CCS Technologies

November 2017
Volume 12, Issue 11

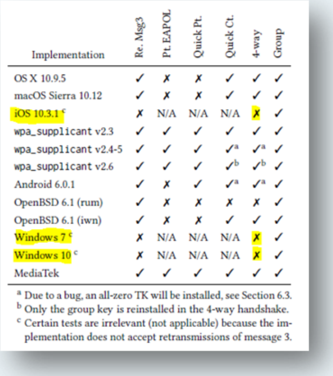
"Local Support • Personal Service • Since 1976"   www.ccstech.net   "Relax...we're on IT"

Wifi Security: How to plug the KRACK!

by Jeff Verry

If you are reading this newsletter on your phone, tablet or laptop, chances are almost 100% that you are connected to a wireless network and that it is running on something called WPA2. You may have heard the news last month about the KRACK (**K**ey **R**einstallation **A**tta**CK**) vulnerability in such networks. This is a big deal because this particular protocol is by far the most common way that wireless devices talk to one another. There are also some critical caveats based on how the vulnerability actually works. Here are some important notes on this threat as well as steps you can and should take.

1. This is big news because WPA2 has been around for a long time (13 years in practice) and is widely trusted.
2. There are some very serious limitations to this vulnerability.
   a. **An attacker needs to be physically in range** of a particular Wi-Fi network to carry out the assaults. (cf. https://www.wired.com/story/krack-wi-fi-wpa2-vulnerability/) This is a local Wi-Fi attack, not something coming over the WAN (Internet) from foreign soil. Think creepy guy in the van in your driveway, not creepy hacker in North Korea.
   b. Which gets us to the second major limitation. **Windows 7/10 and iOS operating systems aren't expected to be affected.** "In practice, some complications arise when executing the attack. First, not all Wi-Fi clients properly implement the state machine. In particular, Windows and iOS do not accept retransmissions of message 3." (pg. 5 Vanhoef, Mathy and Frank Piessens, Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, CERT/CC 2017) SO it's the creepy guy in the van, attacking your nanny cam or your router; something like that. Furthermore, although Windows is not expected to be affected by this particular threat, Microsoft released a patch addressing this kind of vulnerability as part of the October updates on 10/10.



Implementation	Re. Msg3	Pt. EAPOL	Quick Pt.	Quick Ct.	4-way	Group
OS X 10.9.5	✓	✗	✗	✓	✓	✓
macOS Sierra 10.12	✓	✗	✗	✓	✓	✓
iOS 10.3.1 [c]	✗	N/A	N/A	N/A	✗	✓
wpa_supplicant v2.3	✓	✓	✓	✓	✓	✓
wpa_supplicant v2.4-5	✓	✓	✓	✓[a]	✓[a]	✓
wpa_supplicant v2.6	✓	✓	✓	✓[b]	✓[b]	✓
Android 6.0.1	✓	✗	✓	✓[a]	✓[a]	✓
OpenBSD 6.1 (rum)	✓	✗	✗	✗	✗	✓
OpenBSD 6.1 (iwn)	✓	✗	✗	✓	✓	✓
Windows 7 [c]	✗	N/A	N/A	N/A	✗	✓
Windows 10 [c]	✗	N/A	N/A	N/A	✗	✓
MediaTek	✓	✓	✓	✓	✓	✓

[a] Due to a bug, an all-zero TK will be installed, see Section 6.3.
[b] Only the group key is reinstalled in the 4-way handshake.
[c] Certain tests are irrelevant (not applicable) because the implementation does not accept retransmissions of message 3.

Here's a list of systems affected (translation: pretty much everybody when it comes to Internet of Things). http://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519&SearchOrder=4

Actions to take:

1. Keep your computer up to date. Also, apply any and all firmware updates and patches for your wireless gear (think, all the stuff that isn't your Windows computer, iPhone or iPad). Some vendors are already taking corrective action.
2. Enable MAC logging and any other measures to monitor traffic if you have not already.
3. Plug in whenever possible. Segment out wifi and wired traffic when storing or transmitting credit card, social security or other sensitive information.
4. Review your physical security measures (remember, hacker needs to be in range).
5. Consider a wireless audit and/or a compliance scan.

If you have any questions on the above, please contact a *CCS Technologies* technician and we can walk you through what this latest threat may mean to you and your business.

"Relax...we're on IT"

Savings Opportunity for November Only!

This may be the best time for you to save money for your organization. As of November 1, 2017 our hourly rates have gone up. The last time we raised our hourly rates was on November 1, 2010. We have used many new efficiencies to keep them from going up over the last 7 years. However, to ease the pain, we are offering a 10% discount on our OLD rate if you buy at least a 20-hour block of time (maximum 60-hour purchase) and we receive your payment by November 30, 2017. You will save over $400 on a 20-hour block. What a great value!
You may want to review and see how many hours you have used in this current year to determine what you should purchase for next year and you'll receive a 10% discount off our OLD rate…where else do you see those types of return rates? Give us a call if you have any questions or would like us to invoice you for a block of 20, 40 or 60 hours.

300 Main Street, Coopersville, MI 49404
616.997.TECH(8324)
Fax 616.997.9317

206 Washington, Grand Haven, MI 49417
616.842.TECH(8324)

3489 Kelly Street, Hudsonville, MI 49426
616.669.TECH(8324)

Contact Information

Information	Info@ccstech.net
Tech Support	Support@ccstech.net
Sales	Sales@ccstech.net
Greg Slater	Gslater@ccstech.net
Ellen Slater	Eslater@ccstech.net
Drew Rowe	Drowe@ccstech.net
Jeff Verry	Jverry@ccstech.net
Joe Halstead	Jhalstead@ccstech.net
Jorge Arias	Jarias@ccstech.net
Karen Strickland	Kstrickland@ccstech.net
Mark Kowitz	Mkowitz@ccstech.net
Ryan McMillen	Rmcmillen@ccstech.net
Eric Ruzek	Eruzek@ccstech.net
Seth Johnson	Sjohnson@ccstech.net

CCS Technologies Store Hours

Coopersville Store

Mon-Fri 8:00 am - 5:30 pm, Sat 9:30 am - 12:00 pm

Grand Haven Store & *Hudsonville Store*

Mon-Thu 9:00 am - 6:00 pm, Fri 10:00 am - 6:00 pm

Sat 10:00 am – 3:00 pm