Wireless and mobile device attacks

Grayware and SMiShing

Grayware

**Is any unwanted application that behaves in an annoying or undesirable manner**.

And while *it may not carry any* recognizable *malware, it may still pose a risk* to the user by, for example, tracking your location or delivering unwanted advertising.

*Authors of these typically maintain legitimacy by including these ‘gray’ capabilities in the small print of the software license agreement.*

This factor poses a growing threat to mobile security in particular, as many smartphone users install mobile apps without really considering this small print.

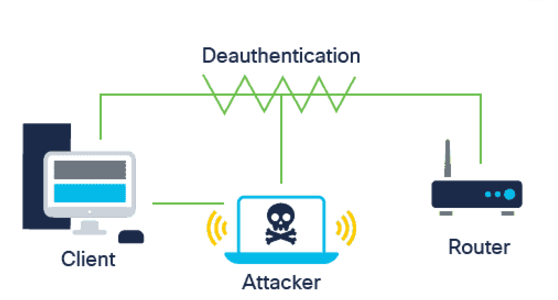
Short msg service phishing (SMiShing)

Is another tactic used by attackers to trick you. **Fake text msges prompt you to visit malicious website or call a fraudulent phone number**, *which may result in malware being downloaded onto your device or personal info being shared*.

Rogue access points

A rogue access point is a **wireless access point installed on a secure network without explicit authorization**, it also presents an opportunity for attackers looking to gain access to an organization's network.

An attacker will often use social engineering tactics to gain physical access to an organization’s network infrastructure and install the rogue access point



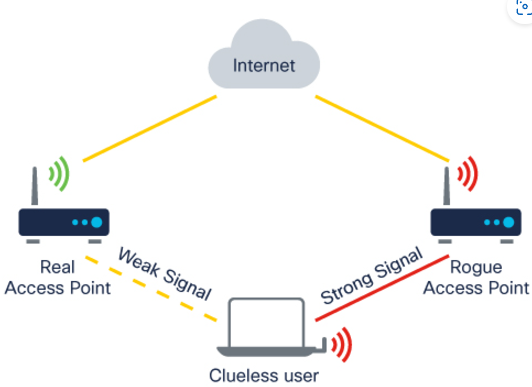
Also known as criminal’s access point,

**the access point can be set up as a MitM** device to capture your login info,

This works by disconnecting the rogue access point, which triggers the network to send a deauthentication frame to disassociate the access point.

This process is then exploitet by spoofing your MAC address and sending a deauthentication data transmission to the wireless access point.

--



An evil twin attack

describes a **situation where the attacker’s access point is set up to look like a better connection option**.

Once your connect to the evil access point, the attacker can analyze your network traffic and execute MitM attacks.

Radio frequency jamming

**Wireless signals are susceptible to**

electromagnetic interference (EMI),

radio frequency interference (RFI) and even

lightning strikes or noise from fluorescent lights.

Attackers can take advantage of this fact by deliberately jamming the transmission of a radio or satellite station to prevent a wireless signal from reaching the receiving station.

*In order to successfully jam the signal, the frequency, modulation and power of the RF jammer needs to be equal to that of the device that the attacker is seeking to disrupt*.

Bluejacking and bluesnarfing

**Due to the limited range of Bluetooth, an attacker must be within range of their target**.

Bluejacking

**Uses wireless Bluetooth technology to send unauthorized messages or shocking images to another Bluetooth device.**

Bluesnarfing

Occurs when an **attacker copies information, such as emails and contact lists, from a target’s device using a Bluetooth connection**.

Attacks against Wi-Fi protocols

Wired equivalent privacy (WEP) and   
 Wi-Fi protected access (WPA)

Are **security protocols that were designed to secure wireless networks** that are vulnerable to attacks.

WEP

Developed to **provide data transmitted over a WLAN with a level of protection** **comparable to** what is usually expected of a traditional **wired network**.

It **added security to wireless networks by encrypting the data**

It used a key for encryption. The problem, however, was that WEP *had no provision*  *for key management* and so the number of people sharing the same key continually grew, giving criminals access to a large amount of traffic data.

Furthermore, WIP’s initialization vector, one of the key components of its *encryption key, was too small, readable and static*

WPA

Were developed to address the problems of WEP

Unlike with WEP, an attacker cannot recover WPA2’s encryption key by observing network traffic. However, they can still use a packet sniffer to analyze the packets going between an access point and a legitimate user.