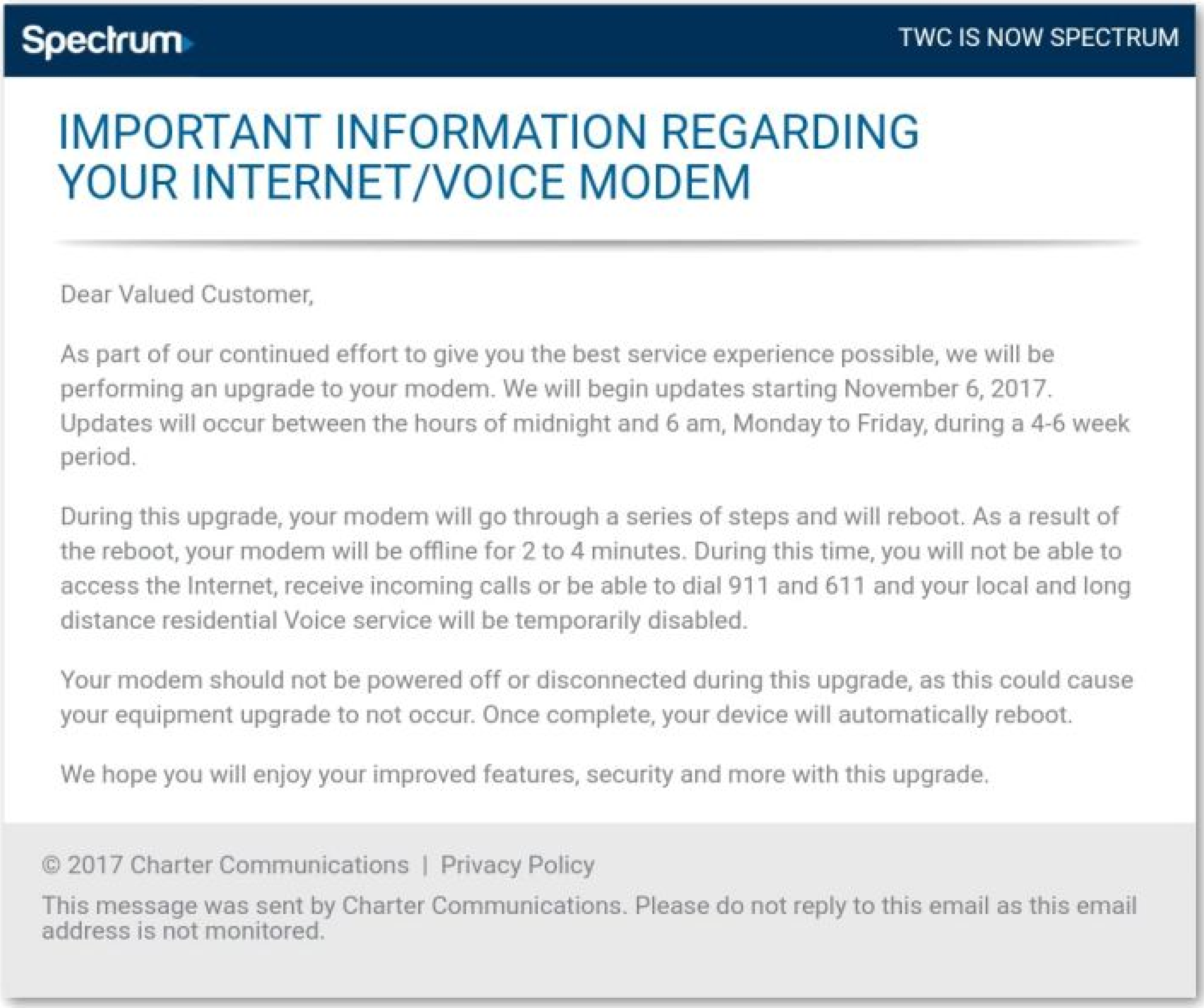
Security Now! #636 - 11-07-17
ROCA Pain

This week on Security Now!

