Are We Safe?

Unit 32, Assignment 1

Thomas Robinson

rob21005043

21st April 2023

Solihull College

Contents

1 Types of Attack **2**
1.1 Spoofing 2
1.2 Mathematical 2
1.3 Software Exploitation 2
1.4 Rootkits 2
1.5 Brute Force 2
1.6 Back Door 2

2 Sources of Attack **3**
2.1 Black-Hat Hackers 3
2.2 Insider Threats 3
2.3 Nation-States 3

3 Recent Network Threats **4**
3.1 Gloucester City Council, 2021 4
3.2 Ubiquiti, 2021 4

4 Authentication Procedures **5**
4.1 Authentication Methods 5
4.2 Cryptography Techniques 6

1 Types of Attack

1.1 Spoofing

A spoof attack is when an attacker disguises themselves as a trusted individual, organization or device to gain access to a network. This could be to eavesdrop and intercept data, gain access to resources. Alternatively, the source of a message or data could be spoofed to appear to be from a trusted source. An example of a spoof attack would be changing the MAC address of a piece of network hardware to bypass a blocklist.

1.2 Mathematical

A mathematical attack is an attack on cryptographically secure resources or communication, through a known weakness or by brute forcing. Use cases for this attack include decrypting encrypted data, bypassing authentication mechanisms and tampering with data.

1.3 Software Exploitation

Software exploits make use of a vulnerability, bug or other issue with a piece of software to gain access to a device or network. This can be used to execute malicious code that can do all-manner of nefarious acts.

1.4 Rootkits

A rootkit is a piece of malicious software that masquerades as a legitimate program that requires elevated privileges. They are often used for installing hidden backdoors, replacing system files, and launching further attacks. Their main goal is to avoid detection.

1.5 Brute Force

The concept of going through many combinations of credentials in an attempt to gain unauthorized access. For example, using a list of common passwords or a trying all available PINs. There are many methods that can be employed, including dictionary attacks (generating passwords using common words) and using rainbow tables (a pre-computed list of hashed table of cryptographic function outputs).

1.6 Back Door

A way of bypassing normally-required authentication or encryption. These could be added intentionally or unknowingly by a malicious party. Often used for covert surveillance and monitoring.

2 Sources of Attack

2.1 Black-Hat Hackers

Black-Hat hackers are individuals or groups that exploit vulnerabilities in networks or systems. One of the primary motives is often financial gains that can be reaped from ransom payments, fraud or selling information. (Kaspersky, n.d.)

2.2 Insider Threats

Insider threats come from within an organisation. They are carried out by people with elevated privileges or knowledge. This privilege can then be exploited to harm the organization, including acts of sabotage or espionage. (Cybersecurity and Infrastructure Security Agency, n.d.)

2.3 Nation-States

Attacks can come from government-sponsored entities (individuals or groups) with the motive of political, economic or militaristic gain. These typically involve sophisticated and targeted attacks that attempt to be well-hidden. (BAE Systems, n.d.)

3 Recent Network Threats

3.1 Gloucester City Council, 2021

In December 2021, Gloucester City Council became aware of malware that had made its way into their network.

The malware was delivered within an email sent to a member of staff and is believed to have lay dormant for months before an impact was noticed.

Online services provided by the Council, including benefit payments and planning applications, were impacted. Staff were blocked from sending emails and other organizations temporarily blacklisted Gloucester City Council addresses.

It is unclear the motive behind the attack, however it is alleged that it could be linked to groups in Russia.

A year later, it is estimated that the attack has cost Gloucester City Council nearly £800,000 of taxpayer money to resolve, including rebuilding much of the Council's IT infrastructure. During this time, it was necessary for staff to perform work and provide services manually.

There are areas still feeling the impact; the Museum of Gloucester is still unable to access or make use of its database of artefacts.

Sources 'Cyber Attack Disrupts Gloucestershire Council's Website', 2021; 'Gloucester Council Cyber Attack Linked to Russian Hackers', 2022; Garcia, 2022; 'Cyber Attack Affecting Gloucester Museum's System One Year On', 2023

3.2 Ubiquiti, 2021

Ubiquiti, a popular manufacturer of networking equipment, was subject to an attack by an inside threat actor.

