Cyberint
Protection Beyond the Perimeter

KRACK Attack

WPA2 Wi-Fi Vulnerability

www.cyberint.com

Cyberint
Protection Beyond the Perimeter

Contents

Executive Summary

In October of 2017, a researcher by the name of Mathy Vanhoef released his research titled "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2". The research describes techniques that can be used to decrypt traffic on nearly any WPA2 encrypted network, which is most commonly used for wireless network security.

The Key Reinstallation Attack method described in the research effects both sides of the Wi-Fi networks. Including devices like computers, smartphones, gaming consoles, cameras and other smart devices are affected by this attack, as well as the Wireless access point, what makes this attack potential effect extremely wide.

Key Points

- Vulnerability in WPA2 encryption algorithm, which effects almost every wireless device
- Enable an attacker to gain access to sensitive information by breaking the WPA2 encryption
- The attack works on all modern protected networks
- Although there is no evidence of this technique being used in the wild, it is our assessment that attackers will make use of those techniques to enhance their attack toolkit.

Technical Analysis

In October of 2017, a researcher by the name of Mathy Vanhoef released his research titled "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2". The research describes techniques that can be used to decrypt traffic on nearly any WPA2 encrypted network, which is most commonly used for wireless network security.

The Key Reinstallation Attack method described in the research effects both sides of the Wi-Fi networks. Including devices like computers, smartphones, gaming consoles, cameras and other smart devices are affected by this attack, as well as the Wireless access point, what makes this attack potential effect extremely wide.

An attacker in range of a victim can exploit these weaknesses using key reinstallation attacks (referred to as (KRACKs) by the researcher who discovered this vulnerability). Concretely, attackers can use this novel attack technique to read information that was previously assumed to be safely encrypted. This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on.

The attack works against all modern protected Wi-Fi networks, depending on the network configuration, it is also possible for the attack to inject and manipulate data. Such as injecting malware into websites and so on.

This vulnerability originates in a weakness within the Wi-Fi standard itself, this fact effects virtually every wireless enabled device in existence. To prevent this attack users and organizations must update their devices as soon as the manufacturer releases a security update for this vulnerability.

The main attack technique is against what is referred to as the 4-way handshake of the WPA2 protocol. This handshake is executed when a client wants to join a protected Wi-Fi network, and is used to confirm that both the client and access point possess the correct credentials.

At the same time, the 4-way handshake also negotiates a fresh encryption key that will be used to encrypt all subsequent traffic. Currently, all modern protected Wi-Fi networks use the 4-way

handshake. This implies all these networks are affected by (some variant of) our attack. For instance, the attack works against personal and enterprise Wi-Fi networks, against the older WPA and the latest WPA2 standard, and even against networks that only use AES.

