Security Now! #633 - 10-17-17

KRACKing WiFi

This week on Security Now!

This week we examine ROCA's easily factorable public keys, the surprising prevalence of web-based cryptocurrency mining, some interesting work in iOS dialog password dialog spoofing, Google's Advanced Protection Program, some good "Loopback" comments from our listeners... and then we take a close look at KRACK - the Key Reinstallation AttaCK against ALL unpatched WiFi systems.

Security News

ROCA: Vulnerable RSA generation (CVE-2017-15361)
The upcoming ACM Conference on Computer and Communications Security (aka CCS), which is the major annual ACM conference of the Special Interest Group on Security promises to be a barn burner.

Not ONLY will the presentation of the KRACK attack be presented (which we'll cover at the end of the podcast) but so, too, will a VERY unsettling discovery by a team of researchers in the Czech Republic, the UK, Italy.

ROCA stands for: the Return Of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli.

Don Coppersmith is a cryptographer with a long resume of crypto accomplishments to his name.

We talk often here about the security of most of the Internet, banking, identity authentication and more, most of which are still based upon the venerable RSA cryptosystem, which relies upon the inherent difficulty of factoring public keys which are the product of two very large prime numbers.

And we also often draw the distinction between theory and practice... where the theory only works in practice IF the implementation is careful and correct... and also how very easy it is for mistakes to be made.

Okay, so these researchers uncovered a doozy of a mistake which exists in the embedded cryptographic library used by Infineon's products, which are very widely used in TPM modules, smartcards, and other embedded applications.

For the past five years, since 2012, many of the supposedly-impractical-to-factor public keys being generated by these embedded crypto chips CAN, unfortunately, be practically factored.

The vulnerability was found by a close inspection of a large number of RSA keys generated and exported from Infineon smartcards by the researchers.

Any candidate public key can be tested for factorability instantly.

The worst cases for the factorization of 1024 and 2048-bit keys are less than 3 CPU-months and 100 CPU-years, respectively, on a single core of a common recent CPU, while the expected time is half of that of the worst case.

The factorization can be performed in parallel on multiple CPUs allowing for practical factorization in hours or days. The worst-case price of the factorization on an Amazon AWS c4 computation instance is $76 for the 1024-bit key and about $40,000 for the 2048-bit key. But only half that will be typical.

To provide a bit more perspective, a properly generated 2048-bit RSA public key should require several quadrillion years—hundreds of thousands of times the age of the universe—to be factored with on general-purpose computer. Factoring a faulty 2048-bit RSA key generated with the Infineon library would take a maximum of 100 years, and on average only half that... and that's on a general purpose computer.

The vulnerability was found by a close inspection of a large number of RSA keys generated and exported from the manufacturer smartcards. The full results will be presented at an academic ACM Conference on Computer and Communications Security (ACM CCS '17) starting from October 30th.

The vulnerability was responsibly disclosed to Infineon Technologies AG, 8 months ago, back in the first week of February to allow time for correction.

Major vendors including Microsoft, Google, HP, Lenovo, Fujitsu already released the software updates and guidelines for a mitigation.

An inspection of available public keys on the Internet discovered thousands upon thousands that could be readily broken. Many on GitHub... who have been notified.

The researchers looked at 41 laptop models that used trusted platform modules. They found vulnerable TPMs from Infineon in 10 of them. The vulnerability is especially acute for TPM version 1.2, because the keys it uses to control Microsoft's BitLocker hard-disk encryption can be factored. So anyone who obtains a Windows machine with a Bitlocker-encrypted drive on top of TPM 1.2 may not be secure.

Both offline and online detection tools have been provided. They are open source and released under the MIT license so that they may be incorporated into other solutions:

ROCA Vulnerability Test Suite
https://keychest.net/roca

The researchers wrote: "Our work highlights the dangers of keeping the design secret and the implementation closed-source, even if both are thoroughly analyzed and certified by experts. The lack of public information causes a delay in the discovery of flaws (and hinders the process of checking for them), thereby increasing the number of already deployed and affected devices at the time of detection."

Infineon has issued a firmware update that patches the library vulnerability, and TPM manufacturers are in the process of releasing one as well.

