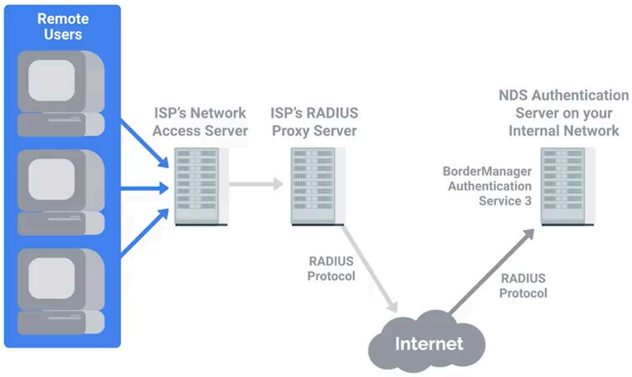
For more information about methods of authentication to protect data, please visit:

- Geolocation—The Risk and Benefits of a Trending Technology - Discusses impacts, benefits, risks, risk mitigation, security, governance, and privacy concerns of geolocation technologies.
- Understanding The 5 Factors Of Multi-Factor Authentication - Overview of the 5 Factors: Something you know, Something you have, Something you are, Somewhere you are, and Something you do.
- Homeland Security Biometrics - History and use cases of biometrics for maximum security and identification of criminals in the United States Departments of Homeland Security, Defense, Justice, and Commerce, as well as the National Institute of Standards and Technology.
- A Review on Authentication Methods - Informative peer-reviewed journal article on authentication methods.
- Modern Authentication Methods: A Comprehensive Survey - Peer-reviewed journal article with expanded coverage of two-factor and multi-factor authentication topics. Provides comprehensive comparisons of advantages and disadvantages of each authentication method.
- What is the Difference Between NFC and RFID? - A comparison of NFC and RFID technologies.
- Fingerprint Reader Replacement Guide - Provides photos of internal fingerprint scanner hardware parts, as well as instructions on how to replace a fingerprint scanner on a laptop.

Certificates, Part 2

RADIUS

A protocol that provides AAA Services → → →



Kerberos

A network authentication protocol that uses "tickets" to allow entities to prove their identity over potentially insecure channels to provide mutual authentication

- Published by MIT in the 1980's as version 4, Version 5 was released in 1993.
- Supports AES encryption and implements check sums to ensure data integrity and confidentiality.
- Windows 2000 and newer use Kerberos as the default authentication protocol.

TACACS+

Terminal Access Controller Access-Control System plus.

- Developed in 1984 for MILNET, the unclassified network for DARPA, which later evolved into NIPRNet.
- Primarily used for device administration, authentication, authorization, and accounting.
- A device access AAA system that manages who has access to your network devices and what they do on them.

Single Sing-On

An authentication concept that allows users to authenticate once to be granted access to a lot of different services and applications.

Authorization and Access Control Methods

Pertains to describing what the user has access to or doesn't have access to.

Mobile Security Methods

Laptop computers, tablets, smartphones, and other mobile devices allow people to remain productive from various locations, such as at home or while traveling. This increased flexibility raises various security concerns that IT departments need to address. This reading provides information about the current security measures used to protect mobile devices.

Common mobile security threats and challenges

Many of the security threats associated with mobile devices are the same as those of traditionally networked devices, such as hacking and malware. However, mobile devices face additional threats that other devices do not.

Here are some threats facing mobile device security:

1. **Phishing**: Phishing attacks can use SMS messaging, email accounts, messages via numerous social media applications, or malicious links in browsers to target your mobile devices.
2. **Malicious applications (malware)**: Malware can take the form of apps designed to collect and transmit personal and corporate information to third parties.
3. **Insecure Wi-Fi and "meddler in the middle" attacks**: An attacker places themself in the middle of two hosts that think they're communicating directly. The attacker may monitor the information from these hosts and potentially modify it in transit. Open or "free" Wi-Fi hotspots are especially susceptible to meddler in the middle and similar attacks.
4. **Poor update habits for devices and apps**: An example is failure to install security patches regularly deployed through software and firmware updates. Unpatched devices and applications often contain exploits and vulnerabilities that attackers may use to collect sensitive data.

You can imagine how all these issues could threaten confidentiality, integrity, or access (the CIA triad)—but confidentiality is of particular concern for mobile security.

Security measures used to protect mobile devices

There are several security measures in place to protect mobile devices from these security concerns.

Screen Locks

Screen locks are methods for preventing unauthorized access to a device. They can be particularly effective for diminishing risks associated with the loss or theft of the device. These measures include:

- **Facial recognition**: uses a device's camera to unlock the device once the user's face is recognized
- **PIN codes**: uses a sequence of four or more numbers to unlock the device
- **Fingerprint recognition**: matches a user's fingerprint with a saved image of the fingerprint to unlock the device
- **Pattern uses**: uses a pattern that users must trace to unlock the device

Remote wipes

Remote wipes are methods to remove data from a device remotely. Remote wiping is another way to diminish risks associated with the loss or theft of a device and include:

- **Locator applications**: apps that help users find lost devices
- **OS updates**: security patches regularly deployed through Operating System updates (as well as firmware and application updates)
- **Device encryption**: encryption techniques that protect the device from unauthorized access
- **Remote backup applications**: apps that allow administrators to remotely remove applications that compromise security
- **Failed login attempt restrictions**: stops access, either completely or for a set period of time, after too many failed attempts to log in
- **Antivirus/Antimalware**: software packages for mobile devices often offered by the same vendors as desktop Antivirus programs
- **Firewalls**: either devices or software that check incoming network traffic and keep out unwanted traffic

Policies and procedures

IT departments establish policies and procedures to ensure users don't make security mistakes. They typically include mobile-specific policies such as acceptable use guidelines, preferred mobile security practices, and security platforms or services.
Once IT staff and management collaborate to build a mobile security policy, there is still work to do. Organizations must find the best way to outline this policy and communicate it to users. A policy is only effective if users understand and adhere to it.

Key takeaways:

As your organization embraces the advantages of mobile devices and wireless networks, your IT security strategies must account for the specific risks, vulnerabilities, and threats associated with mobile computing by:

1. Monitoring for common mobile security concerns such as phishing, malicious applications, insecure Wi-Fi, and poor upgrade habits and applying the current methods for addressing them
2. Implementing security measures to protect mobile devices like screen lock and remote wipes
3. Providing clear mobile security policies and procedures and communicating them to users

Access Control

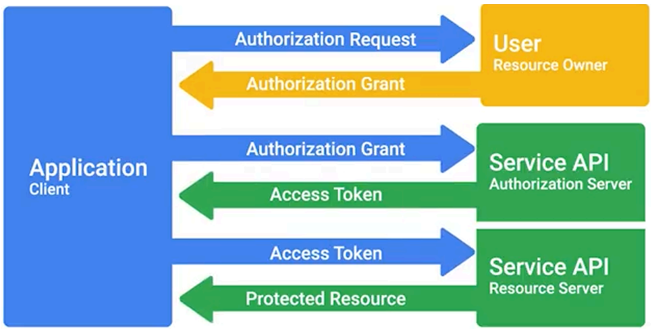
OAuth: An open standard that allows users to grant 3rd-party websites and applications access to their information without sharing account credentials.

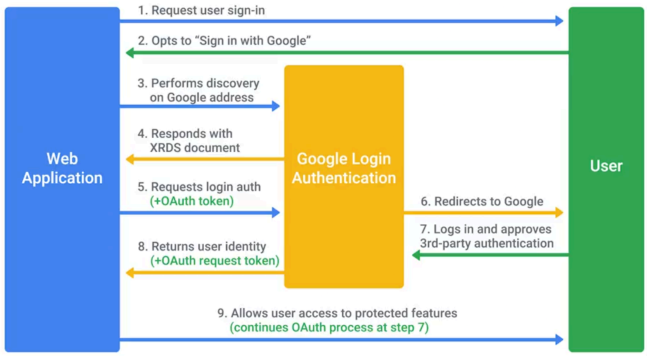
OAuth permissions can be used in phishing-style attacks to gain access to accounts, without requiring credentials to be compromised.

Distinction:
OAuth is specifically an authorization system. →

OpenID is an authentication system. → → → →

OpenID connect is an authentication layer built on top of **OAuth2.0**



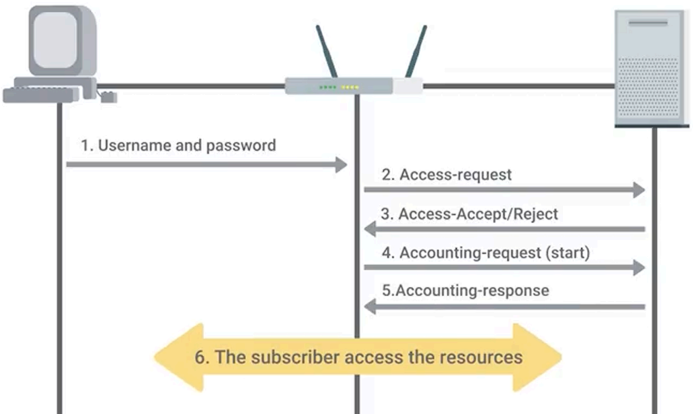


Tracking Usage and Access

Accounting
Keeping records of what resources and services your users accessed, or what they did when they were using your systems.

RADIUS Accounting in action → → → →

1. The **network access server sends** an accounting request packet to the **accounting server** that contains an event record to be logged
2. An accounting session begins **on the server**.
3. The **server replies** with an accounting response indicating that the message was received.
4. The **NAS** will continue sending periodic accounting messages with statistics of the session until an accounting stop packet is received.



Module 4: Securing Your Networks

Network Hardening Best Tools

The process of securing a network by reducing its potential vulnerabilities through configuration changes and taking specific steps.

Implicit Deny
A network security concept where anything not explicitly permitted or allowed should be denied.
- Essentially a “white listing” method.

Analyzing Logs
The practice of collecting logs from different networks and sometimes client devices on your network, then performing an automated analysis on them.

Splunk
A popular and powerful log analysis system, flexible and extensible log aggregation and search system.
- Can be configured to create alerts and allows for powerful visualization of activity based on log data.

Flood Guards
Provide protection against DoS Attacks.

Fail to Ban
A common open-source flood guard protection tool.
- It watches for signs of an attack on a system and blocks further attempts from a suspected attack address.

Supplemental Reading for Network Hardening Best Practices

For more information on this Video Lecture check out the following links:

Cisco IOS firewall rules
Juniper firewall rules
Iptables firewall rules
UFW firewall rules
Configuring Mac OS X firewall
Microsoft firewall rules

Network Hardware Hardening

Rogue DHCP Server Attack
Where a threat actor is able to hand out DHCP leases with whatever information they want.

DHCP Snooping
A feature of Enterprise switches that allows a server to monitor DHCP traffic being sent across it.
- It will also track IP assignments and map them to hosts connected to port switches.

Dynamic ARP Inspection (DAI)
A feature of enterprise switches that prevents ARP snooping attacks.
- Uses DHCP Snooping to evaluate addresses.

802.1X
This is the IEEE standard for encapsulating EAP or Extensible Authentication Protocol traffic over the 802 networks.

EAP-TLS

Supplicant
A Client Device *or* the software running on the client machine that handles the authentication process for the user.

Supplemental Reading on IEEE 802.1X

IEEE 802.1X

When clients are trying to communicate on a local network, the devices must have a standard method of communication and authentication. The Institute of Electrical and Electronics Engineers (IEEE) created a standard called IEEE 802.1X. This standard specifies a common architecture, functional elements, and protocols that support authentication between the clients of ports attached to the same Local Area Network (LAN). This reading will cover what 802.1X is, basic components of authentication and how it works, and different kinds of authentication available for use under the standard.

IEEE 802.1X Protocol

IEEE 802 networks are deployed in locations that provide access to critical data, support mission critical applications, or charge for service. Port-based network access control regulates access to the network, guarding against attacks by unauthorized parties, network disruption, and data loss.

Authentication
The three main components in the authentication process are:

- **Supplicant** is the client making the request to access the LAN or wireless access point.
- **Authenticator** takes the packet from the supplicator and sends it to the authentication server until the session is authenticated. Any other information sent before authentication occurs is dropped.
- **Authentication server** provides a database of information required for authentication, and informs the authenticator to deny or permit access to the supplicant.

Authentication occurs when a client first connects to a network. The client sends a packet of information to the authenticator, which sends the packet to the authentication server. In some instances, the authenticator and authentication server may be integrated into a single point. The authentication server then verifies the identity or key against the information in its database. If the credentials are valid, the authentication succeeds and the server begins processing the connection request. If the credentials are not valid, the authentication fails. The authentication server sends an Access Reject message and the connection request is denied.

