

What's New October 2017

Todd McDaniel
Mac Group, Marriott Library, ITS

ALL U
NEED



J. Willard Marriott Library
THE UNIVERSITY OF UTAH

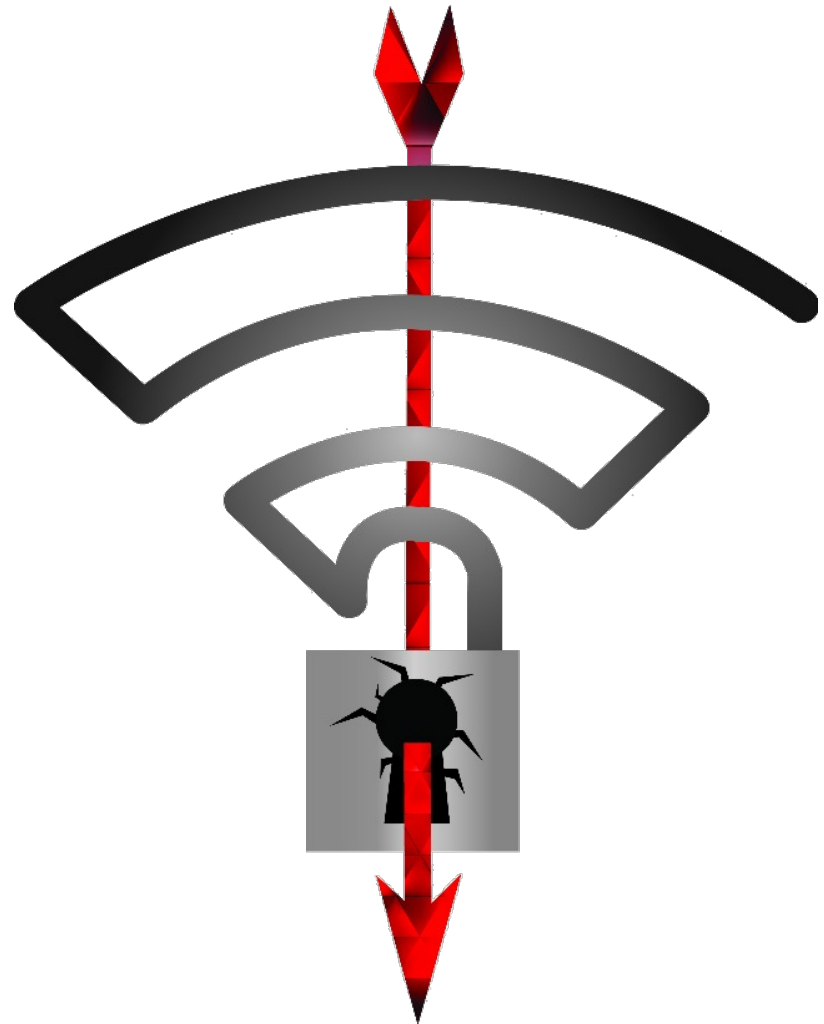
ALL U
NEED



THE UNIVERSITY OF UTAH

KRACK

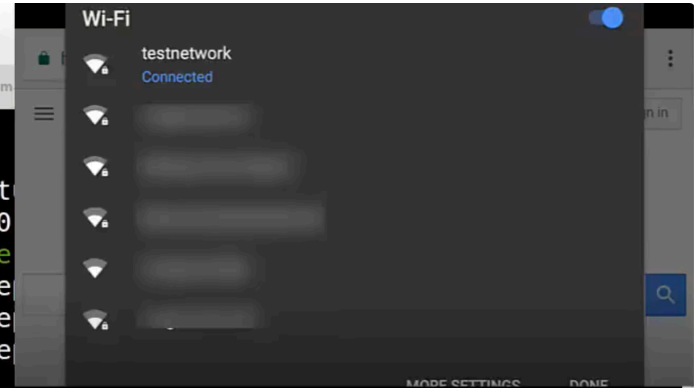
- **K**ey **R**einstallation **A**ttack**S**
- Exploits vulnerabilities in Wi-Fi Protected Access II (WPA2)
- Leverage other tools to strip HTTPS protection
- Inject and manipulate data, MitM attacks
- Weakness in the standard itself, clients and routers impacted
- <https://www.krackattacks.com>



```
mathy@mathy-msi:~/research/wifi/breaking-wpa2-attack-zero-tk/krackattack
File Edit View Search Terminal Tabs Help

mathy@mathy-msi:~/research/wifi/breaking-wpa2-attack-zero-tk/krackattack x mathy@mathy-msi:~/research/wifi/breaking-wpa2-attack-zero-tk/krackattack x m

[17:28:24] Injected 1 CSA beacon pairs (moving stations to channel 1)
[17:28:24] Injected 1 CSA beacon pairs (moving stations to channel 1)
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: Auth(seq=1497, stat
[17:28:24] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=4, sleep=0
Established MitM position against client 90:18:7c:6e:6b:20 (moved to state
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: EAPOL-Msg1(seq=0, re
[17:28:24] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EAPOL-Msg2(seq=0, re
[17:28:24] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: EAPOL-Msg3(seq=1, re
Not forwarding EAPOL msg3 (1 unique now queued)
[17:28:24] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: QoS-Null(seq=5, sleep=0)
[17:28:25] Real channel : bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: EAPOL-Msg3(seq=2, replay=4) -- MitM'ing
Got 2nd unique EAPOL msg3. Will forward both these Msg3's seperated by a forged msg1.
==> Performing key reinstallation attack!
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EAPOL-Msg4(seq=1, replay=3)
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=6, sleep=0)
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=7, sleep=0)
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EncryptedData(seq=2, IV=1)
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EncryptedData(seq=3, IV=2)
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=8, sleep=0)
[17:28:25] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=9, sleep=0)
[17:28:26] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EncryptedData(seq=4, IV=1)
SUCCESS! Nonce reuse detected (IV=1), with usage of all-zero encryption key.
Now MitM'ing the victim using our malicious AP, and interceptig its traffic.
[17:28:26] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EncryptedData(seq=5, IV=2)