This week we discuss the inevitable dilution in the value of code signing, a new worrisome cross-site privacy leakage, is Unix embedded in all our motherboards?, the ongoing application spoofing problem, a critical IP address leakage vulnerability in TOR and the pending major v3 upgrade to TOR, a Signal app for ALL our desktops, an embarrassing and revealing glitch in Google Docs, bad behavior by an audio driver installer, a pending RFC for IoT updating, two reactions to Win10 Controlled Folder Access, a bit of miscellany, some closing the loop with our listeners, and, three weeks after the initial ROCA disclosure I'm reminded of two lines from the movie "Serenity": Assassin:"It's worse than you know." Mal:"It usually is."

Our Picture of the Week



IMPORTANT INFORMATION REGARDING YOUR INTERNET/VOICE MODEM

Dear Valued Customer,

As part of our continued effort to give you the best service experience possible, we will be performing an upgrade to your modem. We will begin updates starting November 6, 2017. Updates will occur between the hours of midnight and 6 am, Monday to Friday, during a 4-6 week period.

During this upgrade, your modem will go through a series of steps and will reboot. As a result of the reboot, your modem will be offline for 2 to 4 minutes. During this time, you will not be able to access the Internet, receive incoming calls or be able to dial 911 and 611 and your local and long distance residential Voice service will be temporarily disabled.

Your modem should not be powered off or disconnected during this upgrade, as this could cause your equipment upgrade to not occur. Once complete, your device will automatically reboot.

We hope you will enjoy your improved features, security and more with this upgrade.

© 2017 Charter Communications | Privacy Policy

This message was sent by Charter Communications. Please do not reply to this email as this email address is not monitored.

Security News

The inevitable dilution of the value of code signing.
https://thehackernews.com/2017/11/malware-digital-certificate.html
Stuxnet-style code signing is more widespread than anyone thought
https://arstechnica.com/information-technology/2017/11/evasive-code-signed-malware-flourished-before-stuxnet-and-still-does/

A/V software needs all the help it can get in the war against malware.

Cryptography some to our aid here, again. Signed hashes of software cannot be practically spoofed.

Windows has been leveraging this power by requiring that device drivers be signed.

So a potentially valuable clue is whether any software being examined has been digitally signed.

This has created a black market for valid digital signing keys.

In years past we've covered instances of break-ins at various manufacturers... apparently with the single goal of obtaining poorly secured digital keys.

But, as with so much, this protection is not perfect.

The famous Stuxnet system carried a valid digital signature.

Three University of Maryland at College Park researchers reported that from a total of 325 SIGNED malware samples, 189 (58.2%) carried valid digital signatures while the balance (136) carried malformed signatures.

They wrote: "Such malformed signatures are useful for an adversary: we find that simply copying an Authenticode signature from a legitimate sample to an unsigned malware sample may help the malware bypass AV detection," the researchers said.

In other words, some AV is not bothering to check the validity of software signatures, only whether the software is carrying a signature block... valid or not.

Of the 189 samples that WERE signed correctly, they were generated using 111 compromised unique certificates issued by recognized CAs and also used to sign legitimate software.

Of the 111 originally-valid and now compromised certificates, 27 had been revoked while 84 remained valid and trusted despite having been used to sign known malware.

The researchers also noted that "A large fraction (88.8%) of malware families rely on a single certificate, which suggests that the abusive certificates are mostly controlled by the malware authors rather than by third parties." In other words, legitimate certificate authorities are issuing valid code-signing certificates to malware front groups posing as legitimate developers who then turn over those valid certificates to malware authors.

The researchers found that at least 34 anti-virus products failed to check the certificate's validity, allowing malicious code to run on the system.

To determine if malformed signatures can affect the anti-virus detections they downloaded 5 random unsigned ransomware samples that almost all anti-virus programs detected as malicious. They then took two expired certificates that previously had been used to sign both legitimate software and in-the-wild malware and used them to sign each of the five ransomware samples. And they found that many anti-virus products failed to detect the malware as malicious.

Three prominent anti-virus products—nProtect, Tencent, and Paloalto—detected the original UNSIGNED ransomware samples as malware, but considered eight of out ten crafted samples as benign.

Kaspersky Labs, Microsoft, TrendMicro, Symantec, and Commodo, failed to detect some of the known malicious samples when they had invalid and expired certificates attached to their code.

Other affected anti-virus packages included CrowdStrike, Fortinet, Avira, Malwarebytes, SentinelOne, Sophos, TrendMicro and Qihoo, among others.

