# Unit 32, Assignment 1

Are we Safe?

George Hotten

April 20, 2023

# Network Attacks

**Spoofing** A spoofing attack is where an attacker impersonates a user or system to gain unauthorized access to a network. Spoofing attacks often take form in main-in-the-middle attacks where criminals intercept and modifies packets flowing between two devices. Another example of spoofing is impersonating a free Wi-Fi access point and intercepting traffic from unsuspecting users attempting to steal their information.

**Mathematical** A mathematical attack uses vulnerabilities in cryptographic algorithms to crack encryption and gain unauthorized access to data. This is done by using advanced mathematical techniques to reverse engineer a cryptographic algorithm to gain access to encrypted data which is typically personal information.

**Software Exploitation** A software exploitation attack is where an attacker uses a vulnerability in a software application or an operating system to gain unauthorized access to a system. This is often done by injecting malicious code into memory by using an exploit such as a buffer overflow. This attack is often used to steal data or to open a back door into a system to allow the criminal to take it over.

**Rootkit** A rootkit is a type of malware designed to be difficult to detect by users and antiviruses. They are often embedded deep inside a system making them difficult to detect, and they are used to steal data and launch other similar attacks.

**Brute Force** A brute force attack is where an attacker tries every possible combination to a password-protected system to gain unauthorized access. This is often used to guess passwords and encryption keys. Running a brute force attack can be very time-consuming and is typically only successful on short or weak keys.

**Backdoor** A backdoor attack is where an attacker has installed a hidden entry point into a system which allows them unauthorized access to a system, bypassing all security measures. Backdoors are often installed through malware and other entry points such as rootkits and software exploits. Backdoors are often used to steal data or surveil what a user is doing.

## Sources of Attacks

**Cyber Criminal** Cyber criminals are individuals or groups who target individuals and organizations with cyber crimes and network attacks. These criminals are typically motivated by political opinions and views, and financial gain. Cyber criminals tend to use techniques such as phishing, social engineering and malware to gain unauthorized access to a network. The criminals target personal data, passwords and other sensitive data.

**Insiders** Insiders are individuals who have access to a network system for legitimate reasons, but abuse their access by performing malicious actives. An insider is often a current or former employee and partners who have access to systems containing sensitive information. Insiders are usually motivated by financial gain or by revenge. Insider attacks are usually harder to detect as their access to the system is authorized, meaning no warning alerts are triggered.

**Nation-State Actors** Nation-state actors are groups that are government-sponsored or are a part of the government that carry out cyberattacks for strategical and political gain. These actors are often motivated by espionage, stealing critical information and disrupting infrastructure. These attacks are often highly targeted and use techniques such as advanced persistent threats.

# Recent Network Attacks

## Cash App, April 2022

In April 2022, Cash App was hit with a data breach leaking the full names, stock activities and unique sensitive financial information of 8.2 million customers. Thankfully other sensitive information such as social security numbers and home addresses were leaked.

This attack was carried out by an employee of the company who had access to Cash App's Investing service's server. The employee downloaded a report containing the above information before leaving the job, suggesting that revenge may have been the employee's motive.

In response to the breach, Block, the company behind Cash App, filled a report with the United States Securities and Exchange Commission. Block has also informed law enforcement and has hired a forensics firm to help with an investigation into the incident. Block has begun to contact all 8.2 million affected users and the applicable regulatory authorities. When asked for comment, Block said "We take the security of information belonging to our customers very seriously, and we are continuing to review and strengthen our administrative and technical safeguards to protect the information of our customers".

## Microsoft, March 2022

In March 2022, Microsoft was breached by the criminal organization Lapsus$. Lapsus$ were able to access the source code of services such as Cortana and Bing. After Lapsus$ announced they gained access to Microsoft's servers, Microsoft ensured customers that no customer information was stolen and that the "viewing source code does not lead to elevation of risk" to customer information.

Lapsus$ has been known for breaching other major tech companies, such as Samsung and Nvidia. Their motives are unknown, but are believed to be for financial gain and political influence. During the breach, Microsoft's cybersecurity teams discovered that a singular account was breached, and their teams "quickly engaged to remediate the compromised account". The account that was compromised had limited access to information, which further helped mitigate the breach. Thanks to Lapsus$'s loud approach to their attacks, Microsoft was able to promptly shut down the attack mid-operation, limiting broader impact.

