Research Paper Summary 1 – Justin Tobiason

Compared to the early 2000s, Wi-Fi equipped devices really have taken the world over. Given that an estimated 18 billion devices have this capability. This is the reason we attack against wireless devices and their defenses are so important.

One of these attacks is the deauthentication attacks. Simply this attack forces a legitimate connection to an endpoint to disconnect opening a vector for potential manipulation and attack. Whether a deauthentication attack is used to prevent a device from working like in the form of a wireless security camera or to attempt a type of spoofing attack and tricking the victim, it can be used maliciously. Leveraging deauthentication with an Evil Twin attack creates a scenario where a user will probably choose the device to be used in acquiring information from the device via a man-in-the-middle attack.

The research found that devices that could contain auto-connection would connect to the evil twin of the access point currently being attack with deauthentication. This was proven to be most effective in getting a device to communicate across the manipulated access point.

WPA 2, based on this paper, is still the most popular security protocol which was created back in 2004. Since then, WPA3 has been released. The big difference between them is how the management frames are handled. In WPA2 the frames are not authenticated so it’s easy to spoof and in WAP3 they use Management Frame Protection MFP which helps mitigate deauthentication and Disassociation attacks. However, this only works if the protocol is being used and since .23 percent of networks currently use this standard most people don’t benefit from it.

Deauthentication works by obtaining the Media Access Control or access point by using a packet sniffing tool. Once it has this information the attacker has an opportunity to send a deauthentication management frame with a spoofed address of the access point or the victim of the device. Once the victim is disconnected the attack is successful.

Evil Twin works by spoofing a legitimate ap by copying its SSID and MAC address. The attacker can acquire this information by positioning a compatible Wi-Fi adapter and device within the communication range or the access point to be attacked. Using a tool like Airgeddon this tool creates a vector of attack using Aircrack-ng and MDK4 (both tools of Wi-Fi exploitation). Once it’s set up these tools make it possible for the device to auto-connect to it.

An interesting find in their experimentation was how simple it was to setup a deauthentication attack. Especially with the fact that they used a Rasberrry Pi and Macbook. The reset of the setup really uses the software Airgeddon. Given the author’s findings not only were they able to conduct deauthentication attacks on all the cameras except Google Nest, but the attack didn’t require sending management frames meaning it could work on WPA3 supported devices. Another interesting finding was that of the Ring Stick Up camera. After the deauthentication attack it would become completely unresponsive. Essentially disabling the device completely making it useless unless completely rebooted.

Possible mitigations included using a VPN to make MITM attacks difficult or impossible. This includes end-to-end encryption of the network traffic from source to destination. A whitelist of BSSIDs or MAC addresses that belong to the organization. An access point with a SSID that matches but a BSSID that is not part of the whitelist could mean an evil twin setup. For cameras, at least, having physical storage on the device means that footage won’t be completely lost. Finally, the last suggestion was to have vendors test their products against these attacks. Given it should be a vendor responsibility this makes the most sense to create a secure wireless device.

**Source:**

Z. Neal and K. Sha, "Analysis of Evil Twin, Deauthentication, and Disassociation

Attacks on Wi-Fi Cameras," 2023 32nd International Conference on Computer

Communications and Networks (ICCCN), Honolulu, HI, USA, 2023, pp. 1-7, doi:

10.1109/ICCCN58024.2023.10230183. keywords:

{Surveillance;Cameras;Computer security;Wireless fidelity;Testing;Business;Evil

Twin;Deauthentication;Disassociation;Wi-Fi;Cameras;WPA2/3;Wireless Security},