Krack and the Ethics of Disclosure

Adon Shapiro

December 12, 2017

Abstract

Vulnerabilities and exploits in software are discovered every day. This is a well-known fact in the cyber-security industry. What is not so universally agreed-upon is the proper way for an ethical hacker or security researcher to disclose a vulnerability they have discovered, and the argument re-surfaces with the disclosure of each new high-profile bug. The most recent such bug is KRACK. In October 2017, researchers at the University of Leuven published details of a vulnerability they had discovered in the WPA2 protocol that secures Wi-Fi connections. They called it KRACK (Key Reinstallation Attack) because of the way it takes advantage of a bug in WPA2 that allows the re-use of insecure cryptographic keys. KRACK is significant because it is a fundamental weakness not in a specific piece of software, but rather in the Wi-Fi standard itself, and so everyone who uses Wi-Fi was susceptible to the attack. Because of its recentness and its far-reaching impact, KRACK is a perfect lens through which to view the problem of ethical disclosure.