Authentication methods

When the request is sent to the authentication server there are a couple of methods for authentication. IEEE defines two different link-level authentication methods:

- **Shared key system** is a shared key or passphrase that is manually set on both the mobile device and the AP/router.
- **Open system** is when the authentication server has a list of authorized clients to check against when a client requests access. This list is usually in the form of MAC addresses but it varies by network.

Shared Key authentication methods

There are several shared key authentication methods that are commonly used:

- **Wired Equivalent Privacy (WEP)** is not recommended for a secure WLAN. The main security risk is hackers capturing the encrypted form of an authentication response frame, using widely available software applications, and using the information to crack WEP encryption.
- **Wi-Fi Protected Access (WPA)** complies with the wireless security standard and strongly increases the level of data protection and access control (authentication) for a wireless network. WPA enforces IEEE 802.1X authentication and key-exchange and only works with dynamic encryption keys.
- **Wi-Fi Protected Access 2 (WPA2)** is a security enhancement to WPA. Users must ensure the mobile device and AP/router are configured using the same WPA version and pre-shared key (PSK).
- **Association** allows the access point or router to record each mobile device so that data is properly delivered. This occurs after authentication is complete.

These authentication methods are standardized under the IEEE 802.1X protocol.

Key takeaways

IEEE 802.1x is a protocol developed to let clients connect to port based networks using modern authentication methods.

- There are three nodes in the authentication process: supplicant, authenticator, and authentication server.
- The authentication server uses either a shared key system or open access system to control who is able to connect to the network.
- Based on the authentication criteria, the authentication server either grants the authentication request and begins the connection process or sends an Access Reject message and terminates the connection.

Network Software Hardening

- HAProxy main documentation
- HAProxy reverse proxy documentation
- nginx main documentation
- nginx reverse proxy documentation
- Apache HTTP server main documentation
- Apache HTTP server reverse proxy documentation

WEP Encryption and Why You Shouldn't Use It

What do you think the best security option is for securing a Wi-Fi network? Some might say WAP3 Enterprise.

- Introduced 1997, no longer used since 2004.
- Never transfer both the plaintext and ciphertext in the same transmission!

Fluhrer S., Mantin I., Shamir A. (2001) Weaknesses in the Key Scheduling Algorithm of RC4. In: Vaudenay S., Youssef A.M. (eds) Selected Areas in Cryptography. SAC 2001. Lecture Notes in Computer Science, vol 2259. Springer, Berlin, Heidelberg https://doi.org/10.1007/3-540-45537-X_1

Let's Get Rid of WEP!

Temporal Key Integrity Protocol (TKIP)
Introduced 3 features to improve security in WAP

1. A more secure key derivation method was used to securely incorporate the IV into the per-packet encryption key.
2. A sequence counter was implemented to prevent replay attacks by rejecting out of order packets.
3. A 64-bit MIC was introduced to prevent forging, tampering, or corruption of packets.

In addition to that, TKIP still used the RC4 cipher as the underlying encryption algorithm.

- It also uses 256-bit long keys

Under WPA, the **pre-shared key** is the Wi-Fi password you share with people when they come over and want to use your wireless network.

WPS
Introduced in 2006.

- PIN Entry Authentication
- NFC or USB
- Push-Button Authentication

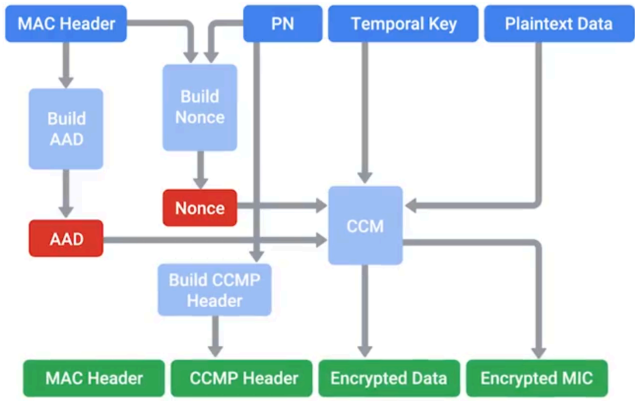
WPA2

CCMP
Counter Mode CBC-MAC Protocol

- Counter with CBC MAC is a particular mode of operation for block ciphers. It allows for authenticated encryption, meaning data is kept confidential and is authenticated.

The Authenticate then Encrypt mechanism:

1. The CBC-MAC Digest is computed first.
2. The resulting authentication code is encrypted along with the message using a block cipher.



Pairwise Master Key (PMK)
A long-lived key that might not change for a long time.

Pairwise Transient Key (PTK)
An encryption key derived from the PMK that's used for actual encryption and decryption of traffic between a client and AP.

- Made up of five individual keys, each with their own purpose.
    - 2 keys are used for encryption and confirmation of EAPoL packets, and the encapsulating protocol carries these messages.
    - 2 keys are used for sending and receiving message integrity codes.
    - The temporal key that is used to encrypt the data.

WPA/WPA2 Enterprise
Adds an 802.1x authentication for Wi-Fi networks.

WPA2-Personal or WPA2-PSK
Non-802.1X configured network security that uses a pre-shared key to authenticate clients.

Supplementary reading on WiFi Protected Setup (WPS) PIN brute force vulnerability

WiFi Protected Setup (WPS) PIN brute force vulnerability

Wireless Hardening

If 802.1X is too complicated for a company, the next best alternative would be WPA2 with AES/CCMP mode.

A long and complex passphrase that wouldn't be found in a dictionary would increase the amount of time and resources an attacker would need to break the passphrase.

If your company values security over convenience, you should make sure that WPS isn't enabled on your APs.

Sniffing the Network

Packet Sniffing (Packet Capture)
The process of intercepting network packets in their entirety for analysis.

Promiscuous Mode
A type of computer networking operational mode in which all network data packets can be accessed and viewed by all network adapters operating in this mode.

Port Mirroring
Allows the switch to take all packets from a specified port, port range, or entire VLAN and mirror the packets to a specified switch port.

Monitor Mode
Allows us to scan across channels to see all wireless traffic being sent by APs and clients.

Open-source Wireless Capture and Monitoring Utilities
- Aircrack-ng
- Kismet

Wireshark and tcpdump

tcpdump
A super popular, lightweight, command-line based utility that you can use to capture and analyze packets.
- Uses open-source libpcap library, a very popular packet capture library that’s used in a lot of packet capture and analysis tools.

Intrusion Detection/Prevention Systems (IDS/IPS)
Systems that operate by monitoring network traffic and analyzing it.

Network Intrusion Detection System (NIDS)
The detection system would be deployed somewhere on a network where it can monitor traffic for a network segment or subnet.

Network Intrusion Prevention System (NIP)
A device that is able to take action against a suspected malicious traffic.

Signatures
Unique characteristics of known malicious traffic. They might be specific sequences of packets or packets with certain values encoded in the specific header field.

Supplemental reading for Intrusion Detection/Prevention System

Snort: https://www.snort.org/
Suricata: https://suricata.io/
The Bro Network Security Monitor has recently been renamed to the Zeek Network Security Monitor: https://www.zeek.org/

Unified Threat Management (UTM)

Previously, you learned about several network security topics, including network hardening best practices, firewall essentials, and the foundations of IEEE 802.1X.

UTM solutions stretch beyond the traditional firewall to include an array of network security tools with a single management interface. UTM simplifies the configuration and enforcement of security controls and policies, saving time and resources. Security event logs and reporting are also centralized and simplified to provide a holistic view of network security events.

UTM options and configurations

UTM solutions are available with a variety of options and configurations to meet the network security needs of an organization:

UTM hardware and software options:

- Stand-alone UTM network appliance
- Set of UTM networked appliances or devices
- UTM server software application(s)

Extent of UTM protection options:

- Single host
- Entire network

UTM security service and tool options can include:

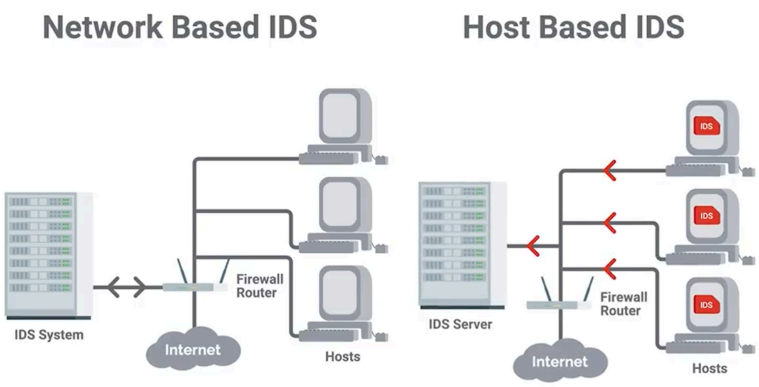
- **Firewall**: Can be the first line of defense in catching phishing attacks, spam, viruses, malware, and other potential threats that attempt to access an organization's network. Firewalls can be hardware devices or software applications. Firewalls filter and inspect packets of data attempting to enter and exit a managed network. Rules can be configured to permit or prevent certain types of packets from entering the network.
- **Intrusion detection system (IDS)**: Passively monitors packets of data and network traffic for unusual patterns that could indicate an attack. IDS devices can monitor entire networks (NIDS) or just a single host (HIDS). IDS identifies, logs, and alerts IT Support about suspicious traffic. However, IDS does not prevent an attack from occurring. This system gives IT Support professionals the opportunity to inspect flagged events to determine how to handle the threat on a case by case basis.
- **Intrusion prevention system (IPS)**: Actively monitors packets and network traffic for potential malicious attacks. IPS systems can be configured to automatically block attacks or to allow manual interventions. IPS devices can monitor entire networks (NIPS) or just a single host (HIPS).
- **Antivirus software**: Uses a signature database to obtain the profiles of malicious files, such as spyware, Trojans, malware, worms, and more. The antivirus software monitors the organization's network and systems for these virus signatures. Once identified, the software will block, quarantine, or destroy them.
- **Anti-malware software**: Scans information streams for known malicious malware signatures and blocks threats. Additionally, anti-malware software can use heuristic analysis to detect novel malware threats by identifying key behaviors and characteristics. The software can also use sandboxing to isolate suspicious files.
- **Spam gateway**: Filters, identifies, and quarantines spam email. Spam gateways are network servers that use Domain Name Server (DNS) management tools to protect against spam.

- **Web and content filters**: Block user access to risky and malicious websites. When a user attempts to access an unauthorized or suspicious website using a browser, the UTM web filter can prevent the website from loading. The filter can also be customized to block certain types of websites or specific URLs, like social media or other websites that might be a distraction in the workplace.
- **Data leak/loss prevention (DLP)**: Monitors outgoing network traffic for personal, sensitive, and confidential data. DLP includes a verification system to determine if the external data transfer is authorized or malicious, and can block unauthorized attempts.
- **Virtual Private Network (VPN)**: Encrypts data and creates a private "tunnel" to safely transmit the data through a public network.

Stream-based vs. proxy-based UTM inspections

UTM solutions offers two methods for inspecting packets in UTM firewalls, IPS, IDS, and VPNs:

- **Stream-based inspection, also called flow-based inspection**: UTM devices inspect data samples from packets for malicious content and threats as the packets flow through the device in a stream of data. This process minimizes the duration of the security inspection, which keeps network data flowing at a faster rate than a proxy-based inspection.



- **Proxy-based inspection**: A UTM network appliance works as a proxy server for the flow of network traffic. The UTM appliance intercepts packets and uses them to reconstruct files. Then the UTM device will analyze the file for threats before allowing the file to continue on to its intended destination. Although this security screening process is more thorough than the stream-based inspection technique, proxy-based inspections are slower in the transmission of data.

Benefits of using UTM

UTM solutions can offer multiple benefits to an organization:

- **UTM can be cost-effective**: Reduces the time and resources needed to manage multiple stand-alone security tools. Purchasing a suite of integrated tools may also be less expensive than buying each tool separately.
- **UTM is flexible and adaptable**: Offers flexible solutions and options for security management. The security services and tools in a UTM can be implemented in any combination that is appropriate for each network environment.
- **UTM offers integrated and centralized management**: Consolidates multiple security tools into a central management console. This simplifies monitoring and addressing security threats, as well as streamlines the management of updates to the UTM components. The central management feature also helps IT Support staff identify and stop the full extent of an attack across an entire network.

Risks of using UTM

- **UTM can become a single point of failure in a network security attack**: If an attack disables an entire UTM solution, there would be no other backup security services or tools to stop that attack. One of the core principles of information systems management is to design and implement redundant, backup, and failover systems. When one element of an IT system is attacked or experiences a failure, there should always be a backup or parallel system to replace it.
- **UTM might be a waste of resources for small businesses**: Small businesses may not need a robust security solution like UTM. The time and money needed to purchase, implement, and manage a complex UTM system may not provide a significant return on security benefits for a smaller network. Cybercriminals are more likely to attack larger targets.

