What's New October 2017

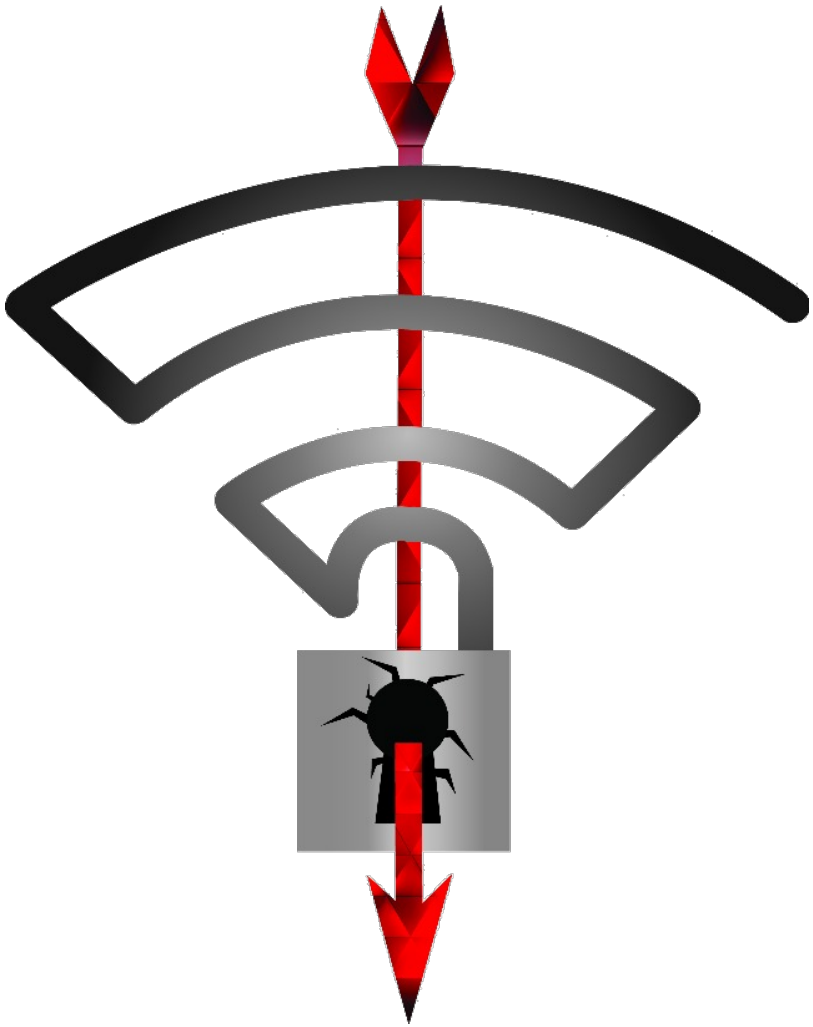
Todd McDaniel
Mac Group, Marriott Library, ITS

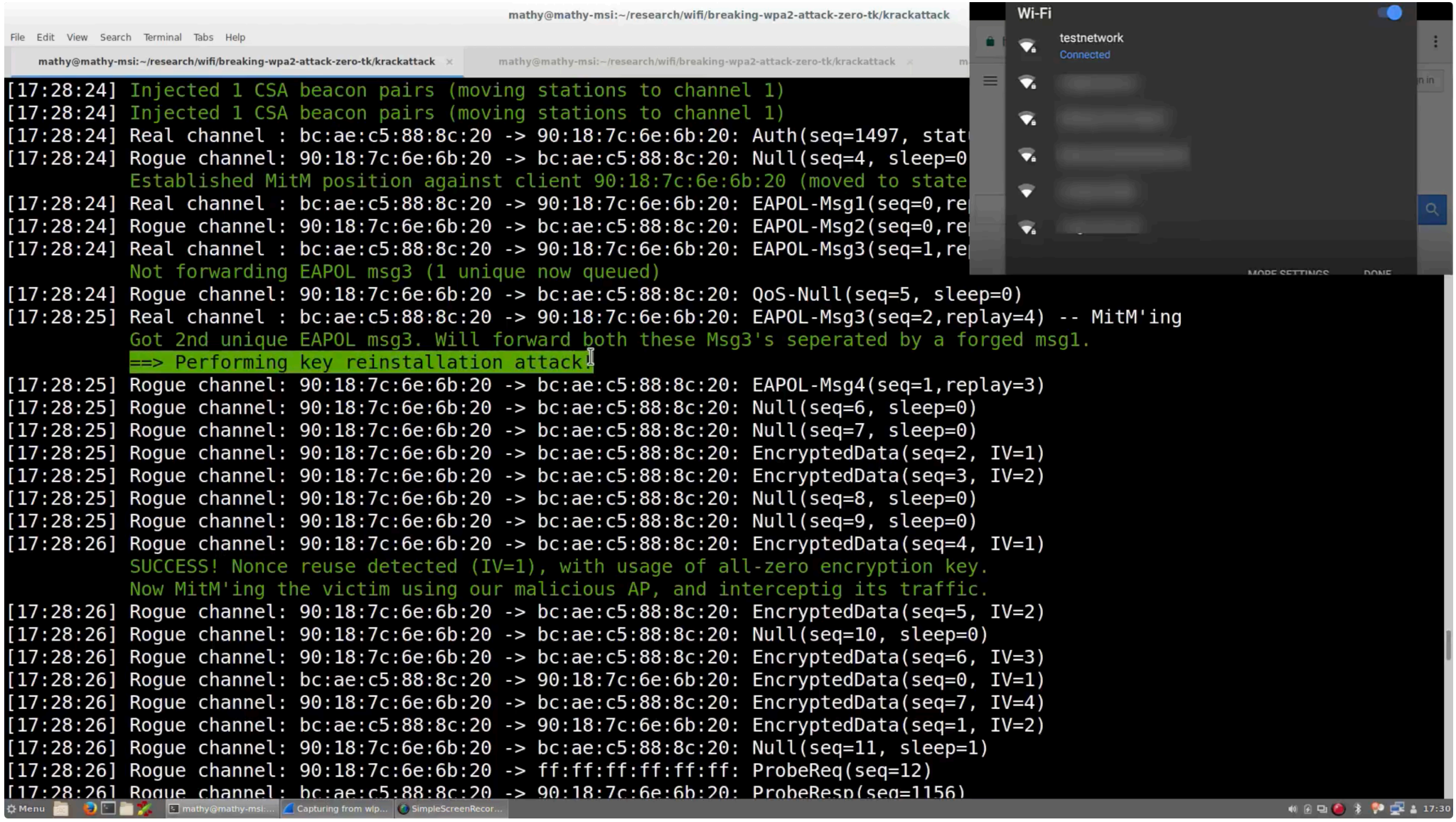
ALL U NEED

J. Willard Marriott Library
THE UNIVERSITY OF UTAH

KRACK

- **K**ey **R**einstallation **A**tta**CK**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





https://youtu.be/Oh4WURZoR98

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?