The rouge employee cloned hundreds of proprietary code repositories from the company's GitHub organization and downloaded dozens of gigabytes of confidential data from their Amazon Web Services account. In an attempt to evade detection, he changed log retention policies and attempted to erase any traces of his actions.

After downloading the data, the employee posed as an anonymous hacker and attempted to extort his employer, demanding a 50 bitcoin (approx. $2 million) ransom to stop the data being posted publicly. Ubiquiti of course, refused to pay the ransom.

When the ransom attempt failed, the employee attempted to masquerade as a whistleblower, sending media outlets reams of false information about what had gone on. These reports caused Ubiquiti's stock price to plummet $4 billion in the space of a few days.

The attack was likely carried out for financial gain and a desire for notoriety. The response from Ubiquiti included the disclosure of a potential data breach to customers.

Sources Burgess, n.d.; Gatlan, n.d.; Department of Justice, 2021; Corfield, n.d.

4 Authentication Procedures

4.1 Authentication Methods

Passwords Password-based authentication involves entering a secret string of characters to access a service, network or device. The benefits of this method of authentication is familiarity; it is unlikely that additional support will need to be provided to users in order to use since its use is widespread in the technological world. Drawbacks of password-based authentication stem primarily from poor user habits. Short or easily-guessable passwords are a security liability but enforcing longer passwords can be a significant annoyance if they need to be entered regularly. Users that re-use passwords between services are at significant risk of account hijacking, since if one service where the password is used is breached and the password leaked, the attacker can now gain access to every service.

Two-Factor Authentication 2FA refers to having two different pieces of private information required when authenticating. For example, both a secure password and a code generated from a TOTP-based (RFC 6238) mobile app. Typically, the two factors are something you *know*—such as a password—and something you *have*–like a phone or security key device. While 2FA is a good way of adding significant additional security to an account, a downside could be the loss of access if the second factor is lost. This problem is often thwarted by the use of recovery keys or codes, but these may be stolen or misplaced.

Multi-Factor Authentication Similar to 2FA, MFA refers to requiring multiple pieces of information when authenticating. However, in this case, more than two may be required. This is commonly employed by services requiring a high-level of security, such as a bank or government account. As an example, Lloyds Bank first asks for an account password, then specific characters from a set word, and then an OTP sent via SMS. The process could be perceived as convoluted, however each additional step is adds more security.

One-Time Password OTPs are a method of authenticating a user by sending a unique code that is only valid for that particular login attempt. This can be used as a replacement for a primary password or as an additional factor when logging in. In the first scenario, rather than a user account having a set-password, a unique code is generated each time they wish to log in, and this code is entered when prompted. In the latter scenario, the code will be sent after a successful password attempt and will need to be entered before the user is authenticated. In both cases, the code may be sent by several methods, including by SMS or by email. Wherever the code is sent, it is important that it is a secure communication method. For this reason, many services prohibit the use of SMS-based OTPs due to the potential of SIM-hijack attacks.

Biometric Authentication This type of authentication makes use of unique physical attributes, like a fingerprint, iris or face. Making use of biometric authentication requires the associated physical hardware for reading the information, which prohibits where it can be used. Biometric authentication is common on both consumer and business devices: both smartphones and laptops now implement fingerprint readers and facial recognition technology. Insecure biometric authentication systems can be a security weak point. As an example, a facial recognition system that does not take into account depth mapping may be fooled by a photograph, or a system that does not have a high enough sensitivity may not be able to tell twins apart. Since this authentication method makes use of ”something you *are*,“ there is nothing to remember or to lose. Biometric is commonly used as a single authentication factor, however it can also be employed as an additional step.

Figure 1: A ‘Touch-ID’ fingerprint sensor embedded in the power button of an Apple MacBook laptop. (Bram Van Oost, Unsplash)

Figure 2: A YubiKey is a USB key that makes use of PKI, and the U2F and FIDO2 protocols to act as an authentication device. (Own Photograph)

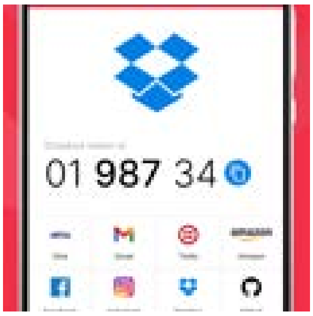


Figure 3: ‘Authy’ is one of many apps that can be used to generate RFC 6238 TOTP codes on a smartphone (Twilio Authy)

In my view, biometric authentication provides a good medium between convenience and security. Fingerprint authentication is widely used in businesses and allows staff to log in quickly without entering a username or password. However, it is important to provide alternatives for those who do not consent to providing biometric data. For this reason, I would also recommend offering a traditional username and password option with required two-factor authentication. This method is less convenient—requiring three individual fields to be filled—however it is a secure choice.