[17:28:26] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=10, sleep=0)
[17:28:26] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EncryptedData(seq=6, IV=3)
[17:28:26] Rogue channel: bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: EncryptedData(seq=0, IV=1)
[17:28:26] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: EncryptedData(seq=7, IV=4)
[17:28:26] Rogue channel: bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: EncryptedData(seq=1, IV=2)
[17:28:26] Rogue channel: 90:18:7c:6e:6b:20 -> bc:ae:c5:88:8c:20: Null(seq=11, sleep=1)
[17:28:26] Rogue channel: 90:18:7c:6e:6b:20 -> ff:ff:ff:ff:ff:ff: ProbeReq(seq=12)
[17:28:26] Rogue channel: bc:ae:c5:88:8c:20 -> 90:18:7c:6e:6b:20: ProbeResp(seq=1156)
```



<https://youtu.be/Oh4WURZoR98>

[https://www.kb.cert.org/vuls/byvendor?
searchview&Query=FIELD+Reference=228519
&SearchOrder=4](https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4)

[CVE-2017-13077](#): Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.

[CVE-2017-13078](#): Reinstallation of the group key (GTK) in the 4-way handshake.

[CVE-2017-13079](#): Reinstallation of the integrity group key (IGTK) in the 4-way handshake.

[CVE-2017-13080](#): Reinstallation of the group key (GTK) in the group key handshake.

[CVE-2017-13081](#): Reinstallation of the integrity group key (IGTK) in the group key handshake.

[CVE-2017-13082](#): Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.

[CVE-2017-13084](#): Reinstallation of the STK key in the PeerKey handshake.

[CVE-2017-13086](#): reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.

[CVE-2017-13087](#): reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

[CVE-2017-13088](#): reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

Patches incoming

- macOS, iOS, tvOS, watchOS patches included in current beta releases.
- Does this include previous OS releases?
Apple has had a spotty record in this regard...
- Check with your hardware manufacturers for patch schedules.

News

- BBEdit 12 released
- VMWare Fusion 10 released
- Adobe CC 2018
- iPhone X initially constrained due to component availability?

macOS Hidden Updates

since 9/20/17

Gatekeeper	3
------------	---

MRTConfigData	0
---------------	---

Chinese Word List Update	0
--------------------------	---

Core Suggestions	1
------------------	---

XProtect	1
----------	---

EFICheck AllowListAll	1
------------------------------	---

More Security News

- Equifax site serving malware
- Kaspersky AV working with foreign intelligence services
- Infineon RSA Vulnerable Key Generation
Trusted Platform Modules, Smart cards, Yubikeys

Questions?

