Cybersecurity

BootCon Presentation

Intercepting and Cracking Traffic from a WAP Mobile Device

By Dylan Dizon, David Lee, Gryphon Doyle, Stefhanus Tjong

Technical Background

WiFi

- WiFi is an essential wireless networking technology, providing widespread connectivity for various devices in homes, offices, and public spaces
- A wireless networking technology that allows devices to interface with the Internet.
- Enables convenient internet access, allowing seamless communication and online activities
- Internet connectivity occurs through a wireless router or wireless connection
- The open nature of wireless transmissions however, makes WiFi susceptible to unauthorized access and potential data breaches

Encryption

- Encryption is crucial for protecting sensitive information by converting it into a secure code that requires the correct key for deciphering
- Protocols like WPA (Wi-Fi Protected Access) and WPA2/WPA3 enhance WiFi security by implementing encryption, preventing unauthorized users from intercepting or tampering with data
- Encryption ensures the integrity of transmitted data, adding a layer of defense against cyber threats
- WiFi and encryption form a critical framework for secure and efficient digital connectivity
- The consequences of having an insecure Wi-Fi network and lacking proper encryption can be significant, leading to various risks and potential negative outcomes

WPA2 - A security protocol used to secure wireless networks by providing encryption and authentication mechanisms, enhancing the protection of data transmitted over WiFi