Key takeaways

- Unified Threat Management (UTM) systems offer multiple options in a comprehensive suite of network security tools. UTM solutions can be implemented as hardware and/or software and can protect either a single host or an entire network.
- UTM security services and tool options include firewalls, IDS, IPS, antivirus and anti-malware software, spam gateways, web and content filters, data leak/loss prevention, and VPN services.
- The benefits of using a UTM solution include having a cost-effective network security system that is flexible and adaptable with a management console that is integrated and centralized. The risks of using UTM include creating a single point of failure for a network security system and it might be an unnecessary use of resources for small businesses.

Home Network Security

Employees who work from home use home networks to access company files and programs. Using home networks creates security challenges for companies. Companies can provide employees guidance for protecting their home networks from attacks. This reading will cover common attacks on home networks and steps to make home networks more secure.

Common security vulnerabilities

Home networks have vulnerabilities to various types of attacks. The most common security attacks on home networks include:

- **Meddler in the middle attacks** allows a meddler to get between two communication devices or applications. The meddler then replies as the sender and receiver without either one knowing they are not communicating with the correct person, device, or application. These attacks allow the meddler to obtain login credentials and other sensitive information.
- **Data Theft** is when data within the network is stolen, copied, sent, or viewed by someone who should not have access.
- **Ransomware** uses malware to keep users from accessing important files on their network. Hackers grant access to the files after receiving a ransom payment.

Keeping home networks secure

To protect company data, employees working from home need to take steps to improve the security of their home networks. Home networks can have added protection without expensive equipment or software.

Employees can take steps to keep home networks more secure:

- **Change the default name and password** using the same password guidelines as your company.
- **Limit access to the home network** by not sharing access credentials outside of trusted individuals.
- **Create a guest network** that allows guests to connect to the internet but not your other devices.
- **Turn on WiFi network encryption** requiring a password before a device can access the internet.
- **Turn on the router's firewall** to prevent unwanted traffic from entering or leaving your wireless network without your knowledge. Regularly update your router firmware.
- **Update to the newest WiFi standard** which is the most secure standard for home WiFi.

Another security measure that a company can take is for employees to work over a virtual private network, or VPN. Using a VPN creates an encrypted, secure internet connection through which employees can access company data.

Key takeaways

Home network security is vital to protect a company's sensitive information when employees work from home.

- Data theft, ransomware, and meddler in the middle are common attacks on home networks.
- Employees working from home need to take steps to improve the security of their home networks.

Module 5: Defense in Depth

Intro to Defense in Depth

Defense in Depth
The concept of having multiple, overlapping systems of defense to protect IT systems

Disabling Unnecessary Components

Attack Vector
The method or mechanism by which an attacker or malware gains access to a network or system.

Attack Surface
The sum of all the different attack vectors in a given system.

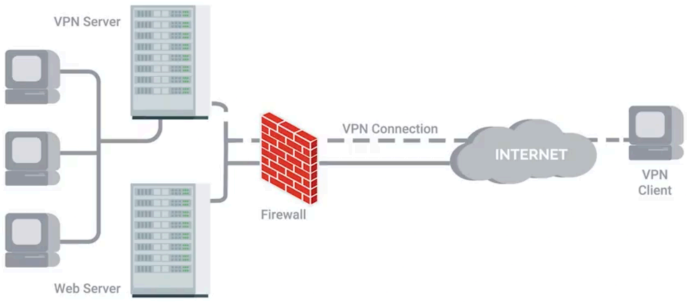
Host-Based Firewalls
Protect individual hosts from being compromised when they're used in untrusted, potentially malicious environments.
- A host-based firewall plays a big part in reducing what's accessible to an outside attacker.

Bastion Hosts/Networks
Specially hardened and minimized to reduce what's permitted to run on them.
- Require special hardening and constant monitoring.
- Monitoring and logging can be prioritized for these hosts more easily.
- Typically have severely limited network connectivity.

It is good practice to keep the network that VPN clients connect into separate using both subnetting and VLANS →

* While adding another server for the VPN clients adds another threat layer to your network, being able to separately monitor traffic coming and going from them is *__highly useful__*.

*Since hosts can effectively change their own firewall rules in their own system, it's a good idea to set up alerts and monitor these settings and changes with logging rules.



*As an administrator in Active Directory, it is good practice to prevent the disabling of the host-based firewall.

Logging and Auditing

Security Information and Event Management Systems (SIEMS)
A centralized log server that holds extra analysis features.

Normalization
The process of taking log data in different formats and converting it into standardized format that's consistent with a defined log structure.

Examples of logging servers and SIEM solutions that are open-source:
- rsyslog (open-source)
- Splunk Enterprise Security
- IBM Security Qradar
- RSA Security Analytics

Microsoft 365 Defender

In this reading, you will learn how Microsoft 365 Defender can be used within an organization for expanded security services and tools. You will also learn about User Account Control (UAC) and its importance in endpoint security.

Microsoft 365 Defender services

Preventing threats across an enterprise environment can be challenging for IT Support professionals. Microsoft 365 Defender can help to simplify this responsibility. Defender provides enterprise-wide security through an integrated suite of tools. It offers tools to prevent attacks, detect threats, investigate security breaches, and coordinate effective response strategies. The Defender portal also offers an action center for monitoring incidents and alerts, as well as for threat hunting and analytics.

Microsoft 365 Defender protection and services include:

- **Defender for Endpoint**: Protects network endpoints including servers, workstations, mobile devices, and IoT devices. Provides preventative safeguards, breach detections, automated analyses, and threat response services.
- **Defender Vulnerability Management**: Protects assets including, hardware, software, licenses, networks, and data. Provides asset inventory, vulnerability discovery, configuration assessment, risk-based prioritization, and remediation tools.
- **Defender for Office 365**: Protects Microsoft 365 (formerly Office 365), including Exchange, Outlook, files, and attachments. Guards against malicious threats entering from email messages, links (URLs), and collaboration tools.
- **Defender for Identity**: Protects user identities and credentials. Detects, identifies, and investigates advanced threats, compromised identities, and malicious actions performed using stolen user identities or by internal threats.
- **Azure Active Directory Identity Protection**: Protects cloud-based identities in Azure by automating detection and resolutions for identity risks.
- **Defender for Cloud Apps**: Protects cloud applications by providing deep visibility searches, robust data controls, and advanced threat protection.

Using Microsoft 365 Defender

As an IT Support professional in an organization, you might use Microsoft 365 Defender to monitor your enterprise's IT security. You can customize the **Defender portal Home page** by job roles. Various security cards can be selected to appear on the Home page for your role. For example, you might see cards for monitoring:

- **Identities**: Monitor user identities for suspicious or risky behaviors.
- **Data**: Track user activity that is risky to data security.
- **Devices**: See alerts, breach activity, and other threats on devices connected to the organization's network.
- **Apps**: Observe how cloud apps are being used in your organization.
- **Incidents**: Review attacks through compiled comprehensive incident data.
- **Alerts**: View alerts compiled from across the Microsoft 365 suite.
- **Advanced hunting**: Scan for suspicious files, malware, and risky activities.
- **Threat Analytics**: View information about current cybersecurity threats.
- **Secure score**: Get a calculated score for your security configuration and recommendations on how to improve your score.
- **Learning hub**: Easily access Microsoft 365 security tutorials and other learning materials.
- **Reports**: Obtain information to help you better protect your organization.

Microsoft 365 Defender aggregates and organizes this monitoring data to provide IT Support professionals details on where attacks began, which malicious tactics were used, the scope of the attacks, and other related incident information.

Microsoft 365 Defender in action

The following are examples of how a cyberattack might penetrate and infect an enterprise network. For each type of malicious attack, a potential Microsoft 365 Defender response follows, illustrating how the security suite could respond:

- **A phishing attempt enters through email**: An employee in an organization receives an email from a business that appears to be legitimate, like a bank. The email might claim that there is a problem with the employee's account and that they must click on a given link to resolve the problem. However, the phishing email actually contains a link to a malicious website that a cybercriminal disguised to look like a real bank. If the employee clicks on the link to view the website, the site requests that the user enter their account credentials or other sensitive information. This information is then transmitted to the cybercriminal.
    - **Microsoft Defender for Office 365** detects the emailed phishing scam by monitoring Exchange and Outlook. Both the employee and the IT Support team are alerted about this attempted phishing attack.

- **Malware enters through social media**: An employee clicks on an enticing link posted on their favorite social media app. The link triggers an automatic download of a malware file to the employee's laptop.
    - **Microsoft Defender for Endpoint** monitors the employee's laptop for suspicious malware signatures. Upon detecting the malware, Defender for Endpoint alerts the employee and the organization's IT Support team about the malware and discloses its endpoint location.

- **A cybercriminal intercepts an employee's work login credentials**: An employee accesses their work account using their laptop and an open Wi-Fi access point in a busy coffee shop. A cybercriminal is in the same coffee shop to intercept and collect unprotected information flowing through the open Wi-Fi access point. The cybercriminal obtains the employee's user account credentials and uses them to hijack the employee's work account. The cybercriminal then begins a malicious attack on the employer's network.
    - **Microsoft Defender for Identity** can detect the sudden change in activity on the employee's user account. Defender for Identity alerts the employee and the IT Support team about the compromised user identity.

- **A virus enters a cloud drive through a file upload**: An employee unknowingly uploads a file that is infected with a virus to their work cloud storage drive. When the employee opens the file from the cloud drive, the virus is activated and begins changing the security settings on the other files in the employee's cloud drive.
    - **Microsoft Defender for Cloud Apps** detects the unusual pattern of activity and alerts the employee and IT Support team of the suspicious activity in the cloud account.

User Account Control (UAC)

User Account Control (UAC) allows IT administrators to create standard user accounts with limited access rights and privileges for end users. This configuration can prevent users from installing unauthorized programs, changing system settings, tampering with firewalls, and more. In order to perform these types of tasks, administrator credentials must be provided. For less restrictive controls, UAC provides the option to grant end users local administrative privileges for approved activities that require administrative privileges. For more restrictive controls, UAC can require global administrator credentials be entered for each and every administrative change the user attempts to make.

– – Continued – –

Resources for more information
To learn more about Microsoft Defender through the Microsoft learning portal, please visit:

- Microsoft Learn: Introduction to Microsoft 365 Defender - Microsoft's self-paced course for Microsoft 365 Defender
- Protect your organization with Microsoft 365 Defender - An interactive guide to Microsoft 365 Defender and how it detects security risks, investigates attacks, and prevents harmful activities.
- Microsoft Defender for Endpoint - Gives an overview of product, services, architecture, and training opportunities.
- Microsoft Defender Vulnerability Management - Provides information about the services and tools available to find and fix vulnerabilities.
- Microsoft Defender for Office 365 - Lists included services and tools for various product levels, as well as the types of threats it protects against.
- Microsoft Defender for Identity - Offers product information, how-to guides, tutorials, and reference information.
- Microsoft Defender for Cloud Apps - Provides product overview, quickstart reference guide, tutorials, best practices, and additional resources.
- How User Account Control works - User Account Control (UAC) is a fundamental component of Microsoft's overall security vision. UAC helps mitigate the impact of malware.

Antimalware Protection

Lots of unprotected systems would be compromised in a matter of minutes if directly connected to the internet without any safeguards or protections in place.

Antivirus software will monitor and analyze things, like new files being created or being modified on the system, in order to watch for any behavior that matches a known malware signature.

There are two issues with antivirus software though:

1. They depend on antivirus signatures distributed by the antivirus software vendor.
2. They depend on the antivirus vendor discovering new malware and writing new signatures for newly discovered threats.

The reason we keep antivirus software: It protects against the most common attacks on the internet.

Antivirus software operates on a "Black List" model.

Binary Whitelisting software operates off a "White List" model.

White List

A known good and trusted software, and only things that are on the list are permitted.

Implicit Deny ACL

Everything is blocked by default

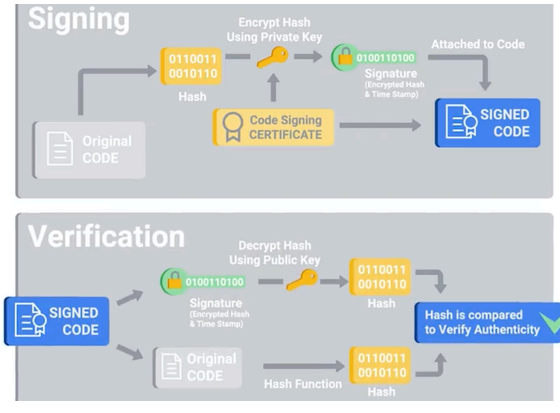
Binary Whitelisting software utilizes several different mechanisms:

1. Using the unique cryptographic hash of binaries which are used to identify unique binaries.
    a. Used to whitelist individual executables.
2. A software signing certificate.