4.2 Cryptography Techniques

Hashing This is the process of encoding an input value as a fixed-length string of characters called a ‘hash.’ Hashing an input is a one-way process; it is not possible to recover the input from the hash. Uses for cryptographic hashes include ensuring data integrity and password security. An example of the former is a website providing ‘file hashes’ of downloads it offers. When a file has been downloaded, a hash can be generated from it which can be compared to the one listed by the site. If they both match, it is certain that the file has not been tampered with in-transit and is the same as the one stored by the server. Password hashes are used when storing passwords in a database to ensure they never have to be saved as plaintext entries. This means that even if an attacker gained access to a database, they would not be able to view user passwords. When logging in, the given password is ran through a hashing function, the output of which is then compared to the value stored in the database. If there is a match, the password entered is correct.

PGP Pretty Good Privacy, or ‘PGP,’ is a method for encrypting and decrypting documents and data. It is most commonly used for encrypting communication when using insecure methods, such as email. PGP makes use of public and private key-pairs that are used to encrypt and decrypt data. When encrypting data, a random key is generated to encrypt the data. This random key is then encrypted with the recipient's public key. These two encrypted components are combined to form a PGP message. When decrypting, the process is reversed. First, the recipient decrypts the encrypted random key using their private key. This decrypted random key is then used to decrypt the encrypted data. PGP allows secure communication over inherently insecure mediums, such as email or messaging apps, and is used for the delivery of confidential or sensitive information by whistleblowers and security researchers.

RSA RSA, from the surnames of those who first described the algorithm (Rivest–Shamir–Adleman), is a widespread asymmetric encryption method. An asymmetric system makes use of public and private keys, where the key used for encrypting data is public, but the key required to decrypt the data is private. The RSA algorithm makes use of two large prime numbers that must be factored. This is a very computationally-intensive process that is functionally-impossible to brute-force, making it a very secure option. RSA supports varying key lengths, which can be adapted based on the computational resources available and the security required.

References

BAE Systems. (n.d.). *The Nation State Actor*. https://www.baesystems.com/en-uk/feature/the-nation-state-actor

Burgess, C. (n.d.). *Ubiquiti breach an inside job, says FBI and DoJ*. CSO Online. Retrieved April 18, 2023, from https://www.csoonline.com/article/3643650/ubiquiti-breach-an-inside-job-says-fbi-and-doj.html

Corfield, G. (n.d.). *Ubiquiti dev charged with data-breaching own employer*. Retrieved April 18, 2023, from https://www.theregister.com/2021/12/02/nickolas_sharp_ubiquiti_hack_charged/

Cyber attack affecting Gloucester museum's system one year on [newspaper]. (2023). *BBC News: Gloucestershire*. Retrieved April 18, 2023, from https://www.bbc.com/news/uk-england-gloucestershire-64917275

Cyber attack disrupts Gloucestershire Council's website [newspaper]. (2021). *BBC News: Gloucestershire*. Retrieved April 18, 2023, from https://www.bbc.com/news/uk-england-gloucestershire-59831468

Cybersecurity and Infrastructure Security Agency. (n.d.). *Defining Insider Threats*. https://www.cisa.gov/defining-insider-threats

Department of Justice. (2021, December 1). *Former Employee Of Technology Company Charged With Stealing Confidential Data And Extorting Company For Ransom While Posing As Anonymous Attacker*. Retrieved April 18, 2023, from https://www.justice.gov/usao-sdny/pr/former-employee-technology-company-charged-stealing-confidential-data-and-extorting

Garcia, C. (2022, December 21). *A year since hackers disrupted services for thousands of citizens*. GloucestershireLive. Retrieved April 18, 2023, from https://www.gloucestershirelive.co.uk/news/gloucester-news/gloucester-cyber-attack-year-hackers-7947958