So in coming weeks we can expect to see important updates to our PCs followed by some sort of rekeying.

https://www.yubico.com/keycheck/

https://crocs.fi.muni.cz/public/papers/rsa_ccs17

The prevalence of web-based Cryptocurrency mining
https://blog.adguard.com/en/crypto-mining-fever/

The folks behind the AdGuard ad blocker did some Internet sleuthing.

220 of the Internet's top 100K sites are known to be mining.

The websites tend to occupy the gray zone -- being largely pirate TV and video sites, Torrent trackers and porn websites.

AdBlock Plus has added a rule to block and uBlock Origin blocks mining by default.

But here's a thought I had while thinking about this again, and which the authors of this blog posting also suggested at the end of their post: Is blocking websits cryptomining what we want?

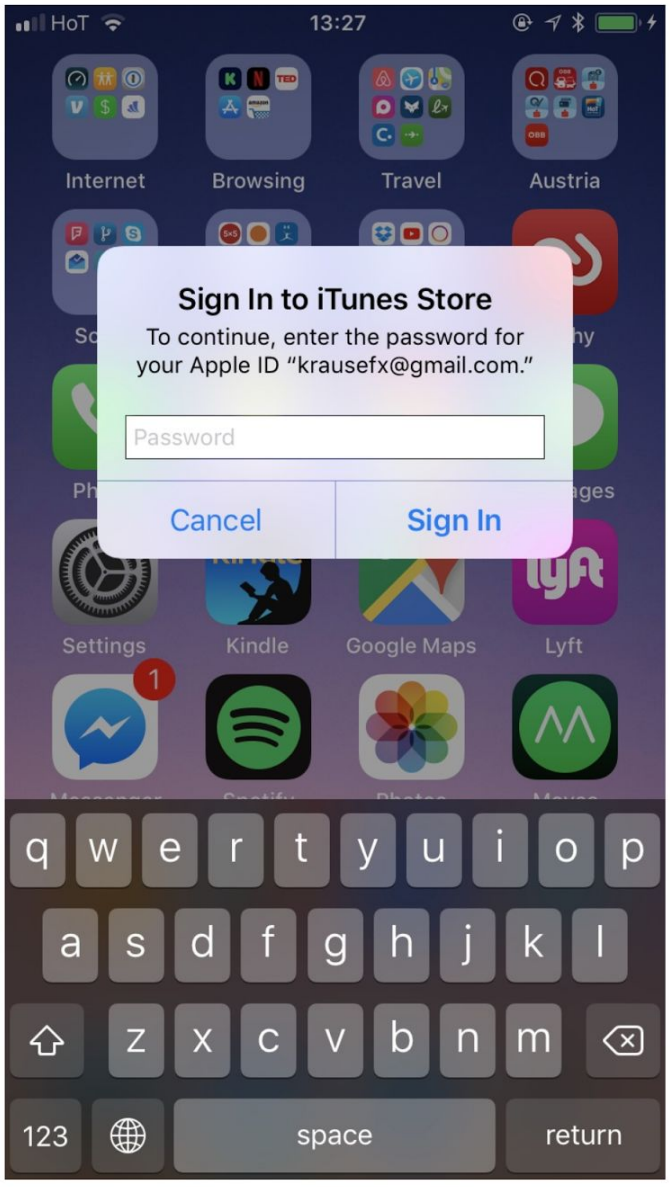
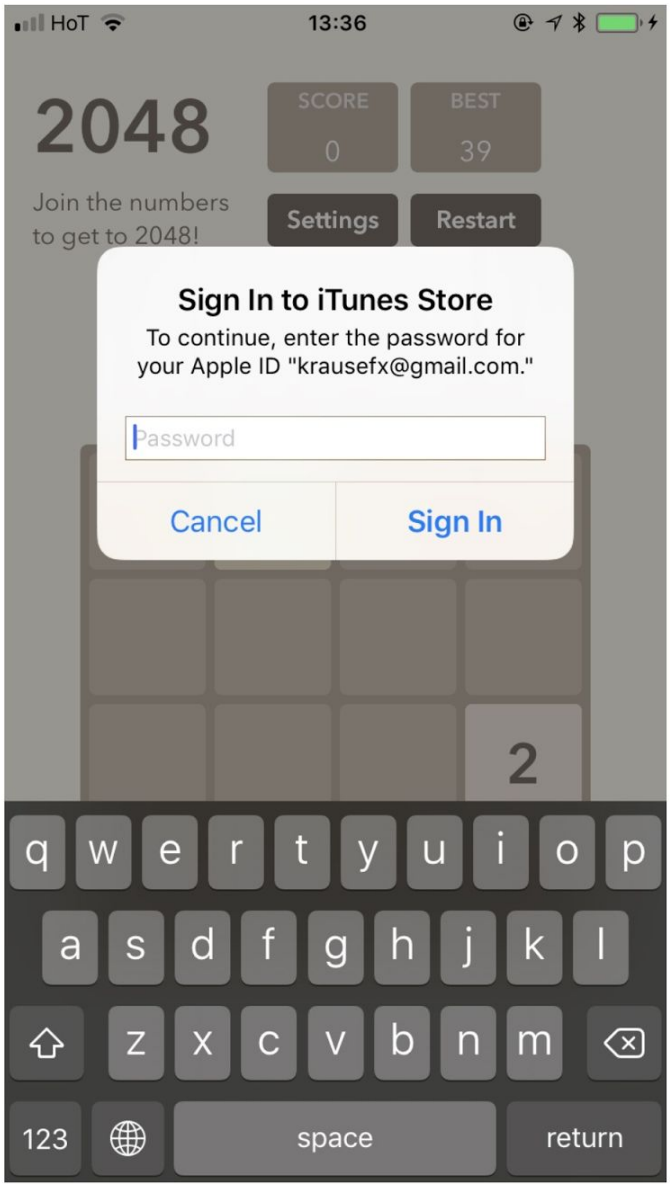
Bitcoin is now above $5600. Cryptocurrency has developed into a real thing.

