Report 1: Wireless Network Security & Threat Analysis

Shai Levin

Foreword

Wireless networks are broadcasted, allowing anyone in proximity to eavesdrop. This is unlike ethernet which requires hardware attachment to a network. As a consequence, security is a crucial element of wireless networking. This report covers two sections: a common attack to wireless networks, and a guideline for setting up a secure enterprise level network. In the conclusion we will discuss recommendations to improve potentially vulnerable networks.

Section I: Attacks

Goals

Capturing WPA-2 handshakes by means of passive traffic monitoring and a deauthentication attack. This handshake contains authentication data that can be used to crack a wireless network password. This demonstrates the vulnerability of WPA-2 and lack of important security features.

Tools Used

- A wireless card that supports monitor mode
- Kali Linux Virtual Machine using the tools: airmon-ng, aireplay-ng, airodump-np, aircrack-ng
- (For Automated Process) Raspberry Pi Zero W with Pwnagotchi installed (see https://pwnagotchi.ai/)

Steps:

Using the wireless card manually:

1. Disable DHCP client to keep our machine in stealth mode and prevent traffic requests.
2. Scan wireless signals to detect the network we wish to attack, and determine the respective BSSID & channel number.
3. Switch card to monitor mode, to monitor traffic within the network passively.
4. Once traffic has been detected from another machine to the router, a deauthentication is sent to the router spoofed to look like it comes from the other machine.

5. The deauthentication triggers a WPA-2 handshake, in which host and client will exchange authentication data. These packets are captured as pcap files.

Using the Pwnagotchi:
The Pwnagotchi is a Raspberry Pi with an OS installed that automates the process above with AI optimisation. The pcap files are retrieved from the internal storage of the Pwnagotchi via ethernet over USB. With the Pwnagotchi, the steps are made even easier as an attacker can simply walk nearby a wireless network and capture handshakes.

Decrypting the handshakes:
Once the handshakes are captured, we can use a dictionary attack and aircrack-ng to attempt to find the password.

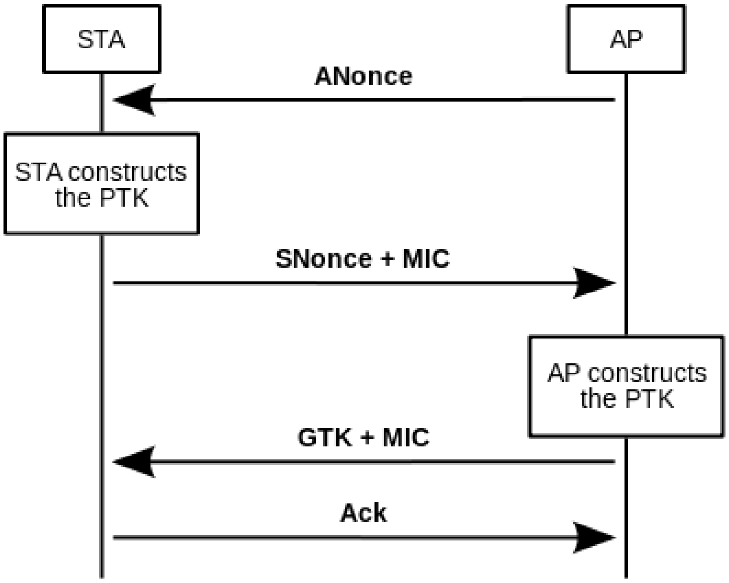

Figure 1

Threat Analysis

There are several weaknesses in WPA/WPA2 for the vulnerability exploited in this deauthentication attack:

- WPA-2 deauthentication packets are not encrypted or authenticated, so anyone who knows the BSSIDs of client/server pairs can initiate a deauth attack and retrieve the handshake data.
- WPA-2 does not provide forward secrecy, so any traffic captured can be decrypted after the password has been derived.
- See the diagram above. The handshake is cryptographically naive. The Preshared Master Key (PMK) is effectively the plaintext password. The PTK is derived directly from the password, BSSIDs of client/host, and the nonces which are

shared in plaintext! This form of key exchange relies on the difficulty of guessing the password, and provides no other security.

Needless to say, depending on your requirements, an attacker having access to your wireless network could be very dangerous. It is easy to assume that those who have access to the wireless network are already trusted, but the ease of this attack should demonstrate that this is often not the case.

There are several solutions to mitigate this attack:

- The simplest but most expensive solution: upgrading the network to use WPA3. This resolves the issues of forward secrecy and adds authentication to the de-auth packet. In addition, the handshakes are no longer able to be cracked offline.
- Deriving the password relies on a dictionary attack, so using a strong password can make it harder to derive the password even if the handshakes are captured.
- Using 2 factor authentication can further secure the network as even if the password is found, strangers cannot enter the network without 2FA.

Section II: Secure Enterprise Networks

Features

Businesses will often require a more complex network configuration than the typical consumer. This will depend on the requirements for the network. In short, the purpose of these features is **access control.** Users should only be able to access what they need to. For example, a web server might only need to accept http related traffic. We can use a firewall to constrain the network to it's requirements, preventing any forms of traffic which can be exploited by attackers.

Needless to say, using a single password for an entire corporate network presents a significant flaw. As a consequence, another constraint is login control. Enterprise hardware supports user-specific login authentication. This means users cannot access any more than they need to. Finally, using a 'Demilitarised Zone' (DMZ) network allows us to manage the traffic between trusted and untrusted sources so that untrusted sources have limited access. If security is paramount, an additional step of two-factor authentication can be implemented. This might require users to have a digital certificate file which grants them access to the network.

