Known Wireless Attacks

Scott Armitage, Loughborough University October 2011

Wireless networks have become ubiquitous as a means of connecting to a network. It is unlikely that there are any remaining academic institutions in the UK which don't offer some kind of wireless networking. However, many wireless network operators have little knowledge regarding the possible ways in which their wireless infrastructure can be attacked. This document briefly describes some of the common attacks which can be performed against IEEE 802.11 based networks.

Denial of Service (DoS) Attacks

Jamming

Jamming works simply by generating Radio Frequency (RF) noise in the frequency range used by wireless networking equipment (2.4GHz and 5GHz). This can often be accidental, particularly in the 2.4GHz range, as certain devices will either operate naturally in these frequency ranges e.g. microwaves, baby monitors, radar etc. Through their everyday use, these devices can disrupt wireless networks operating nearby. In addition to accidental noise, devices can be built which generate noise to deliberately interfere with 802.11 wireless networks.

Authentication / Association Flooding

One way in which a wireless network can be attacked is to try to flood the Access Point (AP) with authentication and association frames. To association flood, the attacking device will spoof its wireless MAC address then, rapidly and repeatedly, try associating to the AP. At each attempt the attacker will change its MAC address, mimicking the existence of many clients. This has the affect of consuming the AP's memory and processing ability, denying service to legitimate clients.

De-Authentication Flooding

This attack works by exploiting a flaw in the wireless state machine and is commonly used as a method to contain rogue APs. The attack works by sending de-authentication packets to clients connected to an access point. The clients receiving the de-authentication will disassociate from the AP immediately. This attack works because AP control traffic is not protected and therefore the de-authentication frame is sent in clear text making it very easy to spoof. This attack can target a whole AP, by sending the de-authentication frames to the broadcast MAC address and spoofing the source as the AP. Alternatively the attack can be targeted at a single client, by sending the de-authentication frame to a single client station.

This attack can be mitigated through the use of IEEE 802.11w (Protected Management Frames) which encrypts the control traffic between the AP and the clients. However, currently 802.11w isn't widely supported or implemented.

TKIP Countermeasure

One of the features of Temporal Key Integrity Protocol (TKIP) is the use of a Message Integrity Check (MIC). However due to MIC being cryptographically weak, countermeasures exist in TKIP to prevent key retrieval. If two incorrect MIC frames arrive within one minute of each other, the AP will implement the cessation of all TKIP activity for sixty seconds followed by the renegotiation of group and all pairwise keys. This provides attackers with the ability to deny service to the AP by sending invalid MIC frames. This attack not only performs a one minute DoS of TKIP clients but also AES clients, as the AP will use the TKIP group key for AES clients if there are any TKIP clients associated to the AP.

Extensible Authentication Protocol (EAP) Attacks

EAP authentication flooding works by a client, or multiple clients, flooding a protected wireless network with EAP authentication requests. This can have the effect of performing a DoS on the RADIUS server if it is unable to handle the volume of authentication requests from the client.

This attack can be mitigated by implementing a temporary block (e.g. 60 seconds) after three failed attempts, on a client trying to EAP authenticate. This mitigation also prevents attempts by clients to brute force attack the user credentials.

As well as authentication flooding, clients can try to use various EAP packets to induce a DoS attack:

- Some APs can be crashed by flooding the AP with EAPOL-Start frames. Most modern equipment should not be susceptible to this attack.
- Some APs can be DoS attacked by the attacker cycling through the EAP Identifier space (0 – 255). Modern APs should not be susceptible to this attack as the EAP Identifier space is only unique to the 802.11 association, with each association having its own EAP Identifier space.

Cipher Attacks

WEP Attacks

Wired Equivalent Privacy (WEP) is relatively trivial to defeat and numerous attacks exist which can either decrypt WEP protected packets or recover the WEP key. WEP has been broken for more than 10 years and should not be used to secure a wireless network. Documented methods for breaking WEP include:

- FMS – which uses predictability of the first few bytes of packets. On a busy network the key can be recovered in couple of minutes.

- KoreK – which uses a similar approach to the FMS attack but requires fewer packets
- PTW – Requires fewer packets than previous attacks
- ChopChop - which can decrypt data packets without the need to recover the key.

