Wi-fi networks

Threats

Unauthorised connection to a shared medium: restricting the physical access to Wi-Fi networks is much harder to enforce than restricting access to wires and switches

Intercepting data transmitted over radio waves: after attackers identify an access point, they can intercept and log every transmission sent through the AP from a safe distance

Spoofing a trusted user. Even if an access point does not broadcast its SSID and uses MAC address filtering, an attacker can intercept data sent by an authenticated user and retrieve the MAC address and SSID contained in the packets. Once this is done, it is enough to use this information to establish a new connection with the Wi-Fi network

Wi-fi networks

Threats

Blocking access points. Generating a radio wave with the right frequency will make it impossible for legitimate users to connect to their Wi-Fi network

Rogue access points. Because client computers connect with an access point that produces the strongest signal, launching a rogue access point can mean computers will send all data through an attacker-controller device

Client attacks

Launching a rogue access point

The most popular attack that targets wireless clients involves launching a rogue access point

It may be launched in public. All an attacker has to do is to run a an access point that has a legitimate-looking SSID

Since the goal of this attack is to persuade users to transfer their data across this AP:

- The networks are unprotected (open) — everyone can connect to them
- The access point works as a router — after the connection is made, users receive Internet access

Client attacks

Launching a rogue access point

If the attacker wants to obtain users credit card details and cheat them out of money, the first page they will see while trying to connect is a spoofed website that looks like the real Internet provider website and a request to make a payment for Internet connection

The only way you can avoid this threat is to never use open wireless networks

Client attacks

Launching a rogue access point

If the attacker wants to break into a client computer, in all likelihood users will receive free Internet access: this time the attack relies on eavesdropping on data sent and received by clients and modifying it on the fly

While simply connecting a user to a rogue AP does not enable attackers to configure a proxy server client-side, most access points are simultaneously DHCP servers

Client attacks

Launching a rogue access point

Using this server, you can for example set up a DNS server: to control all packets sent by clients, an attacker only needs to run a DNS server that will respond to all web server IP requests with providing requesters with the same rogue proxy server address. This can be done for example by adding an unnoticeable image (1x1 pixel) stored on a local share to every requested website: by using Fiddler to inject the following tag into every page:

While displaying a page, a browser will automatically try to download this image and connect to the share that stores it. Windows uses authenticated user credentials to connect to local network shares, so this means a user's NTLM or LM credentials will be sent to the 10.0.0.1 server

Client attacks

Launching a rogue access point

The attacker will be able to not only crack the user's password based on these credentials, but also use them to spoof the user

Equally prevalent are attacks that use a proxy server and the ability to modify data transmitted between a client and web server that rely on filling text fields in displayed websites: in this case an attacker places scripts that redirect users to the web servers he controls on selected websites (an XSS attack)

Client attacks

Launching a rogue access point

Increasingly popular are attacks related to modifying executables users download. Since http does not verify the authenticity of downloaded packets, and majority of files are shared using this protocol, an attacker might be able to add fragments of malicious code to these files

As a result, when a user opens a file downloaded from a secure, trusted website, in reality the file may come with a code injected by an attacker. While today systems run warning windows when you try to open a program downloaded from the Internet, most users tend to ignore them, especially if the file is from a secure and trusted website

Client attacks

Launching a rogue access point

Also access points may be used to run these attacks. They can be made to listen on for inbound requests to connect to wireless networks with a specified SSID and automatically run a Wi-Fi network with the same SSID. If a client computer is configured to automatically connect to an open network with a specified SSID when it's found, you can fall victim to this attack by simply turning on your computer and activating its NIC

But if you choose to use open networks regardless, immediately after you connect, remember to set up a secure VPN connection with a trusted server and make sure the data you send really is transmitted using the VPN connection

Client attacks

Evil twin

In this attack, an access point is configured to pretend to be the enterprise access point on premises: it's a rogue AP that is set for a network that holds the same SSID but has a stronger signal

Because most enterprise networks are protected using WPA2 or WPA, to make a client connect to a malicious access point the AP also has to be protected in the same way

Also, most corporate networks run in the Enterprise mode: they use a RADIUS server to authenticate users

Attackers have bypassed this problem: they can make the RADIUS server of their rogue AP authenticate all users regardless of the credentials they send

Client attacks

Evil twin

To connect to this access point, you don't need to submit the WEP shared key or have the correct user credentials

If user credentials are sent in plaintext (and with EAP-PAP they are), the attacker already has obtained them at this point

If more secure authentication protocols are used, the attacker not only has the data necessary to crack the credentials, but can also use an encrypted version of the credentials

Next, a rogue access point sends the intercepted credentials to the enterprise access point and establishes a connection with the enterprise network for the user