In response to the breach, Microsoft has shared new detection, hunting and mitigation tactics to help them remain vigilant against further attacks. Microsoft has also written a blog post explaining the different methods Lapsus$ uses to compromise accounts and gain access to a company's systems. Microsoft has further written up recommendations to prevent similar attacks, including using securer MFA requirements, such as number matching rather than SMS and telephony-based methods to avoid SIM-jacking risks.

# Authentication Methods

## Password Authentication

Passwords are the most basic authentication method, and are often the most insecure. Google researchers found that over 52% of passwords are reused across accounts, and FIDO researchers found that passwords were the root cause of over 80% of cyberattacks. This is often because users are unable to remember multiple passwords, and therefore result to using the same one over all their accounts. If a company then suffers a data breach, your password for all your accounts will have been leaked and gives hackers the opportunity to breach your data and privacy.

To attempt to mitigate the effects of insecure password habits you should provide a password manager to your users, such as Bitwarden, which is able to generate random and secure passwords for users. All data stored on Bitwarden is encrypted, and for extra security you can self-host a Bitwarden server so all data can be stored in-house. This means your passwords aren't stored on a third party's server, preventing data leaks of all your passwords, such as the LastPass incident in August 2022.

## Magic Links / One Time Passwords

Magic links are a type of authentication where a link is sent to a user, via e-mail or SMS, which will allow them to authenticate and sign in just by clicking it. One time passwords are similar to magic links: a code is sent to a user, and they must type that in to be authenticated. OTPs can either be used in conjunction with a password, or as a replacement, whereas magic links are designed to completely replace passwords.

Magic links and OTPs (replacing passwords) are most appropriate where security isn't highly critical and the user experience is important. These should not be used in a high security environment as it makes it easier to attackers to take over an account if they have access to the user's e-mail.

Even if security is not important, choosing magic links may not be the best option depending on your target audience. If your target audience is the elderly, they may have trouble understanding and working with their device and trying to find an e-mail to login may be challenging to them.

## Multifactor Authentication

Multifactor authentication is typically used in conjunction with a password, providing an extra step of security. The most common types are:

- One time passwords - generated by an app or sent via SMS and e-mail
- Biometrics - your face, fingerprint, etc
- Number matching and push notifications - enter a number in an app or approve a notification

MFA can also be used without a password. For example, you could approve a push notification on your phone, and before it approves your request a biometric is checked, such as a fingerprint.

MFA is most suited for higher security applications where security is more important than convenience. You should ensure your target audience is confident in using mobile devices and being able to respond to potential false requests.

It is important that MFA is not required on every request, and intelligence should be used to detect a high risk sign-in and block it with an MFA request. Such high risk events would be impossible travel to another country or a change of IP address. MFA should also be requested when a user attempts to perform a dangerous action, such as changing their password or account details. In an example of a bank, they may want to request MFA when a user tries to transfer a large amount of money.

## OAuth 2.0

OAuth 2.0 allows users to sign in to a service using an existing account from a service provider such as Apple or Google. This is typically known as ‘Single Sign On’ (SSO). OAuth allows users to use one account to sign-in to everything and eliminates the need of remember multiple passwords.

An OAuth provider gives the site you’re logging into an access token which allows the site to authenticate you and sign you in. For added security, OAuth providers allow you to revoke access tokens to sites requiring the user to sign back in through the provider. OAuth providers support MFA too, allowing them to make the sign-in process more secure.

However, the main risk of OAuth is that if an attacker has access to your account with the service provider, they will be able to log into all your accounts that use OAuth. When selecting OAuth as a method of logging in, you must ensure that the service is secure and provides the appropriate MFA options, and intelligence for high-risk logins. Regardless of how secure your OAuth provider is, it is not recommended to use OAuth in high security environments. It is also not recommended to use OAuth as your authentication system would rely on an external company’s services and if their systems go down, you will not be able to authenticate and sign in.

## FIDO2

FIDO2 is a standard of cryptographic authentication using a public key. FIDO2 is often used a replacement for a password, or as an MFA method. Authenticators are typically in the form of a USB stick (such as a YubiKey), however they can also be found in the Trusted Platform Module of a laptop or smartphone. Other forms of the FIDO2 standard can include biometrics such as your face or fingerprint.