So if a website borrows my system's processing power -- WHILE I'M borrowing their site's content -- this seems like a fair exchange, especially if it means I get an ad-free visit while my machine is mining cryptocurrency for them.

As I noted last week, there's no security implication. Battery powered mobile devices might not want to participate due to power consumption. But laptops and desktops could without ill effect.

iOS Privacy: steal.password - Easily get the user's Apple ID password, just by asking
https://krausefx.com/blog/ios-privacy-stealpassword-easily-get-the-users-apple-id-password-just-by-asking

It's easy to obtain someone's iOS password: Just ask.

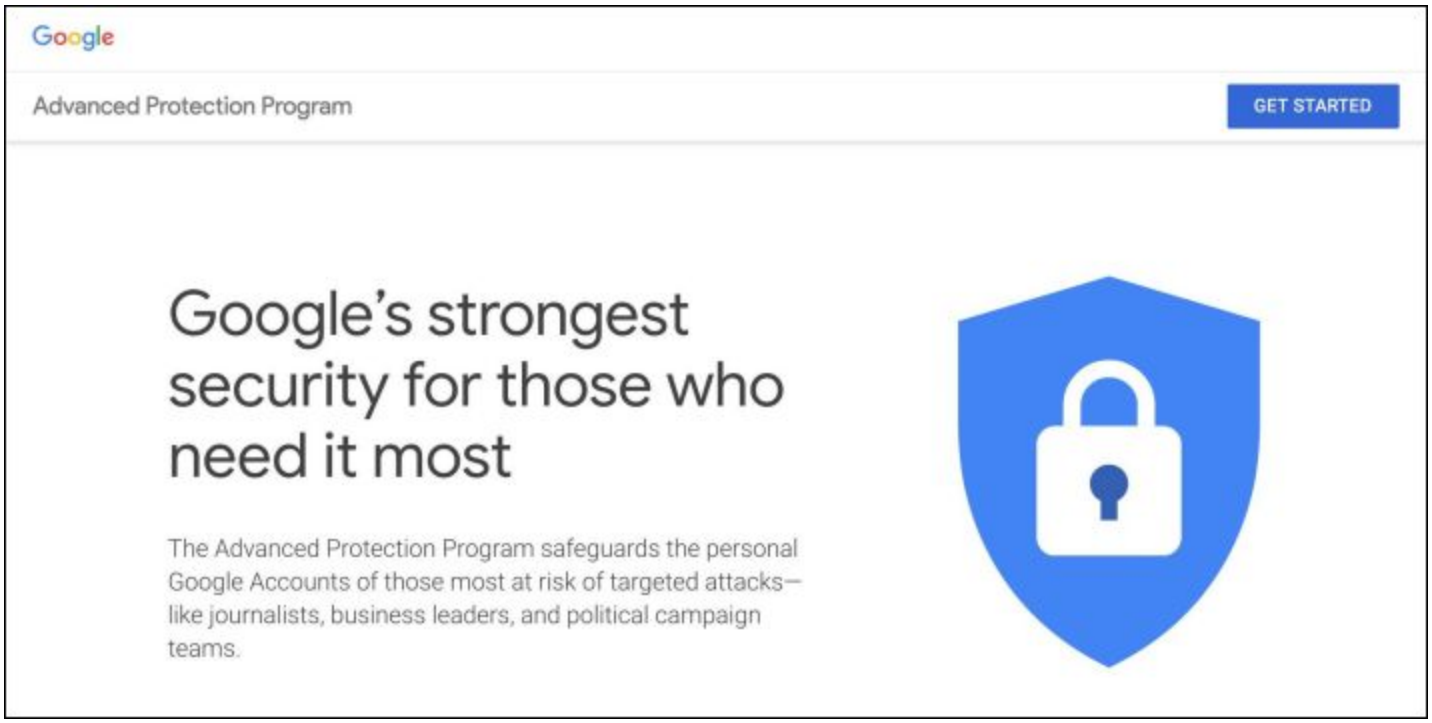
Random system popup	Phishing popup in app/game
	