A software vendor can cryptographically sign binaries they →→→ distribute using a private key.

The signature can be verified at execution time by checking the →→ signature using the public key embedded in the certificate and verifying the trust chain of the public key.

If the hash matches and the public key is trusted, then the software can be verified that it came from someone with the software vendor's code signing private key. Binary whitelisting systems can be configured to trust specific vendors code signing certificates.



Supplemental Readings for Antimalware Protection

Learn how long it would take for an unprotected system to be compromised by bots, viruses, and worms in the link here.

If you're interested in why security experts question the value of antivirus software, check out the link here.

If you want to read about how the Sophos antivirus system was maliciously compromised, see the link here.

If you want to learn how hackers bypassed the binary whitelisting defenses that were in place for a software vendor, check out the link here.

Dark Encryption

Full-Disk Encryption (FDE)

Works by automatically converting data on a hard drive into a form that cannot be understood by anyone who doesn't have the key to "undo" the conversation.

- Provides protection from some physical forms of attack.
- Likely to be implemented as an IT Tech.
- Migrating between FDE solutions
- Troubleshoot issues with FDE systems like forgotten passwords.
- Systems with their entire hard drives encrypted are resilient against data theft.

Secure Boot

Uses public key cryptography to secure these encrypted elements of the boot process.

- Does this by **integrated code** signing and verification of the boot files

Platform Key

The public key corresponding to the private key used to sign the boot files.

- Written to firmware and is used at boot-time to verify the signature of the boot files.
- Only files correctly signed and trusted will be allowed to execute.

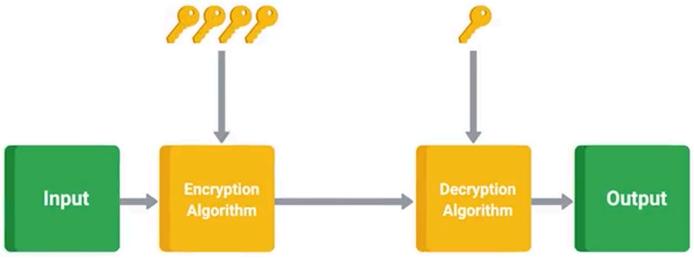
1st Party Full Disk Encryption:

- Apple: File Vault
- Microsoft: BitLocker

3rd Party Full Disk Encryption:

- Linux: dm-crypt
- PGP: https://www.openpgp.org/
- TrueCrypt: https://truecrypt.sourceforge.net/ [Orange Flag]
- FileCrypt: https://github.com/Filecrypt/Filecrypt

Full-Disk Encryption:



Full disk encryption schemes rely on a secret key for actual encryption and decryption operations. They typically password protect access to this key and in some cases the actual encryption key is used to derive a user key which is then used to encrypt the master key.

If the encryption key needs to be changed, the user key can be swapped out without requiring a full decryption and re-encryption of the data being protected. This would be necessary if the master encryption key needs to be changed.

Password protecting the key works by requiring the user entry pass phrase to unlock the encryption key.

Key Escrow
Allows the encryption key to be securely stored for later retrieval by an authorized party.

File-Based Encryption
Where only some files or folders are encrypted and not the entire disk.
- Usually implemented as a **Home Directory**
    - Only guarantees confidentiality and integrity of files protected by encryption.

Browser Hardening

In this reading, you will learn how to harden browsers for enhanced internet security. The methods presented include evaluating sources for trustworthiness, SSL certificates, password managers, and browser security best practices. Techniques for browser hardening are important components in enterprise-level IT security policies. These techniques can also be used to improve internet security for organizations of any size and for individual users.

Identifying trusted versus untrusted sources

Some cybercriminals monitor SEO search terms for popular software downloads. Then they create fake websites to pose as hosts for these popular downloads. They might even use advertising and stolen logos of trusted companies to make the sites appear to be legitimate businesses. However, the downloadable files available on the cybercriminals' websites are usually malicious software. Unaware of the deception, users download and install the malware. In some cases, the users don't even need to download a file. Savvy cybercriminals can design web pages that have the ability to infect users' devices simply upon visiting the sites.

To guard against threats like this, there are checks you can perform to evaluate websites:

- **Use antivirus and anti-malware software and browser extensions**. Run antivirus and anti-malware scans regularly and scan downloaded files. Ensure antivirus and anti-malware browser extensions are enabled when surfing the web.
- **Check for SSL certificates**. See the "Secure connections and sites" section below.
- **Ensure the URL displayed in the address bar shows the correct domain name**. For example, Google websites use the Google.com domain name.
- **Search for negative reviews of the website from trusted sources**. Be wary of websites that have few to no reviews. They may not have been active long enough to build a bad reputation. Cybercriminals will create new websites when they get too many negative reviews on their older sites.
- **Don't automatically trust website links provided by people or organizations you trust**. They may not be aware that they are passing along links to malicious websites and files.
- **Use hashing algorithms for downloaded files**. Compare the developer-provided hash value of the original file to the hash value of the downloaded copy to ensure the two values match.

Secure connections and sites

Secure Socket Layer (SSL) certificates are issued by trusted certificate authorities (CA), such as DigiCert. An SSL certificate indicates that any data submitted through a website will be encrypted. A website with a valid SSL certificate has been inspected and verified by the CA. You can find SSL certificates by performing the following steps:

1. Check the URL in the address bar. The URL should begin with the https:// protocol. If you see http:// without the "s", then the website is not secure.
2. Click on the closed padlock icon in the address bar to the left of the URL. An open lock indicates that the website is not secure.
3. A pop-up menu should open. Websites with SSL certificates will have a menu option labeled "Connection is secure." Click on this menu item.
4. A new pop-up menu will appear with a link to check the certificate information. The layout and wording of this pop-up will vary depending on which browser you are using. When you review the certificate, look for the following items:

    a. The name of the issuer - Make sure it is a trusted certificate authority.
    b. The domain it was issued to - This name should match the website domain name.
    c. The expiration date - The certificate should not have passed its expiration date.

Note that cybercriminals can obtain SSL certificates too. So, this is not a guarantee that the site is safe. CAs also vary in how thorough they are in their inspections.

Password managers

Password managers are software programs that encrypt and retain passwords in secure cloud storage or locally on users' personal computing devices. There are a wide variety of activities users perform online that require unique and complex passwords, such as banking, managing health records, filing taxes, and more. It can be difficult for users to keep track of so many different logins and passwords. Fortunately, password managers can help.

- **Advantages of using a password manager**:
  - It provides only one password for a user to remember;
  - Can generate and store secure passwords that are difficult for cybercriminal tools to crack;
  - Is more secure than keeping passwords written down on paper or in an unencrypted file on a computer; and
  - Works across multiple devices and operating systems.

- **Disadvantages of using a password manager**:
  - It can expose all of the user's account credentials if a cybercriminal obtains the master password to the password manager;
  - Can be very difficult for a user to regain access to the password manager account if the master password is lost or forgotten;
  - Requires the user to learn a new method for logging in to their various accounts in order to retrieve passwords from the password manager software; and
  - Often requires a fee or subscription for password management services.

A few of the top brands for password manager applications include Bitwarden, Last Pass, and 1Password. Please see the Resource section at the end of this reading for more information.

Browser settings

Browser settings can be configured for additional safety measures. Some additional options for hardening browsers include:

1. Use pop-up blockers: Disable Web Browser Pop-up Blockers
2. Clear browsing data and cache: Clear your web browser's cache, cookies, and history
3. Use private-browsing mode: How to Turn on Incognito Mode in Your Browser
4. Sign-in/browser data synchronization:
   a. Turn sync on and off in Chrome
   b. Disable Firefox Sync
   c. Change and customize sync settings in Microsoft Edge
5. Use ad blockers: How to block ads

Key takeaways

You learned about multiple steps you can take to harden a browser and protect your online security:

- Identify if sources can be trusted or not:
  - Use antivirus and anti-malware software and browser extensions.
  - Check for SSL certificates.
  - Ensure the URL displayed in the address bar shows the correct domain name.
  - Search for negative reviews of the website from trusted sources.
  - Don't automatically trust website links provided by people or organizations you trust.

- Use a password manager
  - Configure your browser settings:
  - Use pop-up blockers.
  - Clear browsing data and cache.
  - Use private-browsing mode.
  - Sign-in/browser data synchronization.
  - Use ad blockers.

Resources for more information

To learn more about hardening bowsers for safer web surfing, please visit the following articles:

- Dubious downloads: How to check if a website and its files are malicious - Provides information on evaluating websites and downloads for the presence of malware.
- The Best Password Managers to Secure Your Digital Life - Compares and contrasts the top password managers on the market.
- Avoiding Social Engineering and Phishing Attacks - Tips for avoiding an array of internet scams.
- Blocking Unnecessary Advertising Web Content - From the United States National Security Agency Cybersecurity Information, notice about ad-blocking through network functions, at the host level, and other concerns.
- Securing Web Browsers and Defending Against Malvertising for Federal Agencies - From the United States Cybersecurity and Infrastructure Security Agency, guide for protecting computing systems from malvertising.
- Browser sync—what are the risks of turning it on? - Explains the security threats associated with having browsers set to synchronize account data across multiple devices.
- List of Participants - Microsoft Trusted Root Program - Microsoft's list of trusted Certificate Authorities and the common names of the issued certificates.

Module 6: Creating a company culture for Security

Security Goals

If your company handles credit card payments, you'll have to follow the **PCI DSS**, or **Payment Card Industry Data Security Standard**.

PCI DSS Objectives

1. Build and maintain a secure network and systems.
2. Protect cardholder data.
    a. Protect stored cardholder data.
    b. Encrypt the transmission of cardholder data across open public networks.
3. Maintain a vulnerability management program.
    a. Protect all systems against malware and regularly update antivirus software or programs.
    b. Develop and maintain secure systems and applications.
4. Implement strong Access control measures.
    a. Restrict access to cardholder data by business need to know.
    b. Identify and authenticate access to system components.
    c. Restrict physical access to cardholder data.
5. Regularly monitor and test networks
    a. Track and monitor all access to network resources and cardholder data.
    b. Regularly test security systems and processes.

Measuring and Assessing Risk

Security is all about determining **risks** or exposure: understanding the likelihood of **attacks**; and designing **defenses** around these risks to minimize the impact of an attack.

Security risk assessment starts with **Threat modeling**.

Vulnerability Scanner

A computer program designed to assess computers, computer systems, networks or applications for weaknesses.

- Ideal to run these often
- Open-source and commercial solutions:
    - Nessus
    - OpenVAS
    - Qualys

Penetration Testing

The practice of attempting to break into a system or network to verify the systems in place.

Privacy Policy

These oversee the access and use of sensitive data. Both privacy and data access policies are important to guiding and informing people how to maintain security while handling sensitive data.

Auditing data access logs is very important. Apply the principle of **lease privilege** here, by not allowing access to this type of data by default.

Any access that doesn't have a corresponding request should be flagged as a **high-priority potential breach** that needs to be investigated as soon as possible.

Data-handling policies should cover the details of how different data is classified.

Data Destruction

Data destruction is removing or destroying data stored on electronic devices so that an operating system or application cannot read it. Data destruction is required when a company no longer needs a device, when there are unused or multiple copies of data, or you are required to destroy specific data.

There are three categories of data destruction methods: recycling, physical destruction, and third-party destruction. This reading will introduce the data destruction methods and how to decide which method to use.

Recycling

Recycling includes methods that allow for device reuse after data destruction. This option is recommended if you hope to reuse devices internally, sell surplus equipment, or your devices are on loan and are due to be returned. Standard recycling methods include the following:

- **Erasing/wiping**: cleans all data off a device's hard drive by overwriting it. Erasing or wiping data can be done manually or with data-destruction software. This method is practical when you only have a few devices that need data destroyed, as it takes a long time. Note that it may take multiple passes to wipe highly sensitive data completely.
- **Low-level formatting**: erases all data written on the hard drive by replacing it with zeros. Low-level reformatting can be done using a tool such as HDDGURU on a PC or the Disk Utility function on a Mac.
- **Standard formatting**: erases the path to the data and not the data itself. Both PCs and Macs have internal tools that can perform a standard format, Disk Management on a PC or Disk Utility on a Mac. Note that standard formatting does not remove the data from the device, enabling data rediscovery using software.