WPA-PSK Dictionary Attack

Whilst the security mechanisms in Wi-Fi Protected Access (WPA) and WPA2 make the protocol secure there is a weak point in the system: the passphrase. Users configuring WPA/WPA2 passphrases often choose short, dictionary based passphrases leaving them susceptible to attack. Attackers can capture packets during the key exchange phase of a client joining a wireless network then perform an offline dictionary attack to obtain the WPA/WPA2 passphrase.

WPA/TKIP

It is possible to decrypt packets which have been protected using Wi-Fi Protected Access/Temporal Key Integrity Protocol (WPA/TKIP). The TKIP attack works in a similar way to the WEP chopchop attack and can provide the cleartext data but doesn't expose the key. This attack relies on the attacker knowing most of the bytes of the IPv4 address range in use on the wireless network.

This attack can be mitigated with a short rekeying time (120 seconds or less). However, the recommend solution would be to use WPA2/AES.

LEAP Attacks

Lightweight Extensible Authentication Protocol (LEAP) is an authentication mechanism implemented by Cisco which can be used to secure a wireless network. LEAP allows authentication via Microsoft's Challenge-Handshake Authentication Protocol (MS-CHAP) and provides dynamic key exchange. However, credentials are not strongly protected, leaving LEAP open to attack. Due to the lack of protection of the authentication mechanism it is possible to perform an offline dictionary attack on captured packets and obtain a user's credentials.

It is recommended that sites do not use LEAP, but instead use a more robust authentication mechanism such as PEAP, EAP/TTLS or EAP/TLS etc.

Man-in-the-Middle Attacks

Captive Portal (Evil Twin)

Walled garden wireless networks are particularly vulnerable to man-in-the-middle attacks. This is because there is no automatic checking of the certificate provided by the authentication server. As users simply use a web browser to login to the network, an attacker need only setup their own login page, which

looks identical to the real one, and capture credentials as people attempt to login. The attacker can even act as proxy passing the credentials onto the real authentication server. This kind of attack is often called an 'evil twin'.

802.1X / EAP

Whilst a properly implemented WPA/WPA2 Enterprise network using 802.1X authentication is secure and not vulnerable to a man-in-the-middle attack, many clients are incorrectly configured, leaving them susceptible to an attack. The vulnerability arises from the use of a certificate to verify the RADIUS server. Many clients will configure their device so that it does not reject certificates provided by the RADIUS server. These may be signed by the wrong certificate authority and/or have the wrong common name. To ensure they are not vulnerable when authenticating to their wireless network, clients should only accept certificates from the correct certificate authority with the correct common name. By accepting any certificate, a malicious AP can use either a self-signed certificate or a certificate signed by the correct certificate authority (if a public certificate authority is used) to intercept credentials. Often an attacker will send a de-authentication frame to a client that is already authenticated to a genuine AP, forcing it to re-associate.

It is advisable that when implementing enterprise wireless, sites should not use public certificate authorities. This will help to prevent attackers obtaining certificates from the same certificate authority (with a different common name) and attempting a man-in-the-middle attack.

Eavesdropping

Open Network

On an open wireless network, it is trivial to capture packets in the air as they are sent in the clear.

WPA/WPA2-PSK

It is a common misconception that because data is encrypted on a WPA or WPA2-PSK client, it is protected from snooping by other users. Unfortunately this is not the case. Since every client uses the same pre-shared passphrase, they can decrypt another user's packets. This is not true for WPA and WPA2 Enterprise where each user has an individual, rotating, key sent from the RADIUS server.

Captive Portal

Once a client is logged in to a captive portal, unless protected by other means (such as a Virtual Private Network (VPN)), their traffic is sent in the clear. This means all the wireless traffic of an authenticated client can be easily sniffed. Some users may be under the impression that because they have had to authenticate, that their data is secure.

Conclusion

Whilst a number of different attacks exist for wireless networks many of these can be mitigated through the use of existing technologies and best practice. Attacks on management traffic such as de-authentication packets can be mitigated through the use of protected management frames e.g. 802.11w. Other risks can be reduced through using 802.1X authentication and educating users about the need to check the validity of the radius server certificate presented to them. Probably the most important mitigation is to use WPA2/AES encryption combined with a properly implemented 802.1X authentication system. This will provide users with the most secure wireless network experience.