Issued 10/16/17

Wi-Fi Security Has Been Breached

At about 7AM ET this morning, researchers revealed details of a new exploit called KRACK that takes advantage of vulnerabilities in Wi-Fi security to let attackers eavesdrop on traffic between computers and wireless access points.

The exploit, as first reported by Ars Technica, takes advantage of several key management vulnerabilities in the WPA2 security protocol, the popular authentication scheme used to protect personal and enterprise Wi-Fi networks. “If your device supports Wi-Fi, it is most likely affected,” say researchers. **So yeah, this is bad.**

The United States Computer Emergency Readiness Team issued the following warning in response to the exploit: US-CERT has become aware of several key management vulnerabilities in the 4-way handshake of the Wi-Fi Protected Access II (WPA2) security protocol. The impact of exploiting these vulnerabilities includes decryption, packet replay, TCP connection hijacking, HTTP content injection, and others. Note that as protocol-level issues, most or all correct implementations of the standard will be affected. The CERT/CC and the reporting researcher KU Leuven, will be publicly disclosing these vulnerabilities on 16 October 2017.

The researchers noted that 41 percent of all Android devices are vulnerable to an “exceptionally devastating” variant of the Wi-Fi attack. All Wi-Fi

devices are to some degree susceptible to the vulnerabilities making them ripe for data theft or ransomware code injection from any malicious attacker within range. The researchers recommend patching all Wi-Fi clients and access points when the fixes are available and to continue using WPA2 until then (WPA1 is also affected and WEP security is even worse). It's not yet clear if the vulnerabilities revealed today are actively being exploited in the wild.