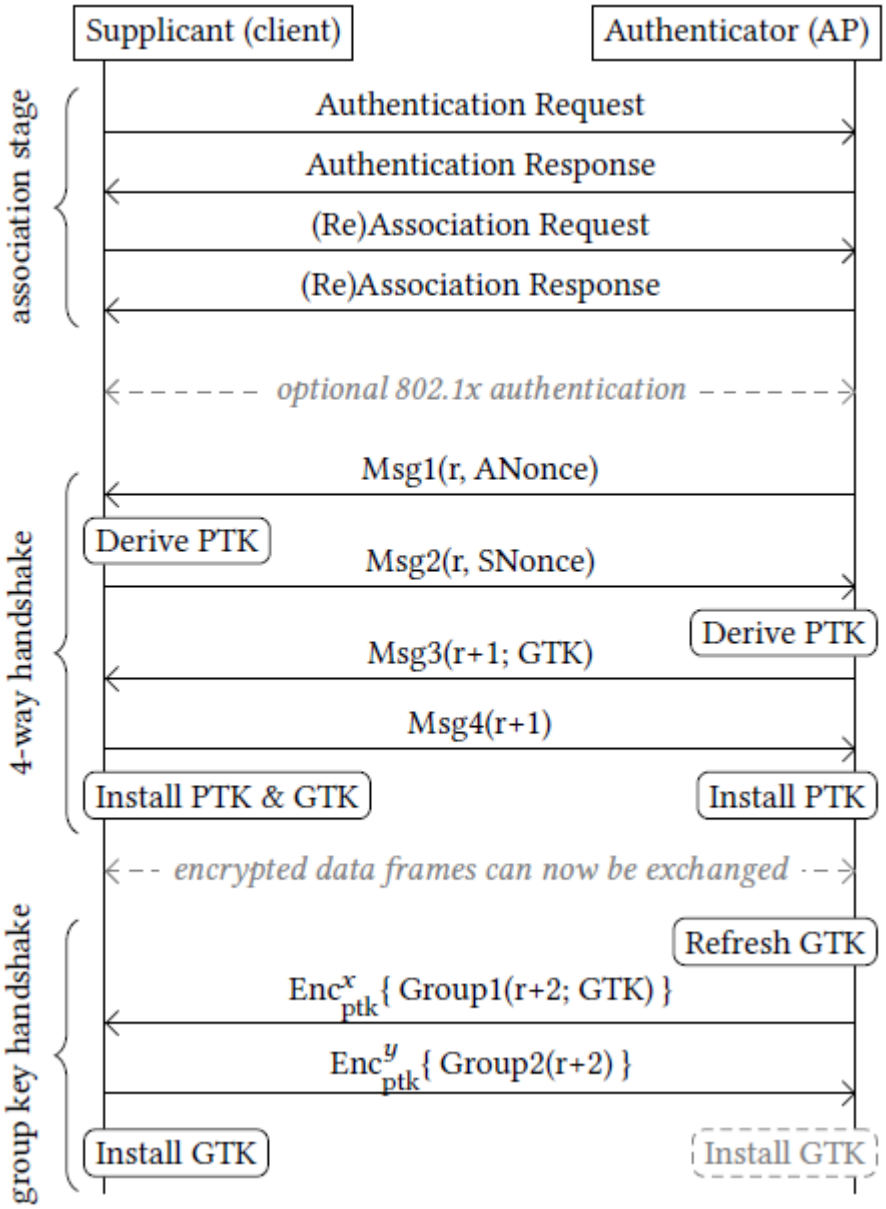

Figure 1.0

The research paper describes the idea behind the key reinstallation attack can be summarized as follows. When a client joins a network, it executes the 4-way handshake to negotiate a fresh encryption key. It will install this key after receiving message 3 of the 4-way handshake. Once the key is installed, it will be used to encrypt normal data frames using an encryption protocol. However, because messages may be lost or dropped, the Access Point (AP) will retransmit message 3 if it did not receive an appropriate response as acknowledgment. As a result, the client may receive message 3 multiple times. Each time it receives this message, it will reinstall the same encryption key, and thereby reset the incremental transmit packet number (nonce) and receive replay counter used by the encryption protocol. By forcing nonce reuse in this manner, the encryption protocol can be attacked, e.g., packets can be replayed, decrypted, and/or forged. The same technique can also

be used to attack the group key, PeerKey, TDLS. Based on the research we assess that the that the most widespread and practically impactful attack is the key reinstallation attack against the 4-way handshake. As the research shows, this technique effects most clients connected to the network and can be used to decrypt packets sent by clients, allowing them to intercept sensitive information such as passwords or cookies. Decryption of packets is possible because a key reinstallation attack causes the transmit nonces (sometimes also called packet numbers or initialization vectors) to be reset to zero. As a result, the same encryption key is used with nonce values that have already been used in the past.

The ability to decrypt packets can be used to decrypt TCP SYN packets. This allows an adversary to obtain the TCP sequence numbers of a connection, and hijack TCP connections. As a result, even though WPA2 is used, the adversary can now perform one of the most common attacks against open Wi-Fi networks: injecting malicious data into unencrypted HTTP connections. For example, an attacker can abuse this to inject malware into websites that the victim is visiting.

Outlook and Implications

Exploiting this vulnerability does not require a man-in-the-middle position! Instead, an adversary merely needs to capture a Fast BSS Transition handshake and save the FT Reassociation Request. Because this frame does not contain a replay counter, the adversary can replay it at any time (and arbitrarily many times). Each time the vulnerable AP receives the replayed frame, the pairwise key will be reinstalled.

An adversary can trigger FT handshakes at will as follows. First, if no other AP of the network is within range of the client, the adversary clones a real AP of this network next to the client using a wormhole attack (i.e. we forward all frames over the internet). The adversary then sends a BSS Transition Management Request to the client. This request commands to the client to roam to another AP. As a result, the client will perform an FT handshake to roam to the other AP.

It is in our assessment that adversaries will in the near future include this technique to improve their toolkits, and take advantage of the fact that this vulnerability effects all modern connected devices, which can provide them many avenues to conduct their operations, whether it be for financial gain or espionage.

Countermeasures

- Check your Wi-Fi manufacturer website for related security patches and apply then as soon as possible, major vendors has already released security patches to address this issue
- Update your computers, Microsoft has already released a patch for this vulnerability and while it can be downloaded directly from this page, it should be included in system updates. On Windows 10, updates can be checked for through the *Settings* window under the "Update & Security" menu. On prior Windows versions, this is available through the Control Panel within the *System and Security* category as "Windows Update."
  On macOS (previously Mac OS X), within the Apple menu, open "System Preferences" and select "App Store" from the list. Ensure that "Automatically check for updates" is enabled and your system is up to date. If you are using Linux, a patch is already available and ported to several distributions. On Debian-based systems like Ubuntu, we can update our system using sudo apt-get update && sudo apt-get upgrade
- Update your mobile devices, On Android, updates can be checked for and installed within the "About device" or "About phone" section of the Settings menu. Specifically look at "Download

updates manually" and "Android security patch level" to make sure that your phone is up to date.

- Unfortunately, Google will not be releasing a patch for this exploit until November 6 (and even then, that will only go out to their latest stock Android devices). As such, if you use an Android phone, your only option is to disable Wi-Fi and use your cellular data if you're doing something online that your worried others may be eavesdropping on. Just remember, in order to execute the attack, someone will have to have a device physically in between you and the router. On iOS devices, such as iPhones and iPads, you would go to "General" in the Settings app, then select "Software Update." If there is an update, you should update immediately.
- Do not access sensitive resources while on untrusted networks, like your bank account or any sensitive corporate resource
- Make sure to enable SSL encryption, make sure webservices are SSL enables by checking the small lock icon on top right hand of the address bar.

- Make sure to enable 2FA (Two-Factor Authentication) to all your sensitive resources like you bank account or any service that require online payment.
- Use the following tool to test if your Wi-Fi device is vulnerable to the KRACK Attack