Gatlan, S. (n.d.). *Former Ubiquiti dev charged for trying to extort his employer*. BleepingComputer. Retrieved April 18, 2023, from https://www.bleepingcomputer.com/news/security/former-ubiquiti-dev-charged-for-trying-to-extort-his-employer/

Gloucester Council cyber attack linked to Russian hackers [newspaper]. (2022). *BBC News: Gloucestershire*. Retrieved April 18, 2023, from https://www.bbc.com/news/uk-england-gloucestershire-60045060

Kaspersky. (n.d.). *What is a Black-Hat hacker?* https://www.kaspersky.com/resource-center/threats/black-hat-hacker

Network Protection Methods

Unit 32, Assignment 1, Task 2a
Thomas Robinson — April 2023

S/MIME & Digital Signatures

- Encrypts and signs email messages
- Protects sensitive information
- End-to-End Encryption ensures integrity
- Can help prevent email spoofing attacks by validating senders

Biometrics

- Uses physical traits for authentication
- Offers convenience and a high-level of security
- Need to be wary of privacy and any potential misuse of biometric data

MAC Association

- Associating a unique address with a device
- Essential to building an Ethernet or Wi-Fi LAN
- Enables devices to communicate at the data link layer
- Security policies can be applied on a per-address basis

WEP & WPA Keys

- Wired Equivalent Privacy and Wi-Fi Protected Access
- Cryptographic standards that secure a Wi-Fi network
- WEP was superseded by WPA and its successors
- Managing credentials correctly contributes significantly to the security of a network
- WPA3 uses AES-256 and SHA-384

TKIP

- Temporal Key Integrity Protocol was used for WPA networks (not WPA2 or WPA3)
- Provided more security than WEP but is now considered insecure
- Should not be used except when necessary for legacy devices

Intrusion Detection Systems

Unit 32, Assignment 1, Task 2b
Thomas Robinson — April 2023

Firewall

- A firewall is an appliance or piece of software that filters traffic based on its properties, such as source/destination address, ports, MAC address, etc
- For example, you could use a firewall to block packets travelling from one network to another based on the source and destination IP addresses
- Can be running on an end-device or as a part of network infrastructure
- Prevents intruders from accessing areas of a network

Virus Protection

- Virus Protection is the process of scanning for, locating, and removing malware and malicious applications from devices on a network
- Virus Protection can also include detecting known malicious traffic and blocking/reporting it
- Helps stop backdoors and RATs from entering a network

File Scanning

- File Scanning follows a similar principal to Virus Protection
- Can refer to scanning files at-rest or in-transit
- Ensures data integrity and protection against unwanted or malicious applications
- Ensures the legitimacy of files and can protect against attacks where one file is disguised as another