The researchers wrote: "We believe that this [inability in detecting malware samples] is due to the fact that AVs take digital signatures into account when filtering and prioritizing the list of files to scan, to reduce the overhead imposed on the user’s machine and the time required to scan. However, the incorrect implementation of Authenticode signature checks in many AVs gives malware authors the opportunity to evade detection with a simple and inexpensive method."

The researchers said they reported this issue to the affected antivirus companies, and one of them had confirmed that their product fails to check the signatures correctly and they had planned to fix the issue.

To compliment their work, the researchers put up the site: http://signedmalware.org/

Remember that a signed certificate attempts to be an assertion of some truth. The assertion made (and makable) by code signing certificates is fundamentally different -- and much weaker -- than the assertion that can be made by a web server's DV, OV or EV domain certificate. Code signing certificates are limited to saying "I'm a person who wants a code signing certificate." That's a low bar to meet.

And AV's use of signing as another signal means that the bad guys now have strong incentive to arrange to obtain code signing certs for their malware. A cert will be used until it is revoked, and then another will be used.

Privacy Concern: Leaking the set of sites you're logged into.
https://robinlinus.github.io/socialmedia-leak/

Any site you visit can probe you to see whether you're logged into specific sites.

Same Origin Policy strongly restricts which web content JavaScript can access to coming from the same hosting site. But IMAGES, being benign and useful, are excluded from the Same Origin Policy.

The login mechanisms of most major sites will check every incoming request for the presence of a logged-in session cookie and, if not present, will redirect the user to their logon page.

In order to present the site's logo in the URL, browser tabs, etc., site place an image called "favicon.ico" in the root (/) page of the server where all visiting web browsers know to fetch it.

These facts enable JavaScript from an snooping site to probe any user's browser for their current logged-in status on another other compliant site. (And most sites are compliant.)

The snooping script simply requests the target site's /favicon.ico file, which the same origin policy allows. If the image request succeeds -- as it would if the user is logged in and the site returns the image -- the snooping JavaScript is able to detect the successful image load. But if the user is NOT currently logged on to the target site, the target site will return a redirect-to-login URL instead of an image, and the snooping JavaScript will see that as an image load failure.

Thus, while this is not a security violation per se, it's a privacy violation. The snoopy site likely DOES know who YOU are... and it can determine whether YOU are likely using any other service that you are currently logged into.

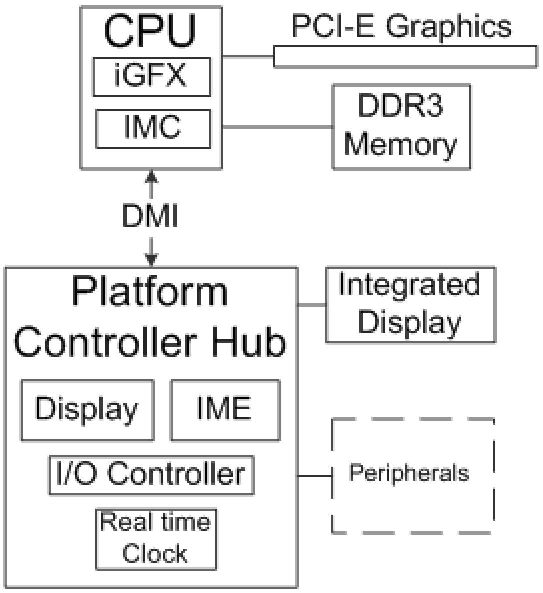
And... since ADVERTISEMENTS are also allowed to run their own JavaScript for ad rotation, etc., that also means that the third part hosts of any ads can similarly perform a rather sophisticated profiling of the person who is visiting the site hosting the advertisement.

MINIX 3 in nearly all PCs
The tech press recently went bonkers with the clickbait news that all of our Intel-based PCs all contained a full UNIX-like operating system.

MINIX 3 is believed to be used in the Intel ME found in Intel PCH (Platform Controller Hub) beginning with the introduction of ME 11 which is used with Skylake/Kaby Lake processors.