In most cases, as FIDO2 is most commonly found in a USB-based form, users would have to purchase two tokens. One token for main use, the other token as a backup key. It is important to have a backup as if a user loses access to their token, they would no longer be able to access the required service. As an example for using a USB-based token a site will ask you to insert the device into your system, and then it will ask you to press something physical on the key. Sometimes this can be a fingerprint sensor, whilst sometimes it is to just confirm you are at your desk and you want to confirm the sign-in.

FIDO2 is a good option when the need for high security is greater than a seamless user experience. It is also important that your target audience is technical enough to know how to understand and use the token. Finally, depending on the data, administrators should be able to recover accounts if a token is lost, providing they can prove their identity with their own key. To ensure your users can never be fully locked out, a master key could be kept in a locked, secure safe.

## My Recommendation

To conclude, I recommend physical FIDO2-based authentication with a username and password as the most secure and suitable for our network. FIDO2 removes any risk of a cyberattack as the token required to access an account is physical and must be inserted into a device for a user to be fully authenticated. This limits the attack vector to be physical only, with the only risks being if a key is stolen or lost. To combat this, it is important to have a backup key stored in a secure place, such as a safe. This ensures that even if a key is lost or stolen, you have a backup key to log in to your accounts and revoke the compromised token. Using FIDO2 would require 3 fields to log in: a username, a password and a FIDO2 key. This further reduces the attack vector if a key is stolen, as the thief would also need to know the user's username and password to login. Because of this I recommend FIDO2 in conjunction with a username and password as the most secure way to authenticate to the network.

# Cryptographic Techniques

## Asymmetric Cryptography

Asymmetric Cryptography, also known as public key cryptography, uses a public-private key pair to encrypt data. When generating a key pair, randomness is an important factor to ensure the encryption is strong. A popular way to generate randomness for a key pair is a user's precise mouse movement. Once the keys are generated, the private key must be stored securely as it is used for decrypting data. It is good practice to further protect your private key with a password. The private key in most cases should never be shared.

The public key is used to encrypt data, and can be shared with others of whom you want to be able to encrypt data. Once data is received, it can be decrypted with the private key. However, for digital signatures, the private key is used to sign the e-mail or document and the public key can be used to decrypt and verify that the signature is legitimate.

For security, public-private key pairs often come with expiration dates to ensure that if a key is breached without the owner's knowledge, it will eventually expire and the criminal will no longer have access. This means it is important to manage your keys appropriately to ensure that they are always up-to-date. For example, if your key has expired and is used for SSL, web browsers may flag your site as insecure which would result in users not visiting your site.

### Advantages of Asymmetric Cryptography

- Key Distribution - only public keys have to be exchanged, ensuring the decryption (private) key never leaves your own device.
- Digital Signatures - with asymmetric cryptography, messages can be signed and verified as legitimate by the recipient (as they are signed with a private key).
- Non-repudiation - ensures that the sender cannot deny that they sent an encrypted message, using digital signatures as they use a private key to sign.

### Disadvantages of Asymmetric Cryptography

- Slower than symmetric cryptography, meaning it is not appropriate for the bulk decryption of messages.
- If a private key is lost, no messages can be decrypted.
- There is no public key authentication, so you cannot confirm who the key belongs to.

## RSA Encryption

RSA encryption is a type of public-key encryption which generates a public-private key pair from two large prime numbers where their product is larger than the current and projected computing power can handle. In 2015, the US Government required the modulus to be at least 2048 bits long, making the two prime numbers have a rough total of 308 decimal digits. This makes the product of the two numbers roughly a 617-digit number. From this an exponent that is relative to the two prime numbers minus one is selected, and a private exponent is computed to create the private key.

To encrypt a message, the following is used: $c = m^e \bmod n$, where:

- $c$ is the encrypted output
- $m$ is the plain text
- $e$ is the selected exponent
- $n$ is the product of the two prime numbers

To decrypt a message, the following is used: $m = c^d \bmod n$, where:

- $m$ is the plain text
- $c$ is the encrypted text
- $d$ is the private exponent
- $n$ is the product of the two prime numbers

### Advantages of RSA Encryption

- Security - RSA is deemed secure as factorizing the product of the two large prime numbers is computationally infeasible.
- Authentication - RSA can sign digital signatures, providing non-repudiation.
- Distribution - only the public key has to be distributed, allowing for scaleability.

