Project Proposal

Key Reinstallation Attacks on Wi-Fi Networks

we're all gonna die

Gurpreet Singh, Konrad Pfundner, Logan Kember, Fernando Campos

 # 250674134, 111111111, 111111111, 111111111

Software Developers

Contents

Attack Description

Since it's introduction in 2006, WPA2 has become the most popular protected access technology used in the consumer industry. Almost every household WiFi network is currently making use of WPA2 to authenticate its devices. Vanhoef [2017]

On October 16th, 2017 a flaw was found in the WPA2 protocol, making every device using it to connect to a Wi-Fi network vulnerable and helpless to hackers. No matter the encryption method, from WPA2 to AES, hackers are able to decrypt any data sent by the victim. In fact, because this is a man in the middle attack, the device can be tricked into using an all-zero encryption key. If no other form of encryption is utilized (HTTPS), the attacker will have access to unencrypted and human-readable data, even when it comes to sensitive information like usernames, passwords, and credit-card information. If that isn't bad enough, it is even possible to inject ransomware or malware into websites. Meaning, this is not only bad for the users but also the web providers. The worst part is that there is no way to stop this, other than hardwiring the device, or hoping the manufacturer of the device offers an update that patches this attack.

The method of using this weakness in Wi-Fi is called a Key Reinstallation Attack (KRACK). Every modern Wi-Fi standard uses a 4-way handshake to connect. This is where the server and client agree on an encryption key to use when encrypting and decrypting all future messages. The attack occurs in the third message of the 4-way handshake. What happens is the hacker tricks the victim into reinstalling the encryption key that is already in use. This is achieved through manipulation and replaying of cryptographic handshake messages. Theoretically, it should not be possible to install the same key multiple times in a row, but because it is very common for messages sent over Wi-Fi to get lost, many messages in this handshake may need to be retransmitted. This makes the attack able to reset the nonce any time it retransmits this third message, enabling packets to be replayed, then decrypted and even forged. The whole purpose of this nonce was to ensure that past massages could not be reused in replay attacks.

There are many variations of this attack that have been discovered that have varying levels of impact. One of the worst and most devastating is being able to reinstall an all-zero encryption key. Being the worst variation one would hope it is not too common, however, all devices using Linux or Android 6+ are susceptible. This all-zero encryption key makes it easy to manipulate and

intercept data sent at will since all of this data is now readable text. With so many Linux and Android devices present, this is especially scary and concerning. Even more so with their only hope being to wait for a security update to fix this vulnerability.

The Goal

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce porta mauris sit amet finibus lacinia. Nunc id pharetra tortor, quis scelerisque tellus. Nunc at est nec sapien tincidunt ultricies a quis mi. Curabitur sed sem vitae ipsum varius molestie. Integer sed arcu velit. Fusce ornare malesuada dolor, ut finibus arcu ornare ut. Nam tincidunt sem in tempor pellentesque. Integer efficitur, nisl vel euismod ultricies, nisl orci volutpat orci, nec ultrices nisi tortor id eros.

Proposed Solution

Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce porta mauris sit amet finibus lacinia. Nunc id pharetra tortor, quis scelerisque tellus. Nunc at est nec sapien tincidunt ultricies a quis mi. Curabitur sed sem vitae ipsum varius molestie. Integer sed arcu velit. Fusce ornare malesuada dolor, ut finibus arcu ornare ut. Nam tincidunt sem in tempor pellentesque. Integer efficitur, nisl vel euismod ultricies, nisl orci volutpat orci, nec ultrices nisi tortor id eros.

Technology Breakdown

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce porta mauris sit amet finibus lacinia. Nunc id pharetra tortor, quis scelerisque tellus. Nunc at est nec sapien tincidunt ultricies a quis mi. Curabitur sed sem vitae ipsum varius molestie. Integer sed arcu velit. Fusce ornare malesuada dolor, ut finibus arcu ornare ut. Nam tincidunt sem in tempor pellentesque. Integer efficitur, nisl vel euismod ultricies, nisl orci volutpat orci, nec ultrices nisi tortor id eros.

Mockups

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce porta mauris sit amet finibus lacinia. Nunc id pharetra tortor, quis scelerisque tellus. Nunc at est nec sapien tincidunt ultricies a quis mi. Curabitur sed sem vitae ipsum varius molestie. Integer sed arcu velit. Fusce ornare malesuada dolor, ut finibus arcu ornare ut. Nam tincidunt sem in tempor pellentesque. Integer efficitur, nisl vel euismod ultricies, nisl orci volutpat orci, nec ultrices nisi tortor id eros.

References

Mathy Vanhoef. Key reinstallation attacks, 2017. URL www.krackattacks.com.