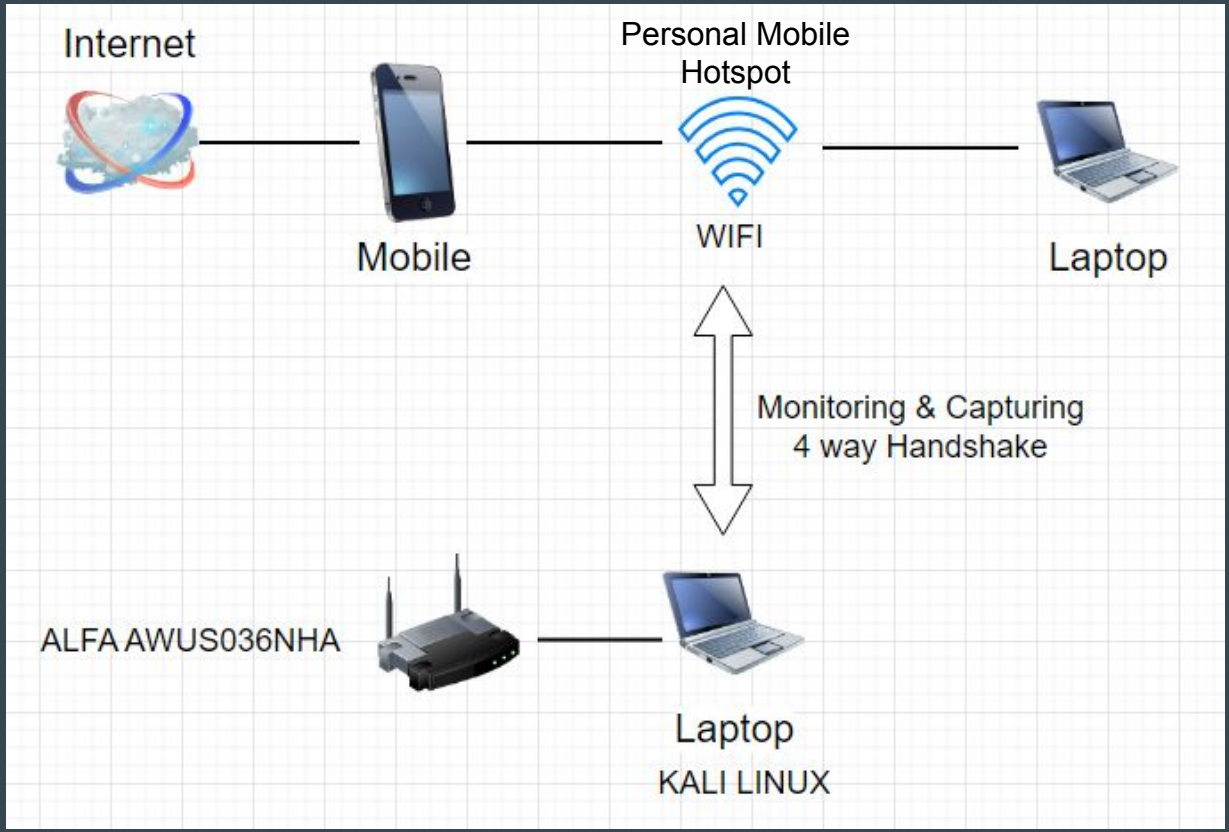
Intercepting and Cracking Traffic

- Traffic interception and cracking involves capturing, analyzing, and decrypting data on a network
- Commonly through methods like packet sniffing or network encryption cracking
- Can pose risks when misused for unauthorized data collection
- Involves breaching and monitoring network encryptions using specialised tools or software
    - Wireshark

Packet Sniffing - Intercepting and monitoring the network traffic flowing through a computer network.

Encryption Cracking - Attempting to circumvent or break the encryption on a piece of data without access to the encryption key.

Visualisation



Demonstration Preview

Tools and Devices Used

Devices

- Mobile Device for Personal Hotspot
- Laptop as a client
- Laptop with Kali Linux
- Wireless USB Adapter AWUS036NHA

Tools

- aircrack-ng
- airmon-ng
- airodump-ng
- aireplay-ng
- wireshark

The Process

- Start Kali Linux
- Connect ALFA AWUS036NHA to Laptop
- Start Monitor Mode
- Scan Networks
- Capture the information
- Open with Wireshark
- Get the 4 Way Handshake
- Crack WPA Handshake with Wordlist
    - rockyou.txt

Demonstration

Demonstration summary

Demonstration Summary

- We use Kali Linux and ALFA Network Adapter AWUS036NHA.
- Use airmon-ng to change ALFA network adapter from managed to monitor mode.
- Use airodump-ng to discover the Wifi AP (Access Point).
- Use airodump-ng to capture packet and obtain essential informations between AP and client.
- Use aireplay-ng to disconnected the client from the AP.
- Airodump-ng captured the 4 way handshakes between AP and client.
- Use wireshark to check the 4 way handshakes.
- Use aircrack-ng to crack the WPA handshakes.

Mitigation Methods

Mitigation Methods

- **Strong Passwords -** Employing the use of strong, complex passwords for your WAP.
- **Fresh Passwords -** Consistently change passwords to reduce the risk of passwords being determined
- **Use Strong Encryption Protocols -** Upgrading the network security to WPA3 offers the latest and most robust encryption standards for Wi-Fi networks. This makes it significantly harder to crack.
- **MAC Address Filtering -** Consider filtering MAC addresses to only allow authorized devices to connect to the WAP.
- **Minimal Access -** Only have hotspot on when needed, disable otherwise
- **Regularly Update Firmware -** Ensuring the WAP's firmware is up-to-date is essential to fixing potential security vulnerabilities within the device.
- **Network Name (SSID) -** Avoid using easily identifiable information in your SSID. Make it unique and not easily associated with your personal details.
- **Hide SSID -** Disable the broadcasting of your SSID to make your network less visible.

General WiFi Safety

- **Intrusion Detection and Prevention Systems (IDS/IPS) -** implementing IDS/IPS to monitor network traffic and detect any suspicious activity
- **WiFi RF Audits -** In other environments with permanent wifi, then a wifi rf audit may be applicable to reduce signal leak outside the boundaries of the office
- **Firewall Configuration ~** Configure your router's firewall settings to restrict unauthorised access. Block incoming traffic that's not needed
- **Change Default Credentials ~** Change the default username and password for your router to prevent attackers from using default credentials to access your network
- **Network Defense Systems -** Contains many technologies and practices to protect networks from unauthorised access

Nzyme - Free and open network defense system.

Conclusion