# WEEK 9 – Task 9.1 P

## Question A

What is a Rogue Access Point (AP)? Briefly explain 2 different approaches to detect a rogue AP. In your answer ensure that you discuss whether you think a rouge AP is a security vulnerability and how may an attacker exploit a rogue AP. (300 words)

An unauthorized wireless access point connects to a network without the network administrator's knowledge or approval is known as a rouge access point. Because attackers can utilize these rouge Aps to get around network security, they can provide serious security issues regulates, eavesdrops on conversations, or initiates more network attacks.

- A highly dangerous security vulnerability is a rogue access point. Attacker can use rouge Aps to carry out man-in-the-middle attacks and eavesdrop on network traffic. Misuse of network resources.
- Methods of Detection
  - ✓ Conduct Examination
    In order to spot anomalous activity that can point to the existence of a rogue AP, behavior analysis analyzes network traffic patterns. Systems for detecting intrusions (IDS): IDS programs scan network traffic for anomalous patterns that depart from predefined standards. An alarm may be triggered by traffic generated by an unknown access point (AP) that begins broadcasting. Algorithms for Machine Learning: By identifying abnormalities in the regular traffic patterns of approved APs, advanced systems can employ algorithms for machine learning to detect rogue APs.

  - ✓ Network Examining
    In order to identify every device connected to the network, including APs, network scanning entails actively probing the network. MAC addresses and other distinguishing characteristics can be used to identify illegitimate devices using this method. Wireless Network Mapping to map every wireless access point (AP) within a specific radius, utilize programs such as Kismet or NetStumbler. Administrators can identify rogue APs by cross-referencing this map with the list of known, authorized APs. Active Scanning to keep an eye out for unauthorized or new devices on the network, network managers might employ tools that do an ongoing scan. Rogue APs, for instance, can be automatically detected and dealt with by enterprise solutions such as Cisco Wireless Intrusion Prevention Systems (WIPS).

- Reference

  - ✓ Gast, M. S. (2005). "802.11 Wireless Networks: The Definitive Guide." O'Reilly Media.
  - ✓ Mareco, D. (n.d.). Rogue AP Detection: What is it & why your WLAN Design needs it. TechGrid. https://techgrid.com/blog/rogue-access-point-detection

## Question B

What is WiFi Protected Setup (WPS)? Which of the following WPS methods is vulnerable? Push-button method, PIN method, Piconet method, NFC method. (200 words)

- The goal of the WiFi Protected Setup (WPS) network security standard is to make connecting devices to wireless networks easier. Users can join devices to their WiFi network without typing lengthy passwords thanks to WPS, which was introduced by the Wi-Fi Alliance in 2007. It provides these four main means of connection the push-button method requires users to physically press both the router's and the device's matching buttons in order to create a connection. PIN Technique to establish a connection, users input an eight-digit PIN that is either shown on the device or supplied by the router. Not a typical WPS approach is the Piconet method. Tap a device against the router to establish a connection via the Near Field Communication (NFC) method.

- The PIN technique is the most susceptible of these. Users using this approach must input an 8-digit PIN, which is frequently displayed on the router. Unfortunately, because of its predictable form and unchanging nature, the WPS PIN is vulnerable to brute-force attacks. Since the first four and last four numbers are validated independently, there are only 11,000 possible combinations instead of the 100 million that there would otherwise be. This vulnerability compromises security by enabling attackers to decipher the PIN and obtain unauthorized access to the network.

- Reference

  - ✓ Wi-Fi Protected Setup | Wi-Fi Alliance. (n.d.). https://www.wi-fi.org/discover-wi-fi/wi-fi protected-setup
  - ✓ Chai, H.-C., & Leong, K. (2016). "Wireless Network Security: Theories and Applications." Springer.

## Question C

Which one is more secure: WEP, WPA, or WPA2? Explain 2 vulnerabilities of WPA that led to the development of WPA2. (300 words)

- In order to remedy flaws in earlier standards, wireless security protocols have developed. The earliest and weakest system is called Wireless Equivalent Privacy (WEP). WEP is susceptible to several attacks since it employs the RC4 stream cipher and a static encryption key. Its short key length (40 or 104 bits) and predictable initialization vector (IV) are its primary weaknesses, which enable attackers to decrypt the encryption using a variety of techniques such IV replay attacks.
- Wi-Fi Protected Access (WPA) was designed to address the shortcomings of WEP. It suggested the Temporal Key Integrity Protocol (TKIP) and a message integrity check. Despite being an improvement over WEP, WPA is still vulnerable, particularly when it comes to backward compatibility and inherent weaknesses in TKIP and WEP. TKIP still contains a number of WEP-related vulnerabilities despite using RCE in place of WEP, and brute-force attacks can be employed against the WPA pre-shared key (PSK) mode. The most secure of the three, Wi-Fi Protected Access II (WPA2), was introduced in 2004. WPA2 uses the Advanced Encryption Standard (AES) for encryption through the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES has stronger encryption and is less susceptible to assaults. Additionally, WPA2 improves data integrity and confidentiality by using CCMP rather than TKIP.TKIP
- Vulnerability: TKIP was created by WPA as a temporary fix that might executed using hardware that is already in place. Even with advancements, the RC4 cipher—which was still susceptible to some attacks—was nevertheless utilized by TKIP. As an example, the The Beck-Tews attack showed how TKIP could be used in less than a minute to decrypt brief packets, giving attackers the ability to insert malicious data. Weakness: Brute-force attacks could be launched against WPA's Pre-shared Key (PSK) mode, which is frequently employed in home networks. By using dictionary attacks, attackers could guess the PSK during the initial handshake between a device and an access point. This was troublesome as a lot of users selected weak passwords, which left the network exposed. In order to combat this, WPA2 introduced stronger encryption and key management protocols that improved defense against these kinds of assaults.
- Reference