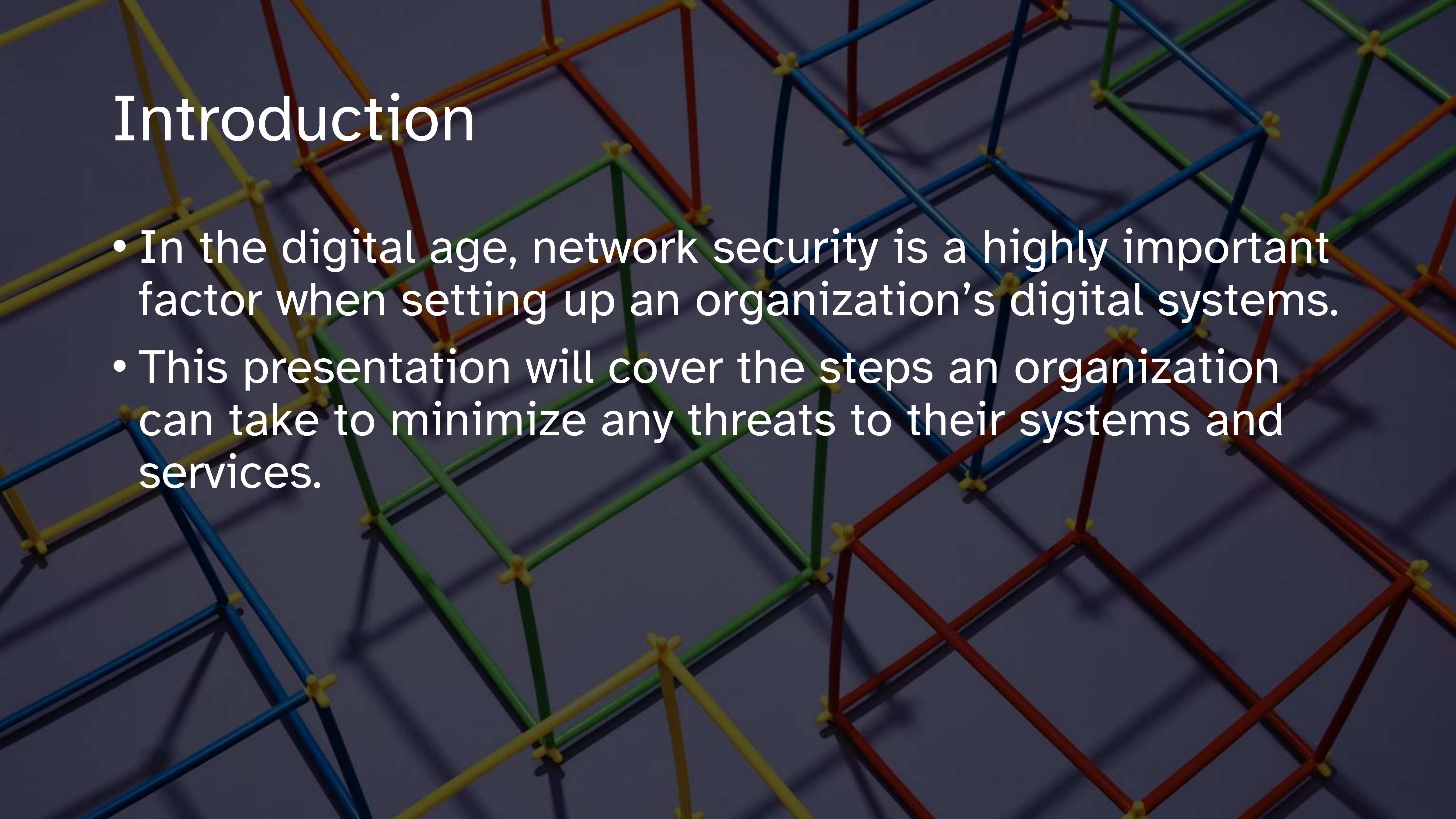
Honeypot

- A honeypot is a decoy system or network that is designed to lure a would-be attacker to the wrong place
- Will mimic a real system or network and log all activities
- Helps an organisation gain insights into attackers' methodology, tools, tactics and goal

Minimising Threats to Network Security

A Comprehensive Approach

Unit 32, Assignment 1
Thomas Robinson – April 2023



Introduction

- In the digital age, network security is a highly important factor when setting up an organization’s digital systems.
- This presentation will cover the steps an organization can take to minimize any threats to their systems and services.

Policies & Procedures

It is important to establish clear and well documented security policies.

These should be updated regularly inline with current technology and threats.

As an organization, you should enforce policies through monitoring and issue penalties for non-compliance.

This is because sensitive business data could be at risk.

In preparation for an incident, a response plan template should be created to allow the swift resolution of any incidents.

Educating Users & Their Responsibilities

- It is important that users are given sufficient IT training to ensure they are aware of the expected standards of security.
- Users should be required to set strong passwords and set up multi-factor authentication when possible.
- Users should only have access to what is required to complete their daily duties. This limits the damage an attacker could do, should they compromise a user's account.
- A good security culture should be established, with users encouraged to be vigilant and report anything suspicious.

Providing Education to Staff

IT staff should be encouraged to keep up with the latest developments both inside and outside of work

Organizations should provide ongoing training about the newest technology, threats and attack vectors to all staff

Learning should be encouraged, for example by supporting the costs of qualifications such as an CCNA

Physical Security Measures

- It is important to ensure that physical systems, including servers and devices remain secure
- This means protecting them from unauthorised access
- Appropriate Access control measures should be in place
  - Key Cards, Biometrics, Etc
  - Should be regularly reviewed
- Restricting access to only those who need it
- Restricting the use of personal devices in sensitive areas

Risk Management

Risk evaluations should be taken on a regular basis

These could cover everything from what measures are in place to what attacks are likely and from whom

Measures should be put in place to minimise risk when it is deemed appropriate

The End

- Everyone has a part to play in maintaining good security
- It is important to provide education and training to keep employees informed and knowledgeable of threats