Felix Krause notes in his blog posting: iOS asks the user for their iTunes password for many reasons, the most common ones are recently installed iOS operating system updates, or iOS apps that are stuck during installation.

As a result, users are trained to just enter their Apple ID password whenever iOS prompts you to do so. However, those popups are not only shown on the lock screen, and the home screen, but also inside random apps, e.g. when they want to access iCloud, GameCenter or In-App-Purchases.

This could easily be abused by any app, just by showing an UIAlertController, that looks exactly like the system dialog. Even users who know a lot about technology have a hard time detecting that those alerts are phishing attacks.

Google's "APT" -- Advanced Protection Program -- goes live.
https://9to5google.com/2017/10/17/google-announces-advanced-protection-program/
Today: Google announced its "Advanced Protection Program"



Protects the Google accounts of "those most at risk of targeted attacks—like journalists, business leaders, and political campaign teams."

Main defense is a physical Security Key for authentication that also requires the Chrome browser.

This is NOT meant for everyone because the security / convenience tradeoffs are several:

- Physical Security Key: To guard against phishing, a physical Security Key will be required every time you log into a device. This will replace and disable other forms of authentication like SMS and the Google Authenticator app.

- Limit data access and sharing: Third-party apps will no longer have access to Gmail or Drive, with email only available through Gmail or Inbox clients. Due to iOS apps not supporting Security Keys, Google notes that the Apple Mail, Contacts, and Calendar apps will not work, with users being forwarded to the first-party apps on iOS. Meanwhile, Google services that require a sign-in, like Photos, will only be available through Chrome.

- Blocking fraudulent account access: The last measure is designed to counter impersonators who claim to be locked out of their account. Google notes "extra steps," like additional reviews and request for more details, in place during the account recovery process. This process will "take a few days."

Miscellany

The Orville
I tried it again. I watched about half of the "Krill" episode, ending when they were in the Krill church for services. It's just not serious enough for me. But I understand TOTALLY that I'm probably in the minority... and that's, of course, fine.

SpinRite

Date: Mon, 16 Oct 2017 07:14:22 -0700
From: Kristopher Ting
Subject: Another SpinRite testimonial for you

Hey Steve,

I'm a long-time user of SpinRite and long-time listener of Security Now!

Wanted to send you a quick success story, in case you wanted one for an upcoming episode...

My dad called me a few days ago, telling me his Windows PC was suddenly telling him his second hard drive ***(the one on which he stores all his important data)*** was not formatted properly. It was the dreaded "This drive is not formatted, would you like to format it? Yes/No." message!