### Disadvantages of RSA Encryption

- Performance - RSA can be slow and can require powerful resources to compute large messages.
- Key size - further contributing to slow performance, RSA's huge key size slows it down at the cost of security.
- Quantum computing - with the introduction of quantum computers, they could break RSA encryption with their powerful components for large prime numbers.

## Pretty Good Privacy

Pretty Good Privacy, PGP, is a widely used encryption method for digital communication and authentication. PGP uses a mix of both asymmetric and symmetric key cryptography.

To encrypt a message, you first must generate a public-private key pair. Once done, the sender must use the recipient's public key to encrypt the message. The sender must then generate a one-time symmetric session key and use that key to further encrypt their message. This can typically be done using a symmetric encryption algorithm. For example, AES. Finally, the session key is encrypted using the recipient's public key and is sent along with the encrypted message.

To decrypt a message, the recipient must use their private key to decrypt the provided session key. The recipient must then use that session key to decrypt the message.

### Advantages of PGP

- Security - PGP uses strong encryption algorithms such as AES and RSA to encrypt session keys and messages.
- Versatility - PGP has a wide range of uses, including digital signatures, secure communications and key exchange.
- User-friendly - PGP is commonly built into applications such as ProtonMail which handles all the key management and encryption for the user.

### Disadvantages of PGP

- Key management and distribution - outside of applications, PGP requires users to manage their own keys and manage the distribution of their public keys.
- Compatibility - not all applications support PGP. For example, while you can use PGP encryption in ProtonMail seamlessly, you must manually attach your session key and public key in clients that do not support it out of the box.
- Performance - for larger messages, PGP can be very computationally expensive.

# Unit 32, Assignment 1

## Are we Safe?

George Hotten

April 20, 2023

# Minimizing Threats to Network Security

# Policies and Procedures

- It is important that your organization has well-documented and clear security policies and procedures.
- These documents should state how users are expected to act online, being vigilant and cautious. There should also be a detailed incident response plan if there is a security breach.
- The created documents should be reviewed and updated regularly to ensure it reflects the latest threats.
- To ensure compliance, monitoring could be used along with testing users with fake phishing e-mails to ensure they are following the latest guidance.

# User Responsibilities

- To ensure users are responsible with their security, your organization should require strong passwords and require regular password updates. Passwords should also not be reused.
- This ensures that in the event of a data breach where a password a user uses has been unknowingly leaked, regular password changes help eliminate the possibility of an attacker attempting to gain unauthorized access to your systems.
- Implementing multifactor authentication is also important to further protect your user's accounts as if a password is guessed or stolen, the attacker would not be able to gain access without completing the required MFA task.

# Providing Education

- It is vital that users are receiving regular IT and security training on the latest threats and security practices.
- This helps users be vigilant of new and emerging threats, lowering the risk of a user following insecure practices.
- Users should further be trained to report anything suspicious online and within the network, no matter how minor it may seem, developing a culture of awareness within your organization.
- You could also encourage users to take certifications in network security to help further expand their knowledge.

# Physical Security

- Whilst there is often threat from bad actors online, there could also be a threat of bad actors within the organization. Because of this, it is vital that proper access control is set up into server rooms and data centres.
- This can take the form of RFID or NFC fobs, combined with a pin code. Ideally, this pin code should change regularly.
- To further increase security, video surveillance should be installed around all entrances and within the server room. This ensures that all possible points of entry and areas are under full surveillance.
- An intrusion detection system should also be installed for out-of-hours security.
- All systems should be regularly tested and maintained to ensure they are working as intended, keeping security at a maximum.

# Risk Assessment and Reduction

- To help identify vulnerabilities within your network, regular testing and risk assments should be done to ensure your network remains secure.
- Risks should be prioritized based upon potential impact. Once risks have been identified, attempts to mitigate them should be implemented as based upon their priority.
- Once a mitigation has been implemented, it should be regularly monitored to ensure that the implementation is effective and is reducing the risk identified.