  - ✓ Kaufman, C. (2002). "Network Security: Private Communication in a Public World." Prentice Hall.
  - ✓ Grubbs, P. (2024, May 15). The security Risks of Pre-Shared Keys (PSKs). SecureW2. https://www.securew2.com/blog/risks-pre-shared-keys-psks

**Question D**

Discuss how Mac Address Filtering may be used to secure a wireless network against threats? (200 words)

- One technique to improve wireless network security is MAC address filtering. limiting network access according to client devices' Media Access Control (MAC) addresses. This is how it functions and how it contributes to wireless network security
- Access Control: A hardware identifier known as a MAC address is specific to every device linked to a network. Administrators are able to establish a whitelist of authorized devices through the use of MAC address filtering. In order to prevent illegal devices from connecting to the network, only devices whose MAC addresses are on this list are permitted.
- Mitigating Unauthorized Access: By preventing the MAC addresses of unauthorized users' devices from being recognized and accepted by the network's Access Point (AP), this method can discourage petty intruders or unauthorized users from connecting to the network.
- Layer of Defense: An extra security layer is provided by MAC address filtering. An attacker needs to impersonate an allowed MAC address in order to obtain access, even if they are aware of the network's SSID or encryption keys.
- Easy to Implement: On the majority of wireless routers and access points, it is simple to set up and maintain. MAC addresses can be manually added to or removed from the list of devices that are permitted by network administrators.
- However, there are certain limitations to MAC address filtering. Although competent attackers can still spoof MAC addresses, this technique is less successful against dedicated or technically astute invaders. As a result, it ought to be combined with WPA3 and ongoing network monitoring, among other security measures.
- Reference

  - ✓ Mitchell, B. (2021, August 5). MAC Address Filtering: What it is and how it works. Lifewire. https://www.lifewire.com/enabling-mac-address-filtering-wireless-router-816571
  - ✓ Tanenbaum, A. S., & Wetherall, D. J. (2011). "Computer Networks." Pearson.

## Question E

Briefly discuss what an Evil Twin AP attack is? (200 words)

- One type of cyberattack in which a malevolent actor sets up an Evil Twin Access Point (AP) attack an impostor wireless access point (AP) that poses as an authentic AP. Tricking users into connecting to the rogue AP rather than the authentic one is the goal. This kind of attack usually entails the subsequent actions,
- Establishing a Rogue AP: The hacker sets up a wireless access point with the identical the valid AP's SSID (Service Set Identifier). To make the fake AP seem even more real, skilled attackers might additionally spoof the MAC address. Entice Users to Connect: When users look for available networks, they come across the rogue AP and connect to it since they think it's real. To draw consumers in, the attacker may employ more powerful signals. Data Interception: The attacker can intercept and collect all user data once they establish a connection with the rogue AP.
- Email addresses, login passwords, and other private information are among the sensitive data that are sent across the network. Malicious uses of this information include identity theft and other assaults. Man-in-the-Middle Attack (MITM): This attack deceives users by using a rogue AP to transfer traffic to a legitimate AP, making it difficult for users to detect the attack. At that point, the attacker has the ability to alter the data or add harmful content.
- Reference

  - ✓ Evil Twin Attack: Fake WiFi access point vulnerabilities | OKTa. (n.d.). Okta, Inc. https://www.okta.com/identity-101/evil-twin-attack/
  - ✓ Barton, R. (2012). "Securing Your Wireless Network: A Primer." SANS Institute

## Question F

Near Field Communication (NFC) is used for contactless payment systems. List and briefly explain 3 different vulnerabilities for NFC. (200 words)

- Near field communication (NFC) is widely used with contactless payment systems to facilitate transactions through close proximity communication. However, NFC technology is prone to several problems.
- Hackers can get data transmitted between an NFC device and a reader by means of eavesdropping. The typical working range of NFC is only 4 cm, but if an attacker has sensitive equipment, they can listen in from a greater distance. This might expose private information, like credit card numbers or personal identification numbers (PINs).
- Malicious actors can increase the communication range between two NFC devices through relay attacks. An attacker can carry out transactions without the user's knowledge or agreement by doing this by relaying signals between the legitimate devices over a longer distance. An important security risk is that an attack can take place without actual physical access to the NFC-enabled device.
- Data Modification: If you want to change the information that is shared between NFC devices, you must modify the data. In order to commit fraud or get unauthorized access to services, attackers have the ability to intercept and alter messages. While less common, this kind of assault is nevertheless quite dangerous because it needs specialized tools and exact timing.
- Reference

  - ✓ Higgins, M., & Higgins, M. (2024, February 7). NFC Security: 10 security risks you Need to know. NordVPN. https://nordvpn.com/blog/nfc-security/
  - ✓ Madlmayr, G., Langer, J., Kantner, C., & Scharinger, J. (2008). "NFC Devices: Security and Privacy." I