Physical destruction

Physical destruction includes any method that physically destroys a device to make it difficult to retrieve data from it. You should only use physical destruction if you do not need to reuse the device. However, only completely destroying the device ensures the destruction of all data with physical methods. Physical destruction methods include the following:

- **Drilling holes** directly into the device wipes data out on the sections where there are holes. However, individuals can recover data from the areas that are still intact.
- **Shredding** includes the physical shredding of hard drives, memory cards, CDs, DVDs, and other electronic storage devices. Shredding reduces the potential for recovery. Shredding requires special equipment or outsourcing to another facility.
- **Degaussing** uses a high-powered magnet which destroys the data on the device. This method effectively destroys large data storage devices and renders the hard drive unusable. As electronic technology changes, this method may become obsolete
- **Incinerating** destroys data by burning the device. Most companies do not have an incinerator on-site. Devices need to be transported to a facility for incineration. Due to this, devices can be lost or stolen in transit.

In addition to effectively destroying data on electronic devices, it is essential to follow best practices for electronic device disposal.

Outsourcing

Outsourcing means using a third-party specializing in data destruction to complete the physical or recycling process. This option appeals to companies that do not have the staff or knowledge to complete the destruction themselves. Once a vendor has completed the task, they issue a certificate of destruction/recycling.

The certificate of destruction serves as a statement of completed destruction of data on electronics, hard drives, or other devices. The certificate includes the client's contact information, date of service, vendor company name, manifest, signature, method of destruction, and legal statement. However, exercise caution as the certificate does not indicate a level of training, auditing, or any other verification that a vendor is knowledgeable about data destruction.

Key Takeaways

Data destruction makes data unreadable to an operating system or application. You should destroy data on devices no longer used by a company, unused or duplicated copies of data, or data that's required to destroy. Data destruction methods include:

- **Recycling**: erasing the data from a device for reuse
- **Physical destruction**: destroying the device itself to prevent access to data
- **Outsourcing**: using an external company specializing in data destruction to handle the process

Resource for further information

For more information about disposing of electronics, please visit Proper Disposal of Electronic Devices, a resource from CISA.

User Habits

You should never upload confidential information onto a 3rd-party service that hasn't been evaluated by your company.

To help prevent password phishing, check out tools like Password Alert.

Incident Reporting and Analysis

The very first step of handling an incident is to **detect it**.

The next step is to **analyze it** and **determine the effects** and **scope** of damage.

- Data leak?
- Information disclosure?
- Was it malware?

Once the scope of the incident has been determined, the next step is **containment**.

Data Exfiltration

The unauthorized transfer of data from a computer.

Recoverability

How complicated and time consuming the recovery effort will be.

Incident Response

When you've had a data breach, you may need forensic analysis to analyze the attack. This analysis usually involves extensive evidence gathering. This reading covers some considerations for protecting the integrity of your forensic evidence and avoiding complications or issues related to how you handle evidence.

Regulated data

It's important to consider the type of data involved in an incident. Many types of data are subject to government regulations that require you to take extra care when handling it. Here are some examples you're likely to encounter as an IT support specialist.

– – Continued – –

1. **Protected Health Information**: This information is regulated by the Health Insurance Portability and Accountability Act (HIPAA). It is personally identifiable health information that relates to:

- Past, present, or future physical or mental health or condition of an individual
- Administration of health care to the individual by a covered provider (for example, a hospital or doctor)
- Past, present, or future payment for the provision of health care to the individual

2. **Credit Card or Payment Card Industry (PCI) Information**: This is information related to credit, debit, or other payment cards. PCI data is governed by the Payment Card Industry Data Security Standard (PCI DSS), a global information security standard designed to prevent fraud through increased control of credit card data.

3. **Personally Identifiable Information (PII)**: PII is a category of sensitive information associated with a person. Examples include addresses, Social Security Numbers, or similar personal ID numbers.

4. **Federal Information Security Management Act (FISMA) compliance**: FISMA requires federal agencies and those providing services on their behalf to develop, document, and implement specific IT security programs and to store data on U.S. soil. For example, organizations like NASA, the National Institutes of Health, the Department of Veteran Affairs—and any contractors processing or storing data for them—need to comply with FISMA.

5. **Export Administration Regulations (EAR) compliance**: EAR is a set of U.S. government regulations administered by the U.S. Department of Commerce's Bureau of Industry and Security (BIS). These regulations govern the export and re-export of commercial and dual-use goods, software, and technology. Dual-use goods are items that can be used both for civilian and military applications. These goods are heavily regulated because they can be classified for civilian use and then transformed for military purposes.

Digital rights management (DRM)

Digital Rights Management (DRM) technologies can help ensure data regulations compliance. DRM technology comes in the form of either software or hardware solutions. Both options allow content creators to prevent deliberate piracy and unauthorized usage. DRM often involves using codes that prohibit content copying or limit the number of devices that can access a product. Content creators can also use DRM applications to restrict what users can do with their material. They can encrypt digital media so only someone with the decryption key can access it. This gives content creators and copyright holders a way to:

- **Restrict users** from editing, saving, sharing, printing, or taking screenshots of content or products
- **Set expiration dates** on media to prevent access beyond that date or limit the number of times users can access the media
- **Limit access** to specific devices, Internet Protocol (IP) addresses, or locations, such as limiting content to people in a specific country

Organizations can use these DRM capabilities to protect sensitive data. DRM enables organizations to track who has viewed files, control access, and manage how people use the files. It also prevents files from being altered, duplicated, saved, or printed. DRM can help organizations comply with data protection regulations.

End User Licensing Agreement (EULA)

End User Licensing Agreements (EULAs) are similar to DRM in specifying certain rights and restrictions that apply to the software. You often encounter EULA statements when installing a software package, accessing a website, sharing a file, or downloading content. A EULA is usually considered a legally binding agreement between the owner of a product (e.g., a software publisher) and the product's end-user. The EULA specifies the rights and restrictions that apply to the software, and it's usually presented to users during installation or setup of the software. You can't complete an installation (or access, share, or download data) until you agree to the terms written in the EULA statement.

Unlike DRM restrictions, EULAs are only valid if you agree to it (i.e., you check a box or click the 'I Agree' button). DRM restrictions don't require your agreement—or rely on you to keep that agreement. DRMs are built into the product they protect, making it easier for content creators to ensure users do not violate restrictions.

Chain of custody

"Chain of custody" refers to a process that tracks evidence movement through its collection, safeguarding, and analysis lifecycle. Maintaining the chain of custody makes it difficult for someone to argue that the evidence was tampered with or mishandled. Your chain of custody documentation should answer the following questions.

Documentation for these questions must be maintained and filed in a secure location for current and future reference.

1. **Who collected the evidence?** Evidence can include the afflicted or used devices, media, and associated peripherals.
2. **How was the evidence collected, and where was it located?**
3. **Who seized and possessed the evidence?**
4. **How was the evidence stored and protected in storage?** The procedures involved in storing and protecting evidence are called **evidence-custodian procedures**.
5. **Who took the evidence out of storage and why?** Ongoing documentation of the names of individuals who check out evidence and why must be kept.

When a data breach occurs, forensic analysis usually involves taking an image of the disk. This makes a virtual copy of the hard drive. The copy lets an investigator analyze the disk's contents without modifying or altering the original files. An alteration compromises the integrity of the evidence. This kind of compromised integrity is what you want to avoid when performing forensic investigations.

Key takeaways:

Incident handling requires careful attention and documentation during an incident investigation's analysis and response phases.

- Be familiar with what types of regulated data may be on your systems and ensure proper procedures are in place to ensure your organization's compliance.
- DRM technologies can be beneficial for safeguarding business-critical documents or sensitive information and helping organizations comply with data protection regulations.
- When incident analysis involves the collection of forensic evidence, you must thoroughly document the chain of custody.

Incident Response and Recovery

Update firewall rules and ACLs if an exposure was discovered in the course of the investigation.

Create new definitions and rules for intrusion detection systems that can watch for the signs of the same attack again.

Mobile Security and Privacy

Screen Lock

Presents a challenge that requires a correct response to unlock the device.

Permissions

Mobile OSs allow the user to control what permissions an app will have to different aspects of the user's personal and/or private data.

Supplemental Readings for Mobile Security and Privacy
Check out the following links for more info:

- Set screen lock on an Android device
- Change access to items when iPhone is locked
- Use a passcode with your iPhone, iPad, or iPod touch
- Control your app permissions on Android 6.0 and up
- Change app access to private data

Bring Your Own Device

In this reading, you will learn about a business practice called "bring your own device" (BYOD), as well as the security risks related to BYOD policies and how to mitigate these risks. Organizations can reduce IT costs by limiting the number of company-owned mobile devices issued to employees. Instead, businesses are passing on the costs of mobile devices and cellular services to employees by allowing employees to bring their own devices for business use.

Bring your own device (BYOD)

Traditionally, IT departments would provide mobile devices to employees for business use. This gave the IT staff control over the security of those devices. Today, an increasing number of companies permit employees to bring their own devices to work. This trend started with employees requesting permission to carry a single smartphone rather than carrying one phone for work and one for personal use. Organizations noticed the cost savings gained by allowing their employees to select their personal smartphones as the single device. By using smartphones with dual SIM card slots or phone apps like Google Voice, users can configure multiple phone lines on a single smartphone. However, BYODs can become dangerous security threats to companies' data and networks. IT departments do not have the same level of control over the security of BYOD devices as they would with company-owned devices.

BYOD Threats

Some of the potential threats BYODs pose to company networks, resources, and data include:

- **Loss or theft** could result in an organization's data being stolen or the lost device being used to gain unauthorized access to a company's network.
- **Data loss**, including:

    1. **Data leakage** losses can happen when a computing device is lost or compromised; when an employee accidentally saves or sends confidential information to the wrong destination; when a disgruntled employee exposes data maliciously; or when viruses, malware, phishing attacks, etc. penetrate organizations' networks.
    2. **Data portability** losses can occur when former employees take company data with them on their BYOD when they resign or are fired by the organization.

- **Security vulnerabilities** are any type of weakness in the security of a device or network that provides access for a threat to penetrate the system.
- **Meddler in the middle attacks (MITM)** occur when an attacker monitors the data transfers between two sources with the intent to copy and/or interfere with that information. One of the most common opportunities for an MITM attack arises when a mobile device accesses important information through a public Wi-Fi connection, such as at a hotel or restaurant.
- **Malware** is malicious software that can be used to steal, modify, or delete data. It can also be used to gain unauthorized access to a device or network.
- **Jailbreaking** happens when a manufacturer's protective restrictions are removed on a mobile device. Without these restrictions, a device becomes vulnerable to the risk of the user unknowingly installing malicious software.

Solutions

To mitigate these threats, organizations and their IT departments should design security policies for BYOD use inside company networks. Some preventative steps could include:

- **Develop a bring your own device (BYOD) policy**: IT departments and organizations can create written policies that detail the minimum technology requirements for permitted BYODs, provide instructions for employees on how to properly secure their devices, and list the rules for safe data access and storage.

- **Use Mobile Device Management (MDM) software**: MDM software can be used to enforce BYOD policy requirements for mobile devices to help secure company data and networks. IT departments can use MDM software to:

    a. Automatically install apps and updates, including antivirus and anti-malware software
    b. Configure secure connections to an organization's wireless networks
    c. Encrypt storage on devices
    d. Require a lock screen and password
    e. Remote wipe a mobile device that is lost or stolen
    f. Block the execution of certain apps
    g. Meet compliance standards
    h. Prevent data being shared or stored in unauthorized locations
    i. Manage devices remotely

- **Use an Enterprise Mobile Management (EMM) system**: MDM policies are specific to mobile operating systems. In order to distribute MDM policies across Android, iOS, and other mobile operating systems, the BYODs can be enrolled through an Enterprise Mobility Management (EMM) system.

- **Require the use of multi-factor authentication (MFA)**: Users can be authenticated by presenting more than one method of identification. Some common identification factors include:

    a. **Something you know**: a password or pin number
    b. **Something you have**: a physical token, like an ATM or bank card, USB device, key fob, or OTP (one-time password)
    c. **Something you are**: biometric data, like a fingerprint, voice signature, facial recognition, or retina scan
    d. **Somewhere you are**: location-dependent access, like a Global Positioning System (GPS) location
    e. **Something you do**: gestures, like swipe patterns; Turing tests, like CAPTCHA; or normal patterns of behavior, like regular login and logout times

- **Set an acceptable use policy (AUP)**: Organizations could create policies that set a code of conduct for use of the companies' data, systems, network, and other resources.

- **Use non-disclosure agreements (NDA)**: Organizations can create legally binding contracts with employees to assert the confidentiality and security policies for the companies' data and intellectual property.

- **Restrict data access**: IT departments should protect company data by limiting access to only those employees who need access to perform their jobs.

- **Educate staff about data security**: Organizations can provide training manuals and seminars to inform employees about network security risks and to instruct on how to secure their BYODs.

- **Back up device data**: IT departments need to create backup policies for all important data. This should include a schedule for frequency of backups, storage space for the back-up copies, how long back-ups should be stored, and disaster recovery plans.