# Conclusion

- It is vital that everyone participates being vigilant and following secure digital practices. This keeps everyone’s data safe and keeps the organization’s systems running smoothly.
- Education is also hugely important to help keep your user’s knowledge and up-to-date with your organization’s security practices.
- You should ensure that you are regularly reviewing and updating your security policies and procedures to keep up with the latest threats.

# Network Protection Methods

## Secure MIME and Digital Signatures

A secure  Multipurpose Internet Mail Extension is used for sending and receiving signed emails  using Public Key Infrastructure providing end to end encryption. This means the sender encrypts their data with a private key and it can only be decrypted with the public key held by the recipient.

MIME can also provide digital signatures to ensure the email hasn't be tampered with during transit and can prove if the email is legitimate.  This is done using the same PKI from above.

## Temporal Key Integrity Protocol

TKIP is an older alternative to AES and was originally used in WPA before being replaced by AES and CCMP. TKIP is similar to WEP encryption and is no longer considered secure.  TKIP uses a number of techniques to provide security, including message integrity checking, encryption, and key management.

## Biometrics

Biometrics are a type of multi-factor authentication, providing something that you are. Commonly used methods are fingerprint recognition, facial recognition and retina recognition. Biometrics are most commonly found on mobile devices, such as phones and laptops.

## MAC association

MAC association is typically found on routers and switches and restricts what device can use each port by their mac address. If an unknown mac address is detect on a port all traffic to and from it will be dropped. This can prevent tampering and device security at a physical level,

## WEP/WPA Keys

Wired Equivalent Privacy was the most common form of Wi-Fi security in the early 2000s using 64-bit encryption. WEP was eventually upgraded to 128-bit encryption however WEP was ridden with vulnerabilities. It was later replaced by Wi-Fi Protected Access which uses a pre-shared key and 265-bit encryption. WPA also had many vulnerabilities and have been replaced by WPA2 which uses AES algorithms and the Counter Cipher Mode with Block Chaining Message Authentication Code protocol (CCMP).

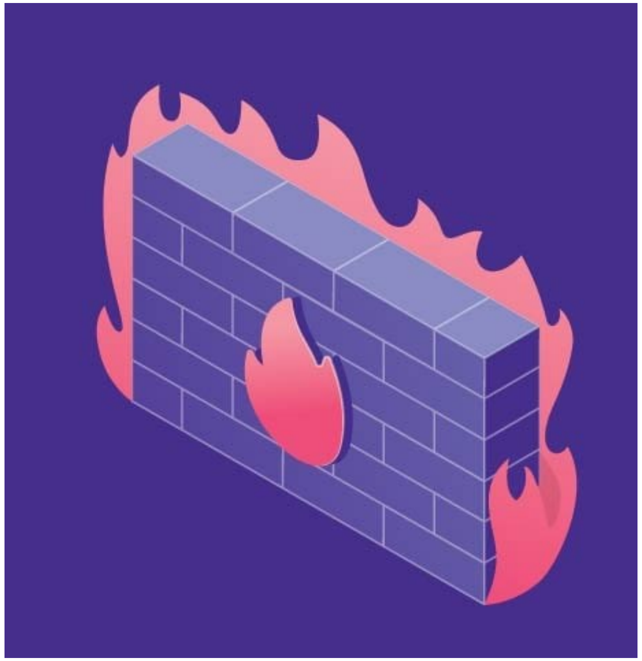
# Intrusion Detection Systems

## Firewalls

Firewalls act a barrier between your devices and other devices on your network and on the internet. They monitor all traffic entering and leaving your device or network and decide which traffic can pass and what will be dropped. Firewalls can detect malicious traffic and block it before it enters your network.

## Virus Protection

Virus protection software can detect any malicious  applications when they execute and can block them before they do any harm to a device. They can stop malware such as spyware, trojans, viruses and ransomware.



## File Monitoring

File monitoring software scans the files on your device checking for many malware that you could have downloaded. It can also detect modification from malware and block it, which is especially helpful in a ransomware attack. File Monitoring can also detect security breaches if a user attempts to access and edit files they don’t have access to. File monitoring software can provide extensive logs which can be helpful in resolving a security breach.

## Honeypots

Honeypots are decoy files to attempt to deter hackers from your important data. They can also be used in an isolated environment to observe the methods hackers used to gain access to your system without risking your actual important data.