Serious Wi-Fi flaw found in WPA2 protocol

By Ilse van den Berg

18 Oct 2017

NEWSWATCH: A new cybersecurity attack, known as a ‘Krack' attack (key reinstallation attack) has revealed a flaw in Wi-Fi's WPA2's cryptographic protocols. Mathy Vanhoef, a cybersecurity researcher of KU Leuven in Belgium, made the discovery of the attack which works against all modern protected Wi-Fi networks. (video)

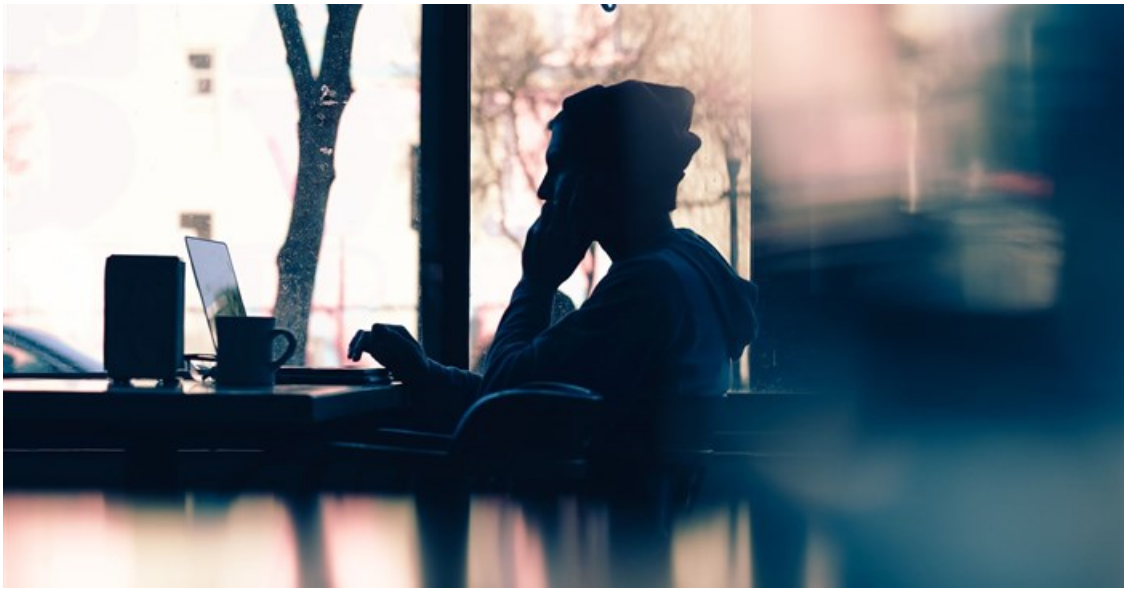

Photo by Hannah Wei on Unsplash

How it works

The WPA2 protocol is the most common and secure Wi-Fi access protocol since 2004 and is trusted for keeping Wi-Fi connections safe. The security flaw allows the attacker to decrypt a user’s data without needing to crack or know the actual Wi-Fi network’s password.

The attacker does this by decrypting the secure Wi-Fi connection and turning it into an unencrypted, and hence unsecure, hotspot. For this reason, merely changing the Wi-Fi network password will not prevent or mitigate such an attack from taking place. However, a limitation of Krack attacks is that they can only be carried out by an attacker who is within actual physical proximity of the targeted Wi-Fi network.

The main attack is against the four-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 (e.g. the pre-shared password of the network). At the same time, the four-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 four-way handshake.

AfriSecure Cybersecurity Summit ready for Johannesburg

16 Oct 2017

WPA protocol encrypts only the physical medium between a user's device and the Wi-Fi connection it is joined to. Furthermore, all secured apps and websites do now use some sort of end-to-end encryption protocol such as HTTPS, which is designed to work over unsecured channels (such as unencrypted Wi-Fi connections). As a result, the only way to access this secure traffic is by performing an additional SSL man-in-the-middle (SSL MITM) attack.

Android and Linux

According to a post on the Krack Attacks website, the attack is especially catastrophic against version 2.4 and above of wpa_supplicant, a Wi-Fi client commonly used on Linux. Because Android uses wpa_supplicant, Android 6.0 and above is especially vulnerable. Currently, 50% of Android devices are vulnerable to this exceptionally devastating variant of our attack.

Cybersecurity company, Check Point, says SSL MITM attacks are already detected and protected by its SandBlast Mobile on both iOS and Android devices by immediately alerting the user and blocking all corporate assets. SandBlast Mobile also helps to verify that mobile devices on your network are in compliance with the latest OS versions and security patches.

South Africans easy meat for hackers

27 Sep 2017

In addition, Check Point's Capsule Cloud provides a worldwide service that secures remote PCs and laptops in any location against SSL MITM attacks, allowing users to connect to the internet securely in any Wi-Fi environment. Depending on an organisation's requirements, the same level of security can also be acquired through Check Point's VPN.

The company advises all mobile users to ensure they have installed a mobile security solution and accept any software updates that their mobile provider issues.

For more, go to www.krackattacks.com

ABOUT ILSE VAN DEN BERG

Ilse is a freelance journalist and editor with a passion for people & their stories (check out Passing Stories). She is also the editor of Go & Travel, a platform connecting all the stakeholders in the travel & tourism industry. You can check out her work here and here. Contact Ilse through her website here.
- #StartupStory: Aura security app to aid beleaguered Uber drivers - 13 Jul 2018
- #StartupStory: BlockMesh - 12 Jun 2018
- Taking telecoms to the next level: Who needs a long-term contract? - 4 Jun 2018
- Nokia makes a comeback in South Africa with new phones - 24 Apr 2018
- New Cape Town/Brazil subsea cable to boost SA broadband - 18 Apr 2018

View my profile and articles...

For more, visit: https://www.bizcommunity.com