- **Data leakage prevention (DLP)**: IT departments can implement DLP software solutions to help manage and protect confidential information.

Key takeaways

Organizations are taking advantage of the cost savings created by adopting “bring your own device” (BYOD) policies for employees. However, permitting employees to connect personal mobile devices to company networks introduces multiple security threats. There are a variety of security measures that IT departments can implement to protect organizations’ information systems:

- Develop BYOD policies
- Enforce BYOD policies with MDM software
- Distribute MDM settings to multiple OSes through EMM systems
- Require multi-factor authentication (MFA)
- Create acceptable use policies for company data and resources
- Require employees to sign NDAs
- Limit who can access data
- Train employees on data security
- Back up data regularly
- Resources for more information

Resources for more information

- BYOD (bring your own device) - Additional information on how BYOD works, why is it important, level of access options, risks, challenges, policy comparisons, best practices, how to implement a BYOD policy.
- BYOD policy: An in-depth guide from an IT leader - Compares BYOD advantages and disadvantages, what should be included in a BYOD policy, tips for reducing security risks, and more.
- What is MDM? - Introduces the purpose of MDM software, how it works, advantages of using MDM, use cases, and more.
- Enterprise Mobility Management (EMM) - Outlines the features, services, and benefits of EMM systems.

Final Project

Organization requirements: As the security consultant, the company needs you to add security measures to the following systems:

- An external website permitting users to browse and purchase widgets
- An internal intranet website for employees to use
- Secure remote access for engineering employees
- Reasonable, basic firewall rules
- Wireless coverage in the office
- Reasonably secure configurations for laptops

What you'll do: You'll create a security infrastructure design document for a fictional organization. Your plan needs to meet the organization's requirements and the following elements should be incorporated into your plan:

- Authentication system
- External website security
- Internal website security
- Remote access solution
- Firewall and basic rules recommendations
- Wireless security
- VLAN configuration recommendations
- Laptop security configuration
- Application policy recommendations
- Security and privacy policy recommendations
- Intrusion detection or prevention for systems containing customer data

To meet the high needs of the company's design and deployment, the first thing that needs to be established are mitigated foundations for each service that is being introduced to the company's resources. To begin, we'll need to build a local proxy server where our public-facing interfaces will have Enterprise level malware and antivirus software as a first defense for the entire network, provided by a trusted 3rd party. I would suggest we utilize a company called eset, as that would allow us the added ability to implement VPN connections on each employee's devices, from PCs and Laptops to cellphones on our plans, while also offering a premium cybersecurity defense layer to our network. The proxy server should also be configured on a managed switch.

A secondary and third server that is filtered past the proxy server should serve as a perfect host for each External and Internal website, respectively. Compartmentalizing these two smaller servers should make monitoring easier, and should allow a safety net in the case that one server is infected by a threat actor.

Building on the security concerns, there should be a dedicated NAS on the network, on a separate VLAN from the other servers. I would recommend the following setup:

60TB RAID 10 split between 3x 20TB drives dedicated to backups of client data, with heavy access control via Active Directory OUs.
40TB RAID 0 split between 2x 20TB drives dedicated to the wireless security network
60TB RAID 10 split between 3x 20TB drives dedicated to Employee data and shared folders

Each RAID drive should be mapped on a different VLAN for security and group policy configurations.

For the wireless access within the company's physical location, I would recommend we utilize a wide mesh setup with a lot of low-powered APs so we can set a balance between speed and accessibility with security in mind. Employee interfaces as well as guest isolated interfaces should all have a WPA3 rated password to secure all connections, and the employee network should remain hidden from being searchable.

Lastly, it would be ideal if each department created a list of programs and websites they like to use for their work so we can create a repository of safe pre-configured images of the base computer in the event we need to add employees or restore a lost/damaged device. This solution will increase the efficiency of the IT department, allowing it to utilize time resources in other needed areas and to focus on company security. This list will also help make a more concise set of firewall rules going forward, making it easier for employees to access approved 3rd-party sites for their business related needs.

Final Project - Sample Submission

Authentication
Authentication will be handled centrally by an LDAP server and will incorporate One-Time Password generators as a 2nd factor for authentication.

External Website
The customer-facing website will be served via HTTPS, since it will be serving an e-commerce site permitting visitors to browse and purchase products, as well as create and log into accounts. This website would be publically accessible.

Internal Website
The internal employee website will also be served over HTTPS, as it will require authentication for employees to access. It will also only be accessible from the internal company network and only with an authenticated account.

Remote Access
Since engineers require remote access to internal websites, as well as remote command line access to workstations, a network-level VPN solution will be needed, like OpenVPN. To make internal website access easier, a reverse proxy is recommended, in addition to VPN. Both of these would rely on the LDAP server that was previously mentioned for authentication and authorization.

Firewall
A network-based firewall appliance would be required. It would include rules to permit traffic for various services, starting with an implicit deny rule, then selectively opening ports. Rules will also be needed to allow public access to the external website, and to permit traffic to the reverse proxy server and the VPN server.

Wireless
For wireless security, 802.1X with EAP-TLS should be used. This would require the use of client certificates, which can also be used to authenticate other services, like VPN, reverse proxy, and internal website authentication. 802.1X is more secure and more easily managed as the company grows, making it a better choice than WPA2.

VLANs
Incorporating VLANs into the network structure is recommended as a form of network segmentation; it will make controlling access to various services easier to manage. VLANs can be created for broad roles or functions for devices and services. An engineering VLAN can be used to place all engineering workstations and engineering services on. An Infrastructure VLAN can be used for all infrastructure devices, like wireless APs, network devices, and critical servers like authentication. A Sales VLAN can be used for non-engineering machines, and a Guest VLAN would be useful for other devices that don't fit the other VLAN assignments.

Laptop Security
As the company handles payment information and user data, privacy is a big concern. Laptops should have full disk encryption (FDE) as a requirement, to protect against unauthorized data access if a device is lost or stolen. Antivirus software is also strongly advised to avoid infections from common malware. To protect against more uncommon attacks and unknown threats, binary whitelisting software is recommended, in addition to antivirus software.

Application Policy
To further enhance the security of client machines, an application policy should be in place to restrict the installation of third-party software to only applications that are related to work functions. Specifically, risky and legally questionable application categories should be explicitly banned. This would include things like pirated software, license key generators, and cracked software.

In addition to policies that restrict some forms of software, a policy should also be included to require the timely installation of software patches. “Timely” in this case will be defined as 30 days from the wide availability of the patch.

User Data Privacy Policy
As the company takes user privacy very seriously, some strong policies around accessing user data are a critical requirement. User data must only be accessed for specific work purposes, related to a particular task or project. Requests must be made for specific pieces of data, rather than overly broad, exploratory requests. Requests must be reviewed and approved before access is granted. Only after review and approval will an individual be granted access to the specific user data requested. Access requests to user data should also have an end date.

In addition to accessing user data, policies regarding the handling and storage of user data are also important to have defined. These will help prevent user data from being lost and falling into the wrong hands. User data should not be permitted on portable storage devices, like USB keys or external hard drives. If an exception is necessary,

an encrypted portable hard drive should be used to transport user data. User data at rest should always be contained on encrypted media to protect it from unauthorized access.

Security Policy
To ensure that strong and secure passwords are used, the password policy below should be enforced:

Password must have a minimum length of 8 characters

Password must include a minimum of one special character or punctuation

Password must be changed once every 12 months

In addition to these password requirements, a mandatory security training must be completed by every employee once every year. This should cover common security-related scenarios, like how to avoid falling victim to phishing attacks, good practices for keeping your laptop safe, and new threats that have emerged since the last time the course was taken.

Intrusion Detection or Prevention Systems
A Network Intrusion Detection System is recommended to watch network activity for signs of an attack or malware infection. This would allow for good monitoring capabilities without inconveniencing users of the network. A Network Intrusion Prevention System (NIPS) is recommended for the network where the servers containing user data are located; it contains much more valuable data, which is more likely to be targeted in an attack. In addition to Network Intrusion Prevention, Host-based Intrusion Detection (HIDS) software is also recommended to be installed on these servers to enhance monitoring of these important systems.

Module 7: Streamline Workflows with AI

Introduction to AI for IT Support

In the fast-paced world of IT support, providing timely and effective assistance requires leveraging the latest technology. AI tools are transforming the way IT support professionals work, offering powerful capabilities to streamline ticket management, automate communications, and proactively monitor systems.

Artificial intelligence (AI) refers to computer programs that can complete cognitive tasks typically associated with human intelligence. You can use AI tools to augment and automate general IT support tasks, such as drafting responses to common inquiries, summarizing technical information, and helping to triage support tickets.

In this lesson, you'll discover how you can integrate AI into your daily IT support activities. We'll explore how AI is already being used by IT support professionals to help automate routine tasks, enhance productivity, and improve the overall user experience.

Throughout this lesson, you will:

- Learn foundational concepts of AI.
- Discover AI tools used in the IT support field.
- Review examples of how AI is used in the day-to-day work of a Google IT support professional.
- Gain hands-on practice in using AI to streamline your tasks.

As you begin your career as an IT professional, this lesson will give you the basic information you need to experiment with AI tools, identify opportunities for leveraging AI in your IT support role, and keep up to date with industry changes.

Support and maintain AI systems

As AI systems become more commonly used in professional fields, it will be part of your job as an IT professional to maintain and protect those systems for your organization. AI systems are complex and rely on large quantities of high-quality data to operate well. For that reason, it's helpful to understand what qualities make AI systems unique and challenges they may present for you as an IT professional. AI systems are unique because they are:

- **Intricate**: Many AI systems are complex, making it hard to understand how they work. For this reason, troubleshooting issues and diagnosing errors may be more difficult with AI systems. However, developing expertise about the architecture of AI can set you apart as an IT professional who knows how to address difficult issues with IT systems.
- **Iterative**: Unlike traditional software, AI systems constantly iterate, or change, so the behavior of the system may vary over time, making it difficult to maintain documentation and predict future issues. This is why it's important for you to stay up-to-date with the latest AI technologies, as well as updates to existing AI technologies.
- **Data dependent**: The performance of an AI system depends on the quality and quantity of its training data. As an IT professional, you will maintain this data. For example, you will likely need to determine where the data is stored and how it's secured.
- **Cybersecurity targets**: Because AI systems rely on a lot of high-quality data to operate, they can become the targets of cybersecurity attacks from malicious actors. AI systems might require additional security measures and expertise to protect them. As an IT professional, you should understand potential attack vectors, as well as how to implement robust defenses, so that you can integrate these technologies safely within your organization's existing systems.
- **Complicated to integrate**: Making sure AI systems work with existing IT infrastructure can be difficult, requiring compatibility checks and adjustments to workflows. This can be particularly challenging when you need to integrate AI systems with legacy systems. But by developing your expertise with AI technologies, you can help your organization integrate AI systems and stay at the forefront of innovation.

Because many of these challenges are unique to AI systems, you will need to develop additional skills as an IT professional. Fortunately, the AI tools themselves can help you do that. AI tools can help you research information about AI, troubleshoot unique errors, and create documentation to reference in the future. As you continue to learn about how AI can be used in IT automation, consider how you can leverage AI tools to help you overcome challenges you might encounter as an IT professional.

Use generative AI to work smarter and faster

In the introductory reading you learned that AI refers to computer programs that can complete cognitive tasks typically associated with human intelligence. One specific type of AI is generative AI (gen AI), which is AI that can generate new content, like text, images, or other media. Gemini, ChatGPT by OpenAI, and Microsoft Copilot are examples of generative AI tools. **You can interact with a generative AI tool by entering a prompt**, which is input that provides instructions to an AI tool about how to generate output. The tool then creates new content based on that prompt.

In your work as an IT support professional, you can leverage generative AI tools to help you complete both practical and creative tasks. Consider these applications of generative AI tools that can help you work more efficiently and effectively:

- **Create content**. You can use generative AI tools to generate text, images, and other media. For example, you might create knowledge base articles, troubleshooting guides, or user training materials.
- **Analyze information quickly**. Generative AI tools can analyze large amounts of content quickly. For example, you might use generative AI to summarize system logs, error reports, or user feedback, helping you identify and diagnose issues more efficiently.
- **Answer questions in detailed and nuanced ways**. Generative AI is effective at summarizing information, which makes it useful for research. For example, you can prompt a generative AI tool to provide you with information about specific software issues, hardware compatibility, or network configurations.
- **Simplify day-to-day work**. You can also use generative AI to augment routine tasks. For example, AI tools can help you draft responses to common user inquiries, automate ticket routing, or even suggest potential solutions to technical problems.

In the upcoming series of videos you will be introduced to Nathalia, an IT support professional working at Google. Nathalia will introduce you to the ways that she incorporates AI into her daily workflows to do things like communicate technical concepts more easily, troubleshoot IT issues, and more.

