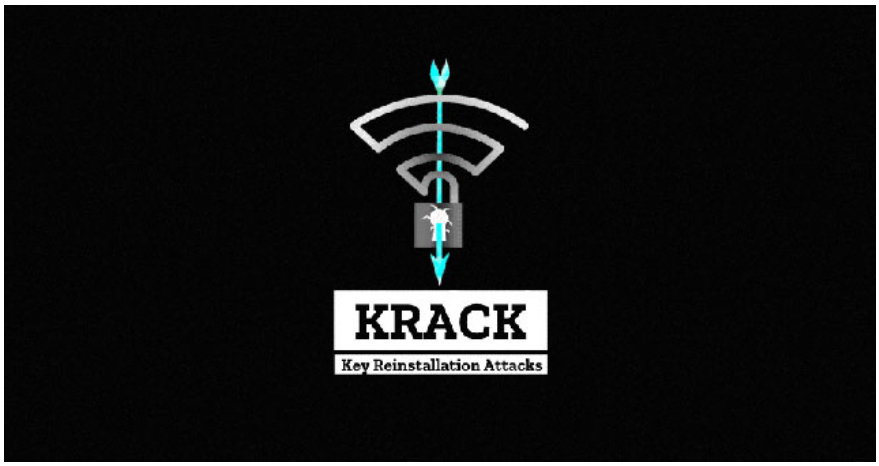
KRACK attack breaks down the WPA2 WiFi protocol

Researcher Mathy Vanhoef from Leuven University discovered a serious security flaw on Wi-Fi Protected Access II (WPA2) network security protocol.

Researcher Mathy Vanhoef from Leuven University discovered a serious security flaw on Wi-Fi Protected Access II (WPA2) network security protocol, the most commonly used protocol for WiFi security today. .

Named KRACK, short for Key Reinstallation Attack, this attack uses some key management vulnerabilities on WPA2, allowing 'eavesdropping' of traffic between the computer and WiFi access point, forcing people in the WiFi network to install re-encrypt key used for WPA2 traffic.

The attacker can then steal personal information and note that the hacker does not change the password but can encrypt the data without knowing the password. It means that even if you change your password, it will not prevent KRACK.



Error on WiFi WPA2 security protocol helps hackers penetrate network traffic

This error is on the WPA2 protocol itself, not with any software or hardware. 'If your device has WiFi support, it's probably affected too,' the researchers said. According to initial reviews, Android, Linux, Apple, Windows, OpenBSD, MediaTek, Linksys or IoT devices are all affected.

How does KRACK WPA2 work?

KRACK exploits WPA2's 4-step handshake protocol, which is used to set up key for encrypting traffic. In order for a hacker to succeed, the victim will need to reinstall the currently used key, obtained by modifying the handshake message to encrypt.

In addition, the attacker must also be in the above WiFi network. HTTPS in some cases can protect traffic for using another encryption layer, but it is also 100% unsafe because an attacker can downgrade the connection, giving access to encrypted HTTPS traffic.

This attack allows a third party to eavesdrop on WPA2 traffic, but if WiFi uses WPA-TKIP or GCMP encryption, the attacker can also inject malicious code into the victim's packet to fake traffic.

To find out more, you can read the website about this type of attack at *https://www.krackattacks.com/*

Below is a list of key management vulnerabilities on WPA2 protocol.

CVE-2017-13077
CVE-2017-13078
CVE-2017-13079
CVE-2017-13080
CVE-2017-13081
CVE-2017-13082
CVE-2017-13084
CVE-2017-13086
CVE-2017-13087
CVE-2017-13088

See also: Microsoft silently patched the KRACK WPA2 security hole