Proposal: Key Reinstallation Attacks on Wi-Fi Networks

Gurpreet Singh, Konrad Pfundner, Logan Kember, Fernando Campos
The University Of Western Ontario

Abstract

Bringing awareness to new attacks that expose the majority of WiFi networks. This proposal discusses the importance of recent attacks executed on the WPA2 protocol and proposes the creation of a mobile application that can showcase and exploit wireless APs.

1. 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.

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.

2. The Goal

With this project we are trying to educate average Wi-Fi users and show them the power of this exploit. The only way to eliminate this attack vector is to patch every access point. If consumers are not concerned with this attack manufacturers are not going to be motivated to produce a patch for their devices. Therefore, we are hoping that consumers see the effects of a key reinstallation attack and show manufacturers that they need an update. By raising awareness the ultimate goal of secure Wi-Fi can be achieved.

Project report for CS4457: Networks 2. University of Western Ontario, Winter 2017.

3. Proposed Solution

3.1. Description

Our proposed solution is to create a mobile application on both iOS and Android showcasing the attack's capabilities. Not only will the bring awareness to the issue, but will let users actually test to see if any of their personal devices are prone to this attack. Furthermore, it will actually allow the user to perform the task and see the decrypted data to allow them to truly understand the dangers. The application will have 3 screens. The first one describing the functionality as well a warning informing the user to only use the app on APs they own. The second screen will allow searching nearby APs and provide a list to choose from. Once the user selects an access point from the list, they will be shown details about the device and buttons for initializing the attack and collecting data.

3.2. Technology Breakdown

References