Sakaki's EFI Install Guide/Disabling the Intel Management Engine
https://wiki.gentoo.org/wiki/Sakaki%27s_EFI_Install_Guide/Disabling_the_Intel_Management_Engine

Nicola Corna's >> me_cleaner >> https://github.com/corna/me_cleaner



As we know, nearly all systems allow the system's BIOS to be updated using software only -- known as "internal flashing" -- on most PCs only the unprotected areas of the flash filesystem (excluding the ME area) can be overwritten. Consequently this guys has bitten the bullet and tackled the challenge of "external flashing"

What this does:

- Sets up a Raspberry Pi 3 Model B ('RPi3') as an in-system flash programmer;
- Reads the original firmware from the BIOS flash chip (and validating this), using the RPi3;
- Uses Nicola Corna's "me_cleaner" to create a modified copy of the firmware;
- Rewrites the modified copy of the firmware back to your PC's BIOS flash chip, again using the RPi3;
- Restarts your PC, and verifying that the IME has been disabled.

OBVIOUSLY, this is NOT for the faint of heart. It would ONLY make sense for someone who really wanted to hack. And/or perhaps in a highly security conscious enterprise where a corporation had a great many identical systems and could afford to kill one to test the solution... which could then be applied with confidence upon all of the other identical machines.

An appropriate IC clip for your target PC's flash chip, e.g.:

- a Pomona 5250 for SOIC-8 chips;
- a Pomona 5208 for unsocketed DIP-8 chips, or
- a Pomona 5252 for SOIC-16 chips;

An incredibly cool hardware hack for someone who's interested.

An Extremely Convincing WhatsApp Fake Was Downloaded More Than 1 Million Times From Google Play
http://fortune.com/2017/11/04/whatsapp-fake-google-play/
Fake WhatsApp On Google Play Store Downloaded By Over 1 Million Android Users
https://thehackernews.com/2017/11/fake-whatsapp-android.html

Hackers simply added a UNICODE "space" to the end of "WhatsApp, Inc." to make the app appear to be from WhatsApp.

Fortunately, the app used minimal permissions and only presented advertisements for other apps... but spoofed applications continue to be a huge challenge for Google... and as we've been noting here for some time, the problem of "spoofing users" shows little sign of improving.

TorMoil: a critical Tor browser vulnerability that leaks users' real IP address!
https://thehackernews.com/2017/11/tor-browser-real-ip.html
https://arstechnica.com/information-technology/2017/11/critical-tor-flaw-leaks-users-real-ip-address-update-now/

As we know, the ENTIRE REASON one uses the TOR network is to hide one's true IP address and indirectly one's identity.

An Italian researcher discovered that the MacOS and Linux flavors of the Firefox descended privacy enhancing browser used by TOR is leaking their user's IP address.

The researcher, who is the CEO of the security firm We Are Segment, privately reported the security vulnerability to Tor developers 12 days ago on Thursday (October 26), and the Tor developers have rolled out an emergency update Tor version 7.0.8.

The TorMoil vulnerability is due to a Firefox issue in "handling file://" URLs when users click on links that begin with file:// addresses.

The TOR Project posted Friday: "The fix we deployed is just a workaround stopping the leak. As a result of that navigating file:// URLs in the browser might not work as expected anymore. In particular entering file:// URLs in the URL bar and clicking on resulting links is broken. Opening those in a new tab or new window does not work either. A workaround for those issues is dragging the link into the URL bar or on a tab instead. We track this follow-up regression in bug 24136."

According to the Tor Project, users of both the Windows versions of Tor, Tails and the sandboxed-tor-browser that's in alpha testing are not affected.

The Signal Messaging App... now as a standalone desktop app!
https://signal.org/blog/standalone-signal-desktop/
https://signal.org/download/ now boasts:
Signal for: Android / iPhone / MacOS / Windows / Debian-based Linux
(And the app for Chrome has been deprecated.)

The new desktop version of Signal runs independently of any browser. Firefox or Safari users no longer need to use Chrome to send and receive Signal messages on their computers. And Chrome users will no longer need to open their browsers to have Signal Desktop open.

Windows 64-bit: 7, 8, 8.1 and 10
MacOS 10.9 and above
Linux distributions supporting APT, like Ubuntu or Debian

As a Windows user I chafe that I cannot have iMessage on my Windows desktop. Being able to link my friends together -- across all our desktops -- with high-security encrypted communications is QUITE COMPELLING.

As we know, I've taken a serious look at the Signal protocol. My first impression was that it was ridiculously over-engineered. But as I kept looking I saw how perfectly everything come together to achieve a very powerful set of security properties without sacrificing any apparent security.

