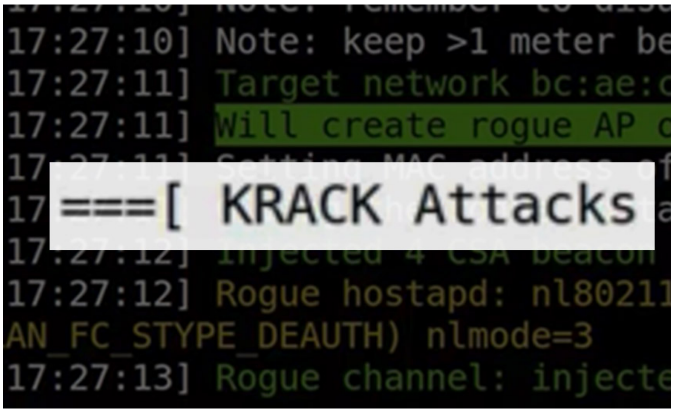
Researchers warn of a serious flaw in the WPA2 protocol securing all wifi networks-- one allowing attackers to steal passwords, emails and other supposedly encrypted data!



```
17:27:10] Note: remember to disc
17:27:10] Note: keep >1 meter be
17:27:11] Target network bc:ae:c
17:27:11] Will create rogue AP c
17:27:11] Setting MAC address of
17 ===[ KRACK Attacks
17:27:12] Injected 4 CSA beacon
17:27:12] Rogue hostapd: nl80211
AN_FC_STYPE_DEAUTH) nlmode=3
17:27:13] Rogue channel: injecte
```

Dubbed Key Reinstallation Attacks (or KRACKs), such attacks even allow those with malicious intent to inject ransomware and malware into a website a user is visiting, all while simply being in range of a vulnerable device. These can be any wifi-capable device, although the flaw is "particularly devastating" in the case of Linux and Android 6.0.

How does KRACK works? As the researchers put it, attackers can duplicate a vulnerable WPA2 network, impersonate the MAC address and change the wifi channel. The fake network acts as a "man in the middle," forcing devices to connect to the rogue network instead of the protected original.

The situation is even worse with Android and Linux, since the attack also forces the device to re-install an all-zero encryption key, beating part of the security the WPA2 protocol provides. A proof-of-concept attack by the researchers on Android decrypts all data transmitted by the victim, and while the attack should not work on a "properly configured HTTPS site," it still works on a "significant fraction" that are, well, not set up properly.

How can one fix this issue? The problem should be easily fixed via firmware, and the researchers add "implementations can be patched in a backwards-compatible manner," meaning an update to WPA3 is not required. But until the updates roll out, worried Android users are advised to turn off the wifi on their devices. One can also visit sites with reputable HTTPS security.

Go Key Reinstallation Attacks