The ways you might use generative AI in your work will likely go beyond these examples as the capabilities of AI tools expand, and as you continue your own development as an IT support professional.

Boost your IT Support Skills with AI

Specify the Task

- Task: What action do you want the tool to help you with?
    - Persona: What expertise do you want the AI tool to draw from and who is the audience?

Provide Necessary Contex

- Reasons and objectives for performing the task
- Rules or guidelines that the output must follow
- Relevant background information the tool should consider

Include References as Examples

- Briefly explain how the references relate to the task
- Use 2-5 High-Quality examples that closely align with your needs
- Include your own work or open-source examples if relevant

Evaluate Your Output

- Accuracy
- Bias
- Relevancy
- Consistency

Iterate for Better Results

- You provide an initial prompt.
- The AI tool responds with an output.
- You evaluate the effectiveness of the AI-generated response.
- You refine your request based on what worked and what didn't.
- The cycle repeats until you produce the desired results.

Role	"You are a professional chef.
Task	Write an easy-to-follow recipe for a classic pasta dish.
Context	The dish should be simple to prepare and beginner-friendly.
Target audience	For busy college students who want a quick, nutritious meal.
Style	Use a friendly, encouraging tone with simple language.
Format	Provide the recipe in bullet points with each step numbered, including a short list of ingredients and estimated prep or cook time."

ChatGPT Handbook "Formula" 🔝

Automate Routine Tasks with AI

Tips for Iteration

- Provide more specific guidance to get what you need.
- Share examples of what you were expecting.
- Use clear phrasing and short sentences.
- Explain why you like or didn't like the output.

Key Takeaways for AI in IT Support

Resources for more information

If you're interested in learning more, please visit the following resources:

- Introducing Google's Secure AI Framework: Explore key elements of Google's Secure AI Framework (SAIF) and learn how Google is actively using and supporting SAIF.
- Science & Tech Spotlight: Generative AI: Discover why generative AI systems matter in today's world in this article by the U.S. Government Accountability Office (GAO).
- There's More to AI Bias Than Biased Data, NIST Report Highlights: Examine the risks involved when bias is present in AI data and recommendations for mitigating these risks, based on research performed by the National Institute of Standards and Technology (NIST), U.S. Department of Commerce.
- What is Artificial Intelligence (AI)?: Explore Google Cloud's introduction to AI, including other cases when AI can be used, such as in speech and image recognition.

– fin –

Glossary

IT Support

Terms and definitions from Course 5

#

802.1X: It is the IEEE standard for encapsulating EAP or Extensible Authentication Protocol traffic over the 802 networks

802.1X with EAP-TLS: Offers arguably the best security available, assuming proper and secure handling of the PKI aspects of it

A

Access Control Entries: The individual access permissions per object that make up the ACL

Access Control List (ACL): It is a way of defining permissions or authorizations for objects

Accounting: Keeping records of what resources and services your users access or what they did when they were using your systems

Activation threshold: Triggers a pre-configured action when it is reached and will typically block the identified attack traffic for a specific amount of time

Advanced Encryption Standard (AES): The first and only public cipher that's approved for use with top secret information by the United States National Security Agency

Adware: Software that displays advertisements and collects data

Analyzing logs: The practice of collecting logs from different network and sometimes client devices on your network, then performing an automated analysis on them

Antivirus software: It monitors and analyze things like new files being created or being modified on the system in order to watch for any behavior that matches a known malware signature

Application policies: Defines boundaries of what applications are permitted or not, but they also help educate folks on how to use software more securely

Asymmetric encryption: Systems where different keys are used to encrypt and decrypt

Attack: An actual attempt at causing harm to a system

Attack surface: It's the sum of all the different attack vectors in a given system

Attack vector: Method or mechanism by which an attacker or malware gains access to a network or system

Auditing: It involves reviewing records to ensure that nothing is out of the ordinary

Authentication: A crucial application for cryptographic hash functions

Authentication server (AS): It includes the user ID of the authenticating user

Authorization: It pertains to describing what the user account has access to or doesn't have access to

Availability: Means that the information we have is readily accessible to those people that should have it

B

Backdoor: A way to get into a system if the other methods to get in a system aren't allowed, it's a secret entryway for attackers

Baiting: An attack that happens through actual physical contact, enticing a victim to do something

Bastion hosts or networks: A server used to provide access to a private network from an external network

Binary whitelisting software: It's a list of known good and trusted software and only things that are on the list are permitted to run

Biometric authentication: Authentication that uses Biometric data

Bind: It is how clients authenticate to the server

Botnet: A collection of one or more Bots

Bots: Machines compromised by malware that are utilized to perform tasks centrally controlled by an attacker

Block ciphers: The cipher takes data in, places that into a bucket or block of data that's a fixed size, then encodes that entire block as one unit

Brute force attacks: A common password attack which consists of just continuously trying different combinations of characters and letters until one gets access

C

CA (Certificate authority): It's the entity that's responsible for storing, issuing, and signing certificates. It's a crucial component of the PKI system

Caesar cipher: A substitution alphabet, where you replace characters in the alphabet with others usually by shifting or rotating the alphabet, a set of numbers or characters

CBC-MAC (Cipher block chaining message authentication codes): A mechanism for building MACs using block ciphers

CCMP (counter mode CBC-MAC protocol): A mode of operation for block ciphers that allows for authenticated encryption

Central repository: It is needed to securely store and index keys and a certificate management

system of some sort makes managing access to storage certificates and issuance of certificates easier
Certificate-based authentication: It is the most secure option, but it requires more support and management overhead since every client must have a certificate
Certificate fingerprints: These are just hash digests of the whole certificate, and aren't actually fields in the certificate itself, but are computed by clients when validating or inspecting certificates
Certificate Revocation List (CRL): A means to distribute a list of certificates that are no longer valid
Certificate Signature Algorithm: This field indicates what public key algorithm is used for the public key and what hashing algorithm is used to sign the certificate
Certificate Signature Value: The digital signature data itself
CIA Triad: Confidentiality, integrity, and availability. Three key principles of a guiding model for designing information security policies
Client certificates: They operate very similarly to server certificates but are presented by clients and allow servers to authenticate and verify clients
CMACs (Cipher-based Message Authentication Codes): The process is similar to HMAC, but instead of using a hashing function to produce a digest, a symmetric cipher with a shared keys used to encrypt the message and the resulting output is used as the MAC
Code signing certificates: It is used for signing executable programs and allows users of these signed applications to verify the signatures and ensure that the application was not tampered with

Confidentiality: Keeping things hidden
Correlation analysis: The process of taking log data from different systems, and matching events across the systems
Counter-based tokens: They use a secret seed value along with the secret counter value that's incremented every time a one-time password is generated on the device
Cross-site scripting (XSS): A type of injection attack where the attacker can insert malicious code and target the user of the service
Cryptanalysis: Looking for hidden messages or trying to decipher coded message
Cryptographic hashing: It is distinctly different from encryption because cryptographic hash functions should be one directional
Cryptography: The overarching discipline that covers the practice of coding and hiding messages from third parties
Cryptology: The study of cryptography
Cryptosystem: A collection of algorithms for key generation and encryption and decryption operations that comprise a cryptographic service
D
Data binding and sealing: It involves using the secret key to derive a unique key that's then used for encryption of data
Data exfiltration: The unauthorized transfer of data from a computer. It's also a very important concern when a security incident happens
Data handling policies: Should cover the details of how different data is classified
Data information tree: A structure where objects will have one parent and can have one or more children that belong to the parent object
Decryption: The reverse process from encryption; taking the garbled output and transforming it back into the readable plain text
Defense in depth: The concept of having multiple overlapping systems of defense to protect IT systems
Denial-of-Service (DoS) attack: An attack that tries to prevent access to a service for legitimate users by overwhelming the network or server
DES (Data Encryption Standard): One of the earliest encryption standards

Deterministic: It means that the same input value should always return the same hash value
DH (Diffie-Hellman): A popular key exchange algorithm, named for its co-inventors
Dictionary attack: A type of password attack that tries out words that are commonly used in passwords, like password, monkey, football
Distinguished name (DN): A unique identifier for each entry in the directory
Distributed Denial-of-Service (DDoS) attack: A DoS attack using multiple systems
DNS Cache Poisoning Attack: It works by tricking a DNS server into accepting a fake DNS record that will point you to a compromised DNS server
DSA (Digital Signature Algorithm): It is another example of an asymmetric encryption system, though its used for signing and verifying data
Dynamic ARP inspection (DAI): A feature on enterprise switches that prevents certain types of attacks
E
EAP-TLS: One of the more common and secure EAP methods
ECDH & ECDSA: Elliptic curve variants of Diffie-Hellman and DSA, respectively

Eliptic curve cryptography (ECC): A public key encryption system that uses the algebraic structure of elliptic curves over finite fields to generate secure keys
Encapsulating security payload: It's a part of the IPsec suite of protocols, which encapsulates IP packets, providing confidentiality, integrity, and authentication of the packets
Encryption: The act of taking a message (plaintext), and applying an operation to it (cipher), so that you receive a garbled, unreadable message as the output (ciphertext)
Encryption algorithm: The underlying logic or process that's used to convert the plaintext into ciphertext
End-entity (leaf certificate): A certificate that has no authority as a CA
Entropy pool: A source of random data to help seed random number generators
Entry point: the act to determine the entry point to figure out how the attacker got in, or what vulnerability the malware exploited
Evil twin: The premise of an evil twin attack is for you to connect to a network that is identical to yours but that is controlled by an attacker. Once connected to it, they will be able to monitor your traffic

Exploit: Software that is used to take advantage of a security bug or vulnerability
Extensible authentication protocol (EAP over LAN, or EAPOL): A standard authentication protocol
F
Fail to ban: A common open source flood guard protection tool
File-based encryption: Guarantees confidentiality and integrity of files protected by encryption
FIPS (Federal Information Processing Standard): The DES that was adopted as a federal standard for encrypting and securing government data
Flood guards: Provide protection against DoS or Denial of Service Attacks
Forward secrecy: This is a property of a cryptographic system so that even in the event that the private key is compromised, the session keys are still safe
Four-Way Handshake: It is designed to allow an AP to confirm that the client has the correct pairwise master key in a WPA-PSK setup without disclosing the PMK
Frequency analysis: The practice of studying the frequency with which letters appear in ciphertext
Full disk encryption (FDE): It is the practice of encrypting the entire drive in the system
G
GTK (Groupwise Transient Key): A temporal key, which is actually used to encrypt data
H
Hacker: Someone who attempts to break into or exploit a system
Half-open attacks: A way to refer to SYN floods
Hash collisions: Two different inputs mapping to the same output
Hashing (Hash function): A type of function or operation that takes in an arbitrary data input and maps it to an output of a fixed size, called a hash or a digest
High value data: usually includes account information, like usernames and passwords. Typically, any kind of user data is considered high value, especially if payment processing is involved

HMAC (Keyed-Hash Message Authentication Codes): It uses a cryptographic hash function along with a secret key to generate a MAC
Host-based firewalls: Protects individual hosts from being compromised when they're used in untrusted and potentially malicious environments
HTTPS: It is the secure version of HTTP, the Hypertext Transfer Protocol
Hubs: Devices that serve as a central location through which data travels through; a quick and dirty way of getting packets mirrored to your capture interface
Identification: The idea of describing an entity uniquely
Impact: The impact of an incident is also an important issue to consider
Implicit deny: A network security concept where anything not explicitly permitted or allowed should be denied
Injection attacks: A common security exploit that can occur in software development and runs rampant on the web, where an attacker injects malicious code
Integrity: Means keeping our data accurate and untampered with
Intermediary (subordinate) CA: It means that the entity that this certificate was issued to can now sign other certificates
Intrusion detection and intrusion protection systems (IDS/IPS): Operates by monitoring network traffic and analyzing it
IPsec (Internet Protocol security): A VPN protocol that was designed in conjunction with IPv6
IP source guard (IPSG): It can be enabled on enterprise switches along with DHCP snooping
Issuer Name: This field contains information about the authority that signed the certificate
J

K
Kerberos: A network authentication protocol that uses tickets to allow entities to prove their

identity over potentially insecure channels to provide mutual authentication
Kerckhoff's principle: A principle that states that a cryptosystem, or a collection of algorithms for key generation and encryption and decryption operations that comprise a cryptographic service should remain secure, even if everything about the system is known except for the key