Tor's Fall Harvest: the Next Generation of Onion Services
https://blog.torproject.org/tors-fall-harvest-next-generation-onion-services

After 4 years of work, the "Next Gen Onion Services" for TOR, known as "v3", is at Alpha release and getting ready for prime time.

Also known within the TOR community as "proposal 224":
https://gitweb.torproject.org/torspec.git/tree/rend-spec-v3.txt

- Better crypto (replaced SHA1/DH/RSA1024 with SHA3/ed25519/curve25519)
- Improved directory protocol, leaking much less information to directory servers.
- Improved directory protocol, with smaller surface for targeted attacks.
- Better onion address security against impersonation.
- More extensible introduction/rendezvous protocol.
- A cleaner and more modular codebase.

MUCH longer Onion addresses:

- Original - nytimes3xbfgragh.onion.
- New v3 - 7fa6xlti5joarlmkuhjaifa47ukgcwz6tfndgax45ocyn4rixm632jid.onion.

Google Docs Glitch That Locked Out Users Underscores Privacy Concerns
https://www.nytimes.com/2017/10/31/technology/google-docs-glitch-bug.html

Last Tuesday a glitch in Google Docs revealed just how much Google is inspecting what its users do.

Some Google Docs users received an alert: “This item has been flagged as inappropriate and can no longer be shared.” Others saw: “You cannot access this item because it is in violation of our terms of service.”

On Halloween, Rachael Bale (@Rachael_Bale), a reporter for National Geographic's Wildlife Watch reporting on wildlife crime, tweeted: "Has anyone had @googledocs lock you out of a doc before? My draft of a story about wildlife crime was just frozen for violating their TOS."

Responding to this last Tuesday, a Google spokesman said: "Google's automated systems periodically scan certain file types in Google Drive that are shared with other users to detect abuse and protect users, Some examples include antivirus scanning, malware and phishing detection."

"Why we can't have nice things" (or, in this case, SECURE things...)
Savitech USB audio drivers install a new root CA certificate
https://www.kb.cert.org/vuls/id/446847

Savitech provides USB audio drivers for a number of specialized audio products. Some versions of the Savitech driver package silently install a SaviAudio root CA certificate into the Windows trusted root certificate store. According to Savitech, this certificate is used for driver signing under Windows XP and is no longer necessary, but was not removed from installers for later operating systems.

A Firmware Update Architecture for Internet of Things Devices (!!)
https://tools.ietf.org/html/draft-moran-suit-architecture-00
ARM Limited
A Internet RFC working draft has been assembled and submitted by a team from ARM Limited, to propose a set of standards for IoT updating mechanisms.

It is well thought through and would be a welcome addition to this entirely vacant need.

When developing IoT devices, one of the most difficult problems to solve is how to update the firmware on the device. Once the device is deployed, firmware updates play a critical part in its lifetime, particularly when devices have a long lifetime, are deployed in remote or inaccessible areas or where manual intervention is cost prohibitive or otherwise difficult:

- Fixes to bugs in software can be applied to the device with a firmware update.

- New functionality can be added to the device with a firmware update.

The firmware update process has to ensure that

- The firmware is authenticated (attempts to flash a malicious firmware are prevented).

- The firmware can be confidentiality protected (attempts by an adversary to recover the plaintext binary can be prevented).

Win10 - Controlled Folder Access
Jakob Engblom @__jengblom
@SGgrc - Windows 10 CFA is off by default for a good reason, it breaks a bit too much stuff. My analysis: http://jakob.engbloms.se/archives/2666

Cranbarry Wallis @BarryWallis
@SGgrc I turned on Controlled? Folder Access. There were 2 old Nikon photo editing progs I had to whitelist but that was it. It works great.

Miscellany

SwiftOnSecurity @SwiftOnSecurity:
"We were the victim of a very simple attack. It was through management's lack of focus on security that this happened." ... said no company ever!

Chris Duncan (@cyberdunks)
I made an entry on TWiTs wiki site with a curricula of Security Now episodes in series.
http://wiki.twit.tv/wiki/Talk:Security_Now#Curricula

Wonderful!!

- VPNs
- Internet & LAN Technologies
- Cryptography
- Virtual Machines & Sandboxes
- Web Code Injection
- Designing a Computer
- SQRL

What was once "Screen Burn In" is now "Differential Aging"
Allen Butler (@Practical_Eng)
@leolaporte @SGgrc I have the screen 'differential ageing' on my original Google pixel and a friend has it on his original pixel xl as well.

