President's Corner: KRACK Wi-Fi Vulnerability
By Eric Moore
January 13, 2018

In October 2017, Belgian researchers Mathy Vanhoef and Frank Piessens of the University of Leuven released a paper detailing a serious vulnerability in the implementation of WPA2 encryption, dubbed *KRACK* (***K**ey **R**einstallation Att**ack**)*. WPA2 is an encryption protocol for Wi-Fi—stronger than the older WEP and WPA protocols. The attack only defeats WPA2 encryption, not other encryption such as PGP for email and SSL for secure websites. However, SSL can also be defeated with a separate tool that decrypts otherwise secure data.

The vulnerability found by Vanhoef and Piessens amounts to a *man in the middle attack*. The attacker uses a computer with a software tool by which to *clone* a Wi-Fi access point (AP) on a different channel. Once the victim's computer is tricked into connecting to the cloned AP, the four-way handshake is manipulated to cause the victim's computer to switch no encryption, thus allowing the attacker to capture data using a network packet tool such as Wireshark. Depending on the victim's activity, the attacker could capture passwords, credit card numbers, or any other sensitive data being sent over the wireless connection. All devices are susceptible—Windows, Apple iOS, Linux, and Android. Linux and Android are especially vulnerable, as they may continue to use no Wi-Fi encryption throughout the victim's wireless session. To summarize, the vulnerability allows the attacker to eavesdrop on the victim's data, but does not allow the attacker to connect to the wireless network.

Because most devices are vulnerability, it is imperative that you protect yourself. Do not cease using WPA2, as offers the best protection. Use AES encryption with WPA2, as it is more secure than TKIP. (Some older operating systems do not support AES with WPA2, so you may need to replace them.) Do use a strong password for your wireless network, as well as a strong administration password for the router. (The administration password allows you to access to change the settings of your router, such as the SSID and wireless password.) Changing the wireless password does not protect against KRACK, as the vulnerability does not allow the attacker to capture this information.

You may not be as likely to be targeted when using your wireless network at your house. Attackers are more likely to target apartments and public places such as libraries and hotels where they can capture data from many different victims without notice, all the while working in close proximity to the APs. Still, depending on the Wi-Fi signal strength, an attacker could compromise your network while parked out on the street. Your best defense until you update your wireless router is to avoid using wireless altogether. When using public wireless, consider using VPN. You should also use SSL whenever possible, as it can (thought not necessarily) protect your data even if an attacker defeats the Wi-Fi encryption. Some websites may use weak SSL, so be cautious. (An SSL-protected website is evident by "HTTPS" in the URL and a lock symbol displayed next to the URL.)

Do keep your computer up-to-date by enabling automatic updates, or at least enabling automatic notification when critical updates become available. Do keep your anti-virus software up-to-date, as KRACK can be used to inject ransomware and other malicious software in the data stream being sent to your computer. A firmware update may also become available for your wireless router—be sure to check the manufacturer's website. (If you rent a wireless modem from your ISP, check with them for available firmware updates.) Some older routers may no longer be supported. If a firmware update is not soon available, then consider replacing the device with a newer one.

Suggested Reading:

For a basic overview of KRACK: https://www.howtogeek.com/329671/your-wi-fi-network-is-vulnerable-how-to-protect-yourself-against-krack/

For a detailed, technical overview including a video demonstration: https://www.krackattacks.com/