So, typically, the key features of a Enterprise Network are:

1. **Firewall** which restricts traffic between zones.

2. **Backend user based authentication** which allows for fine tuning of access.
3. **DMZ Network** which splits traffic between networks requiring them to pass a firewall.
4. **Two-factor authentication** is the ultimate, but inconvenient method of authentication.

Implementation

In our implementation, we are using an all-in-one enterprise device, a XTM Watchguard Router. We have the convenience of firewall, router, and access point all in one device. This allows for simpler implementation and better device support. We have chosen to use all of the features above, given the network configuration in the diagram below.

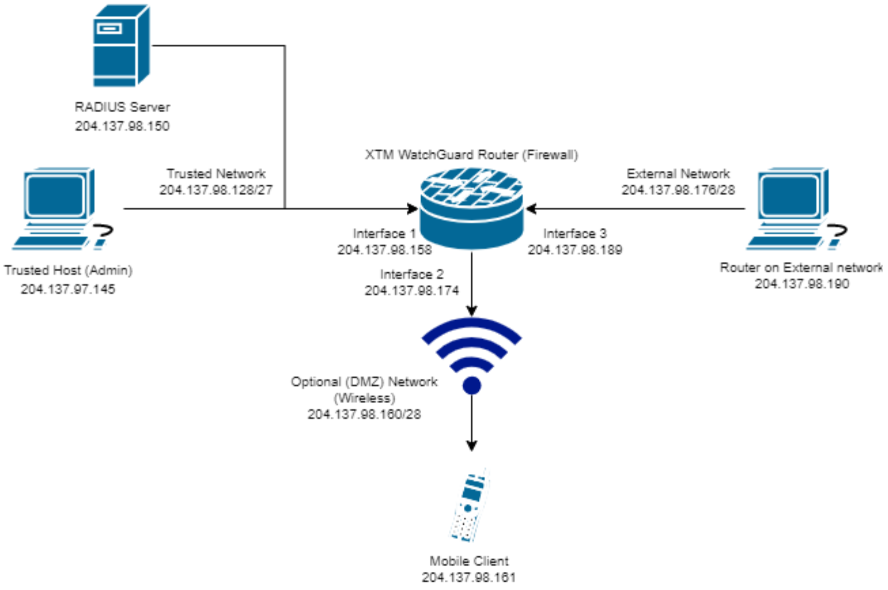

Figure 2

We use the Firebox System Manager client to configure our requirements for the network. Now, we have set up the wireless network on our optional DMZ interface. This allows us better control of what wireless network users can access in the trusted network as they must pass through the firewall. For the purpose of the example, we have configured our firewall to block any external access, and the network allows FTP, HTTP, Ping, and RADIUS traffic between the wireless network and the trusted network. The core of our secure implementation is our firewall, and the packet filters can be adjusted to suit business requirements. Thus the network implementation *relies* on a good firewall policy.

When configuring the wireless network we have several options for authentication and encryption. MAC Access control is not recommended as MAC spoofing can easily be implemented to bypass this. Using WPA3 would be ideal but is not supported. The most modern and reliable choice would be WPA2 CCMP/AES. Other options are not recommended as they are out of date and insecure. Now we have two possibilities: to authenticate via the built in Firebox server, or an external backend authentication server via RADIUS. In an enterprise network, typically we will choose the latter. We may implement digital certificates as well.

RADIUS allows us lots of flexibility in control policies via NPS, such as time-of-day restrictions, and limiting user specific access of the network. We can also set passwords to expire to force users to regularly update them.
Without 2FA, this is still technically vulnerable to the attack in Section I. If the wireless network is not locked down, and has a high level of access to the trusted network, the most secure option would be to implement 2-Factor authentication. In this implementation, each user is authenticated additionally by means of a signed digital certificate.

Now wireless devices can connect via the wireless network with the respective authentication method with their login credentials (and optionally a digital certificate).

Conclusion

We have shown a common attack on wireless networks that is extremely cheap and fast to stage, and how to integrate an enterprise level network subject to business requirements to circumvent these forms of attack. As expected, the level of security depends on the use case of the network. Conversely, the more one invests in security, the harder it will be for an attacker to break in. Here are two extreme examples to demonstrate this:

Case 1: A small coffee shop with a consumer grade wireless network.
The business requires a cheap and easy solution. They do not want the expense of an enterprise all-in-one router. Ensure the most up to date encryption package is being used i.e. WPA2 AES. Then simply choose a regularly updated password, which is sufficiently complex to be hard to crack via dictionary attack. This relies solely on the complexity of the password and it being updated regularly. There are no stop-guards, but it is extremely economical.

Case 2: A large corporate office with a business grade network.
The business has lots of sensitive data, multiple employees and is publicly visible. Relying on the implementation above would not be sufficient, and an implementation might look something like that in Section II.

One final take away from this report, is that **strong, hard to guess passwords that are regularly updated** are the key to preventing easy network penetration.

References:

- Figure 1:Taken from https://en.wikipedia.org/wiki/IEEE_802.11i-2004#/media/File:4-way-handshake.svg
- Figure 2: Made using draw.io
- See https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Security_Considerations_201911.pdf for information on WPA3 improvements