Key: A crucial component of a cipher, which introduces something unique into your cipher
Key escrow: Allows encryption key to be securely stored for later retrieval by an authorized party
Key length: It defines the maximum potential strength of the system
Key signing parties: Organized by people who are interested in establishing a web of trust, and participants perform the same verification and signing
Key size: It is the total number of bits or data that comprises the encryption key
Keylogger: A common type of spyware that's used to record every keystroke you make
L
Lightweight Directory Access Protocol (LDAP): An open industry-standard protocol for accessing and maintaining directory services
Logic bomb: A type of Malware that's intentionally installed
Logs analysis systems: They are configured using user-defined rules to match interesting or atypical log entries
L2TP (Layer 2 Tunneling Protocol): It is typically used to support VPNs
M
MACs (Message Authentication Codes): A bit of information that allows authentication of a received message, ensuring that the message came from the alleged sender and not a third party masquerading as them
Malware: A type of malicious software that can be used to obtain your sensitive information or delete or modify files
MD5: A popular and widely used hash function designed in the early 1990s as a cryptographic hashing function
Meddler in the middle (formerly known as Man in the Middle): An attack that places the attacker in the middle of two hosts that think they're communicating directly with each other
MIC (Message Integrity Check): It is essentially a hash digest of the message in question
Monitor mode: It allows to scan across channels to see all wireless traffic being sent by APs and clients

Multifactor authentication (MFA): A system where users are authenticated by presenting multiple pieces of information or objects
N
Network hardening: Is the process of securing a network by reducing its potential vulnerabilities through configuration changes, and taking specific steps
Network separation (network segmentation): A good security principle for an IT support specialists to implement. It permits more flexible management of the network, and provides some security benefits. This is the concept of using VLANs to create virtual networks for different device classes or types
Network software hardening: Includes things like firewalls, proxies, and VPNs
Network time protocol (NTP): A network protocol used to synchronize the time between the authenticator token and the authentication server
NIST: National Institute of Standards and Technology
Normalization: It's the process of taking log data in different formats and converting it into a standardized format that's consistent with a defined log structure
O
OAuth: An open standard that allows users to grant third-party websites and applications access to their information without sharing account credentials
One-time password (OTP): A short-lived token, typically a number that's entered along with a username and password
One-time password (OTP) tokens: Another very common method for handling multifactor
OpenID: An open standard that allows participating sites known as Relying Parties to allow authentication of users utilizing a third party authentication service
Organizational units (OUs): Folders that let us group related objects into units like people or groups to distinguish between individual user accounts and groups that accounts can belong to
P
Packet sniffing (packet capture): the process of intercepting network packets in their entirety for analysis

Pairwise Transient Key (PTK): It is generated using the PMK, AP nonce, Client nonce, AP MAC address, and Client MAC address
Password attacks: Utilize software like password crackers that try and guess your password
Password salt: Additional randomized data that's added into the hashing function to generate the hash that's unique to the password and salt combination
PBKDF2 (Password Based Key Derivation Function 2): Password Based Key Derivation

Function 2
PCI DSS: Payment Card Industry Data Security Standard
Penetration testing: The practice of attempting to break into a system or network to verify the systems in place
PGP (Pretty Good Privacy) encryption: An encryption application that allows authentication of data along with privacy from third parties relying upon asymmetric encryption to achieve this
Phishing attack: It usually occurs when a malicious email is sent to a victim disguised as something legitimate
Physical tokens: They take a few different forms, such as a USB device with a secret token on it, a standalone device which generates a token, or even a simple key used with a traditional lock
PIN authentication method: It uses PINs that are eight-digits long, but the last digit is a checksum that's computed from the first seven digits
Ping flood: It sends tons of ping packets to a system. If a computer can't keep up with this, then it's prone to being overwhelmed and taken down
PKI system: A system that defines the creation, storage and distribution of digital certificates
Platform key: It's the public key corresponding to the private key used to sign the boot files
Port mirroring: Allows the switch to take all packets from a specified port, port range, or the entire VLAN and mirror the packets to a specified switch port
Post-fail analysis
Pre-shared key: It's the Wi-Fi password you share with people when they come over and want to use your wireless network
Principle of least privilege: Helps to ensure that sensitive data is only accessed by people who are authorized to access it
Privacy policies: Oversees the access and use of sensitive data

Promiscuous mode: A type of computer networking operational mode in which all network data packets can be accessed and viewed by all network adapters operating in this mode
Proxy: Can be useful to protect client devices and their traffic. They also provide secure remote access without using a VPN
Pseudo-random: Something that isn't truly random
Public key authentication: A key pair is generated by the user who wants to authenticate
Public key signatures: Digital signature generated by composing the message and combining it with the private key
Q
R
RA (Registration Authority): It is responsible for verifying the identities of any entities requesting certificates to be signed and stored with the CA
Rainbow table attacks: To trade computational power for disk space by pre-computing the hashes and storing them in a table
Rainbow tables: A pre-computed table of all possible password values and their corresponding hashes
Random numbers: A very important concept in encryption because it avoids some kind of pattern that an adversary can discover through close observation and analysis of encrypted messages over time
Ransomware: A type of attack that holds your data or system hostage until you pay some sort of ransom
RC4 (Rivest Cipher 4): Asymmetric stream cipher that gained widespread adoption because of its simplicity and speed
Recoverability: How complicated and time-consuming the recovery effort will be
Remote attestation: The idea of a system authenticating its software and hardware configuration to a remote system
Remote Authentication Dial-in User Service (RADIUS): A protocol that provides AAA services for users on a network
Reverse proxy: A service that might appear to be a single server to external clients, but actually represents many servers living behind it

Risk: The possibility of suffering a loss in the event of an attack on the system
Risk mitigation: Understanding the risks your systems face, take measures to reduce those risks, and monitor them
Rogue Access Point (AP) Attack: An access point that is installed on the network without the network administrator's knowledge
Rogue DHCP server attack: An attacker can hand out DHCP leases with whatever information they want by deploying a rogue DHCP server on your network, setting a gateway address or DNS server, that's actually a machine within their control
Root certificate authority: They are self signed because they are the start of the chain of trust, so there's no higher authority that can sign on their behalf
Rootkit: A collection of software or tools that an admin would use
RSA: One of the first practical asymmetric cryptography systems to be developed, named for

the initials of the three co-inventors: Ron Rivest, Adi Shamir and Leonard Adleman

S
Screen lock: A security feature that helps prevent unwanted access by creating an action you have to do to gain entry
Secure boot protocol: It uses public key cryptography to secure the encrypted elements of the boot process
Secure channel: It is provided by IPsec, which provides confidentiality, integrity, and authentication of data being passed
Secure element: It's a tamper resistant chip often embedded in the microprocessor or integrated into the mainboard of a mobile device
Secure Shell (SSH): A secure network protocol that uses encryption to allow access to a network service over unsecured networks
Security: It's all about determining risks or exposure understanding the likelihood of attacks; and designing defenses around these risks to minimize the impact of an attack
Security information and event management systems (SIEMS): Form of centralized logging for security administration purposes
Security keys: Small embedded cryptoprocessors, that have secure storage of asymmetric keys and additional slots to run embedded code

Security through obscurity: The principle that if no one knows what algorithm is being used or general security practices, then one is safe from attackers
Seed value: A secret value that is used to initialize a process that is generated by software using one or more values
Self-signed certificate: This certificate has been signed by the same entity that issued the certificate
Serial number: A unique identifier for their certificate assigned by the CA which allows the CA to manage and identify individual certificates
Session hijacking (cookie hijacking): A common meddler in the middle attack
Session key: The shared symmetric encryption key using TLS sessions to encrypt data being sent back and forth
Severity: Includes factors like what and how many systems were compromised and how the breach affects business functions
SHA1: It is part of the secure hash algorithm suite of functions, designed by the NSA and published in 1995

Shannon's maxim: It states that the system should remain secure, even if your adversary knows exactly what kind of encryption systems you're employing, as long as your keys remain secure
Single Sign-on (SSO): An authentication concept that allows users to authenticate once to be granted access to a lot of different services and applications
Social engineering: An attack method that relies heavily on interactions with humans instead of computers
Software signing certificate: Trust mechanism where a software vendor can cryptographically sign binaries they distribute using a private key
Spear phishing: Phishing that targets individual or group - the fake emails may contain some personal information like your name, or the names of friends or family
Spoofing: When a source is masquerading around as something else
Spyware: The type of malware that's meant to spy on you
SQL Injection Attack: An attack that targets the entire website if the website is using a SQL database
SSL 3.0: The latest revision of SSL that was deprecated in 2015

SSL/TLS Client Certificate: Certificates that are bound to clients and are used to authenticate the client to the server, allowing access control to a SSL/TLS service
SSL/TLS Server Certificate: A certificate that a web server presents to a client as part of the initial secure setup of an SSL, TLS connection
StartTLS: It permits a client to communicate using LDAP v3 over TLS
Steganography: The practice of hiding information from observers, but not encoding it
Stream ciphers: It takes a stream of input and encrypts the stream one character or one digit at a time, outputting one encrypted character or digit at a time
Subject: This field contains identifying information about the entity the certificate was issued to
Subject Public Key Info: These two subfields define the algorithm of the public key along with the public key itself
Substitution cipher: An encryption mechanism that replaces parts of your plaintext with ciphertext
Symmetric key algorithm: Encryption algorithms that use the same key to encrypt and decrypt messages
SYN flood: The server is bombarded with SYN packets

T
TACACS+: It is a device access AAA system that manages who has access to your network devices and what they do on them
Tailgating: Gaining access into a restricted area or building by following a real employee in
Tcpdump: It's a super popular, lightweight command-line based utility that you can use to capture and analyze packets
Threat: The possibility of danger that could exploit a vulnerability
Threats & password policies: Protects Data & IP, Data Protection, Infrastructure Defense, Identity Management, and users
Ticket granting service (TGS): It decrypts the Ticket Granting Ticket using the Ticket Granting Service secret key, which provides the Ticket Granting Service with the client Ticket Granting Service session key
Time-based token (TOTP): A One-Time-Password that's rotated periodically
TKIP (Temporal Key Integrity Protocol): To address the shortcomings of WEP security

TLS 1.2: The current recommended revision of SSL
TLS 1.2 with AES GCM: A specific mode of operation for the AES block cipher that essentially turns it into a stream cipher
TLS Handshake: A mechanism to initially establish a channel for an application to communicate with a service
TPM (Trusted Platform Module): This is a hardware device that's typically integrated into the hardware of a computer, that's a dedicated crypto processor
Transport mode: One of the two modes of operations supported by IPsec. When used, only the payload of the IP packet is encrypted, leaving the IP headers untouched
Trojan: malware that disguises itself as one thing but does something else
Trusted execution environment (TEE): It provides a full-blown isolated execution environment that runs alongside the main OS
Tunnel: It is provided by L2TP, which permits the passing of unmodified packets from one network to another
Tunnel mode: One of the two modes of operations supported by IPsec. When used, the entire IP packet, header, payload, and all, is encrypted and encapsulated inside a new IP packet with new headers
U
Unbind: It closes the connection to the LDAP server
Username and password authentication: Can be used in conjunction with certificate authentication, providing additional layers of security
U2F (Universal 2nd Factor): It's a standard developed jointly by Google, Yubico and NXP Semiconductors that incorporates a challenge-response mechanism, along with public key cryptography to implement a more secure and more convenient second-factor authentication solution
V
Validity: This field contains two subfields, Not Before and Not After, which define the dates when the certificate is valid for
Vendor risk review: Questionnaire that covers different aspects of their security policies procedures and defenses
Version: What version of the X.509 standard certificate adheres to

Viruses: The best known type of malware
VPN (Virtual Private Network): A secure method of connecting a device to a private network over the internet
VPNs: Commonly used to provide secure remote access, and link two networks securely
Vulnerability: A flaw in the system that could be exploited to compromise the system
Vulnerability scanner: Detect lots of things, ranging from misconfigured services that represent potential risks, to detecting the presence of back doors and systems

W
Web of trust: It is where individuals instead of certificate authorities sign other individuals' public keys
WEP (Wired Equivalent Privacy): First security protocol introduced for Wi-FI networks
Wireshark: It's another packet capture and analysis tool that you can use, but it's way more powerful when it comes to application and packet analysis, compared to tcpdump
Worms: They are similar to viruses except that instead of having to attach themselves onto something to spread, worms can live on their own and spread through channels like the network
WPA (Wi-fi protected access): Designed as a short-term replacement that would be compatible with older WEP-enabled hardware with a simple firmware update
WPA2 Enterprise: It's an 802.1x authentication to Wi-Fi networks
WPS (Wifi Protected Setup): It's a convenience feature designed to make it easier for clients to join a WPA-PSK protected network

X

X.509 standard: It is what defines the format of digital certificates, as well as a certificate revocation list or CRL

XTACACS: It stands for Extended TACACS, which was a Cisco proprietary extension on top of TACACS

Y

Z

0-Day Vulnerability (Zero Day): A vulnerability that is not known to the software developer or vendor, but is known to an attacker