After telling him to immediately click "NO" and remove the drive, he brought the drive over to my house and I mounted it into my PC. As I expected, my Windows PC had the same problem accessing any partition information for this drive (saw it as a RAW instead of an NTFS). I immediately rebooted into SpinRite ran a Level 2 on it. It was a standard 250 GB SATA drive, so the estimated time to complete was under 40 minutes. At around the 95% mark, SpinRite detected a sector that needed further analysis, and after about 3 minutes it was ultimately marked as Unrecoverable. The rest of the drive checked out OK.

Thinking that the one Unrecoverable item was the cause of my dad's original issue, I felt certain that I would reboot only to find I had the same issue and that his data was officially "toast". But to my pleasant surprise, the drive and it's original partition were there and fully accessible! I immediately copied all his data onto my PC, and will be replacing his with another in the near future.

Dad's happy, and of course that makes me happy! Kudos to such a great product Steve!

Thanks!

Kristopher Ting
Powell Technologies
Johnson City, TN

Closing The Loop

crackruckles (@crackruckles)
@leolaporte @SGgrc Just found a great site to show what info is leaked from your browser & torrent clients: https://ipleak.net/

Steverino (@DaMoisture)
@SGgrc Security at USAA bank just tried to tell me "they have done the research, and found that shorter passwords are more secure than longer passwords" when I complained about their website's 12 character password limit.

Ryan Scullen (@techlife)
@SGgrc how would DANE prevent man in the middle attacks?

Eric Vollbrecht (@ericvollbrecht)
@SGgrc how is publishing a public key via DNSSEC any different than a self signed TLS certificate? Other than the method of distribution

Barbara (@Barbara130)
@SGgrc re: security.txt file, what stops bad guys from spamming the contact email address?

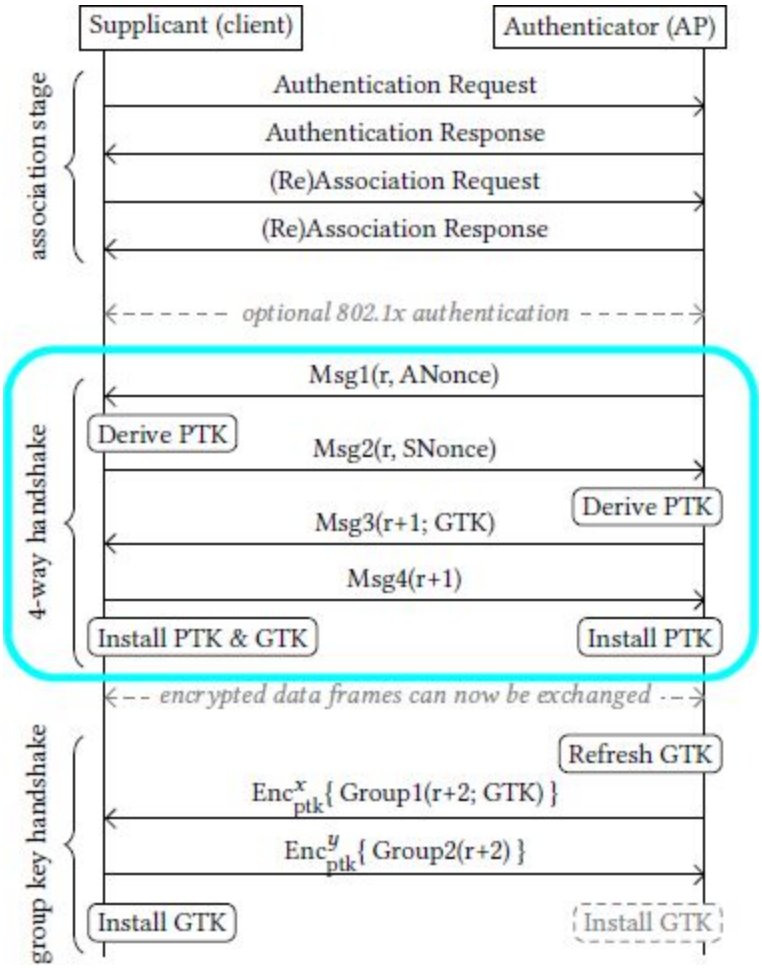
Richard Petrie (@deedasmi)
@GibsonResearch You asked one last week's episode why people were adverse to printing password recovery tokens. I have no physical security

Brad Dux (@Bradisbest)
@SGgrc re: people wanting no password for SQRL. The protocol is open, so do you not expect people to release implementations without a password?