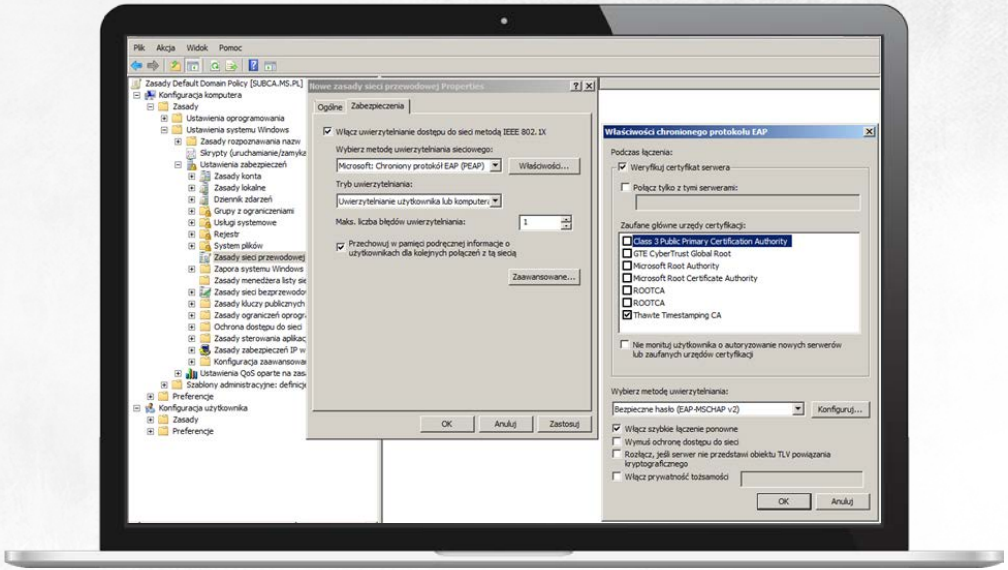
From this point, the attacker can intercept and modify all data sent and received by the user in this way

Client attacks

Evil twin

You can use Wireless Network Policies to protect the network against evil twins

Apart from picking a secure authentication method, force clients to check the RADIUS server identity by verifying the certificates issued for the server



Client attacks

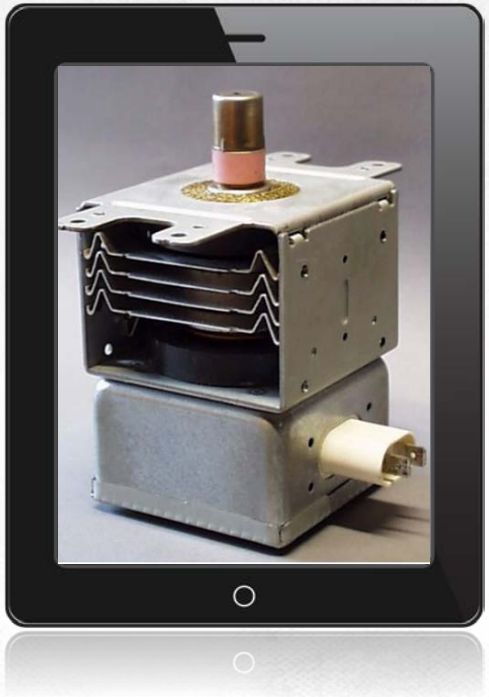
Denial of service

DOS attacks can be run using a device that radiates a strong electromagnetic signal, for example the magnetron, which can be found in every kitchen in a microwave oven

The basic preventive measure that secures wireless networks against infrastructure attacks is not using the WEP standard

WPA and WPA2 can also be susceptible to:

- Dictionary attacks targeting pre-shared keys (coWPAtty)
- Brute-force attacks using programs that use graphics processing units (Elcomsoft Wireless Security Auditor)
- Attacks targeting PSKs stored client-side (Proactive System Password Recovery)

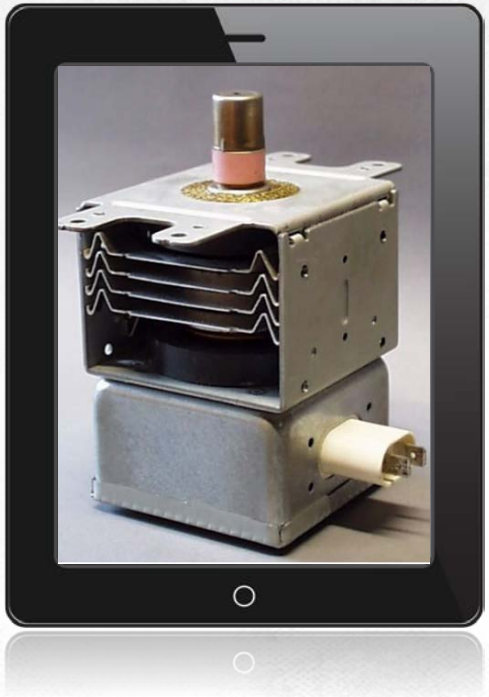


Client attacks

Denial of service

Securing wireless networks effectively requires:

- Authenticating users using the 802.1x protocol
- Securing data transmitted in the network using the 802.11i WPA2 standard



infrastructure attacks

Network intrusions

Client attacks primarily exploit weak authentication methods used

Wireless infrastructure methods are based on weak encryption of data transmitted in these networks

You can find tools online that fully automate Wi-Fi network intrusions

infrastructure attacks

Network intrusions

Most Wi-Fi client attacks require attackers to intercept packets sent over radio waves but also send the packets to access points

NIC drivers for Windows prevent active communication with an access point with which a computer is not yet connected to

exercise

Infrastructure Attacks

Breaking into a WEP/WPA network

THANKS