SpinRite

From: Yann Fitzmorris
Subject: another success story SpinRite data recovery

Dear Steve and GRC team,

I purchased SpinRite a few years ago and have been using it to keep my drives in good health. I personally have never had to use it for data recovery, however, a friend asked for my help this week because her laptop would no longer boot to the log in screen. **Her laptop contained the only copy of pictures and videos of the first 2 years of her daughter's life.**

It wasn't looking good for the patient - when I plugged the drive into an external dock, no OS would recognize the drive.

I used my dedicated PC for SpinRite, plugged in the drive and ran level 2.

Success!

We plugged the drive into the doc and we were able to recover ALL pictures and videos - over 70GB. Needless to say, my friend will now seriously consider a backup solution, and I'm hoping she will buy her own copy of SpinRite to show her gratitude for this amazing product!

Thanks again for all your hard work and research. Love the Security Now podcast as well - I've been a listener since 2015.

regards,
Yann Fitzmorris

Closing The Loop

TonySalonia (@TonySalonia)
@SGgrc Steve, does uBlock Origin stop ad tracking by default? If not, what settings are necessary? I don't want to install ad track block

The BigBear UK (@TheBigBearUK)
@SGgrc what is the name of FF extension to capture whole page? you mentioned in SN?
(((Screengrab!)))

Douglas Krug (@dougkrug)
@SGgrc Just installed @TPLINK Archer C2300 router for client (new model w/ latest FW). UPnP was on by default. Someone's asleep at the wheel.

Ivan Cook (@ianc)
@SGgrc Glad I followed your suggestion to print all 2FA codes. Made updating auth app on new iPhone X much easier.

Daniel James Buckley (@buckshottz)
@SGgrc Do you have a recommendation for the most secure Identity theft protection service?

Jason Ogaard (@JasonOgaard)
@SGgrc re:miners and AV. Windows defender nuked my (legit) Monero miners when I tried to run them as Admin. Was fine with nonadmin execution.

Casey Bailey (@reptarwilleatu)
@SGgrc on the topic from this weeks SN on Chrome removing PKP soon, doesn't Google themselves use certificate pinning or is that diff?

Brian Adams (@techknowlogical)
@SGgrc You mentioned on SN a YouTube downloader you use. Since they all seem so sketchy, I'd love to know which one meets your standards.

Justin Alcorn (@JaBbA64)
@SGgrc dark matter was a 5 season arc. Cancelled after 3 seasons, breaking fans hearts. Ends on cliffhanger never resolves

ROCA Pain

Bruce Schneier: "Attacks only ever get better, they never get worse."
Further analysis of ROCA
https://arstechnica.com/information-technology/2017/11/flaw-crippling-millions-of-crypto-keys-is-worse-than-first-disclosed/

When researchers first disclosed the flaw three weeks ago, they estimated it would cost an attacker renting time on a commercial cloud service an average of:

- $38 and 25 minutes to break a vulnerable 1024-bit key and
- $20,000 and nine days for a 2048-bit key.

Organizations known to use keys vulnerable to ROCA have largely downplayed the severity of the weakness.

Estonian officials initially said the attack was "complicated and not cheap" and went on to say: "Large-scale vote fraud is not conceivable due to the considerable cost and computing power necessary of generating a private key."

But then, Sunday, researchers Daniel J. Bernstein and Tanja Lange reported they developed an attack that was 25 percent more efficient than the one created by original ROCA researchers. The new attack was solely the result of Bernstein and Lange reading the original research paper, which at the time omitted specifics of the factorization attack in an attempt to increase the time hackers would need to carry out real-world attacks.

After creating their more efficient attack, they submitted it to the original researchers.

The original researchers have since **privately disclosed their own revised attack that's as much as four times as efficient.** The release last week of the original attack may help to improve attacks further and to stoke additional improvements from other researchers as well.

So… Friday, Estonia's Police and Border Guard suspended an estimated 760,000 ID cards known to be affected by the crypto vulnerability.

The country is now issuing cards that use elliptic curve cryptography instead of the vulnerable RSA keys, which are generated by a code library developed and sold by German chipmaker Infineon.