KRACKing WiFI

- Block ciphers vs Stream ciphers.
- The power (and danger) of XOR
- A review of RAID 5.
- XORing with random data produces a random output since random bits are flipped.
- WiFi uses stream ciphers - essentially keyed pseudo-random bitstreams which are XORed with the data.
- NEVER REPEATING the bitstream is crucial.

The WiFi 4-way handshake



This is NOT a simple attack to perpetrate. It requires the attacker to install themselves as a WiFi MITM. But since every node's MAC address is factored into the crypto, the MITM *must* have the same MAC as the AP. So the researchers solved this by running the attacking AP on a different WiFi radio channel.

By blocking the 4th steps -- the client's final reply to the handshake -- the real AP won't get verification and will resend the 3rd handshake step. All WiFi clients will accept this repeated 3rd packet -- EVEN WITH THE SAME KEYS -- and will reset their nonce counters to 0... thus violating the cardinal rule to NEVER REUSE the same IV (nonce) under the same key.

Remediation:

Key reinstallation attacks can be mitigated at two layers.

First, the entity implementing the data-confidentiality protocol should check whether an already-in-use key is being installed. If so, it should not reset associated nonces and replay counters. This prevents the attacks so long as an attacker cannot trick an implementation into installing a different (old) key before reinstalling the current one.

A second solution is to assure that a particular key is only installed once into the entity implementing the data-confidentiality protocol during a handshake execution. For example, the generated session key in a 4-way handshake should only be installed once. When the client receives a retransmitted message 3, it should reply, but not reinstall the session key. This can be accomplished by adding a boolean variable to the state machine. It is initialized to false, and set to true when generating a fresh PTK in PTK-START. If the boolean is true when entering PTK-DONE, the PTK is installed and the boolean is set to false. If the boolean is false when entering PTK-DONE, installation of the PTK is skipped. Note that this is precisely what version 2.6 and higher of wpa_supplicant is doing.

Mitigation:

This is not good... but neither is it the end of the world. VPNs, TLS and HTTPS all prevent much harm from this. We should all update our APs and clients, and as soon as test apps appear we should verify.

Do ACCESS POINTS need to be patched? (hint: No!)

From the author's FAQ:

What if there are no security updates for my router?

<quote> Our main attack is against the 4-way handshake, and does not exploit access points, but instead targets clients. So it might be that your router does not require security updates. We strongly advise you to contact your vendor for more details. In general though, you can try to mitigate attacks against routers and access points by disabling client functionality (which is for example used in repeater modes) and disabling 802.11r (fast roaming). For ordinary home users, your priority should be updating clients such as laptops and smartphones. </quote>

Microsoft quietly fixed the KRACK vulns last Tuesday.

Android after v6.0 is vulnerable... and the trouble there is even worse, since a forced key reinstallation not only resets the nonce to zero, but also completely ZEROES the key!! Google is said to be preparing patches.

Ubuntu has already been updated:
https://launchpad.net/ubuntu/+source/wpa/2.4-0ubuntu6.2

SECURITY UPDATE: Multiple issues in WPA protocol
- debian/patches/2017-1/*.patch: Add patches from Debian stretch
- CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088

DD-WRT has been updated
http://svn.dd-wrt.com/changeset/33525

Rene posted on iMore that "Apple has already patched the KRACK attack WPA2 Wi-Fi vulnerability in the developer and public betas for iOS, watchOS, tvOS, and macOS."
But note that the AirPort is not known to have a patch underway.
https://www.imore.com/krack-wpa2-wi-fi-exploit-already-fixed-ios-macos-tvos-watchos-betas
Bleeping Computer is maintaining a list of updates:
https://www.bleepingcomputer.com/news/security/list-of-firmware-and-driver-updates-for-krack-wpa2-vulnerability/

And another page:
https://char.gd/blog/2017/wifi-has-been-broken-heres-the-companies-that-have-already-fixed-it

~30~