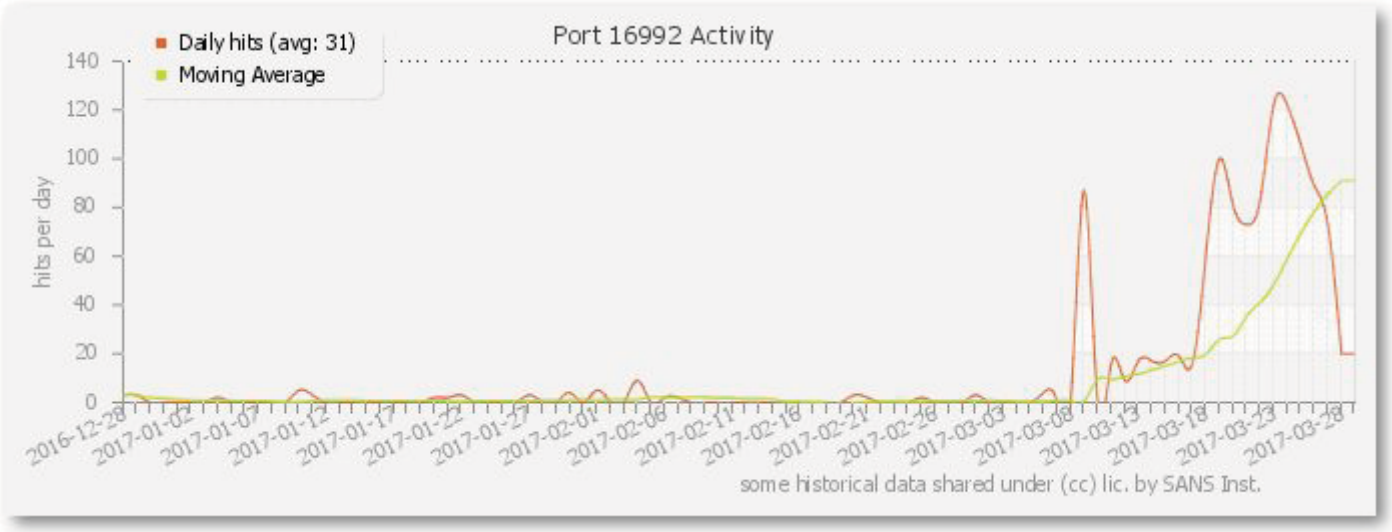
Security Now! #611 - 05-09-17

Go FCC Yourself

This week on Security Now!

This week Steve and Leo discuss much more about the Intel ATM nightmare, Tavis and Natalie discover a serious problem in Microsoft's built-in malware scanning technology, Patch Tuesday, Google's Android patches, SMS 2 factor authentication breached, Google goes phishing, the emergence of ultrasonic device tracking, lots of additional privacy news, some errata and miscellany, actions US citizens can take to express their dismay over recent Net Neutrality legislation, and some quick closing the loop feedback from our terrific listeners.

Our Picture of the Week



x0rz (@x0rz)

5/2/17, 1:00 AM

Intel released their advisory yesterday, yet people started scanning for 16992 or 16993 last month • •#Intell #AMTT #vulnerability

Security News

Intel ATM follow-up...
Last Monday, May Day, Intel released news of patches to critical vulnerabilities throughout the range of their vPro-based systems incorporating IME (Intel Management Engine) and Intel's AMT.

The AMT problem got a lot worse later in the week when the discovery was made public that all admin authentication could be trivially bypassed.

The guys at Tenable wrote this:

On May 1, 2017 Intel disclosed the AMT vulnerability (INTEL-SA-00075), but details of that vulnerability were not made public. However, Tenable researchers were able to overcome this challenge and make Tenable the first to deliver Intel AMT vulnerability detection capabilities to customers, just minutes after Intel’s announcement yesterday. This is the story of how we did it.

The hunt

The first thing our research team tried was to set up a known vulnerable target. After some searching, we found a Dell computer that had Intel AMT support but there was a problem. It was not configured/provisioned for what we needed.

The Intel Management Engine Interface (MEI) driver was installed but the Local Management Service (LMS) was not. Intel AMT documentation says the AMT configuration tool ACUWizard.exe requires LMS to be running.

So we searched and found a software package for installing LMS on Dell's website. After LMS was installed, we were able to configure/provision AMT on the computer, giving us access to AMT via the web interface.

So... in other words, AMT could not be accessed by Intel's tool from within Windows without the interfacing LMS service present and running.

The Intel Management Engine / AMT ports:

- 16992: Intel AMT HTTP
  Used for WS-Management (Web Services Management) messages to and from Intel AMT. This port is open over the network only when Intel AMT is configured or during the configuration process. Starting with Release 6.0, the port is optionally open when TLS is enabled. The port is always open locally. (But may NOT be open to the Network.)

- 16993: Intel AMT HTTPS
  Used for WS-Management messages to and from Intel AMT when TLS is enabled.

- 16994: Intel AMT Redirection/TCP
  Used for redirection traffic (SOL, Storage Redirection, and KVM using Intel AMT

authentication). Enabling the redirection listener enables this port.

- 16995: Intel AMT Redirection/TLS
  Used for redirection traffic (SOL, Storage Redirection, and KVM using Intel AMT authentication) when TLS is enabled. Enabling the redirection listener enables this port.

- 623: ASF Remote Management and Control Protocol (ASF-RMCP)
  Used for RMCP pings. This port is a standard DMTF port and accepts WS-Management traffic. It is always enabled.

- 664: DMTF out-of-band secure web services management protocol ASF Secure Remote Management and Control Protocol (ASF-RMCP)
  Used for secure RMCP pings. This port is a standard DMTF port and accepts secure WS-Management traffic. It is always enabled.

- 5900: VNC (Virtual Network Computing) - remote control program
  Used for KVM viewers that do not use Intel AMT authentication but use the standard VNC port instead. See Working with Port 5900 and Changing the Default KVM Port Setting.

The guys at SSH.COM: "This is like giving everyone with intranet access root privileges on every server whose AMT port they can communicate with (including janitors who can plug into the internal network). This also means root access to every virtual machine, container, and database running on those servers. (People with internal firewalls and dedicated management networks are in a better position!)

If your Active Directory server's AMT ports can be accessed, this is like giving every internal user Domain Administrator rights to your domains.

Intel's INTEL-SA-00075 Detection Guide
https://downloadcenter.intel.com/download/26755
https://downloadmirror.intel.com/26755/eng/Intel-SA-00075_1.0.1.6.zip

Disabling Intel AMT on Windows (and a simpler CVE-2017-5689 Mitigation Guide)
https://mattermedia.com/blog/disabling-intel-amt

Links:

- https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm
- https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm?turl=WordDocuments%2Fintelamtrelease90architecture.htm

AMT Authentication Bypass - "Silent Bob is Silent"
CVE-2017-5689, first discovered in mid-February by Berkeley, California researchers at "Embedi" who specialize in embedded system security. They reverse-engineered and examined Intel's AMT code.

As ArsTechnica wrote:

The hijacking flaw that lurked in Intel chips is worse than anyone thought
"A remote hijacking flaw that lurked in Intel chips for seven years was more severe than many people imagined, because it allowed hackers to remotely gain administrative control over huge fleets of computers without entering a password. This is according to technical analyses published Friday."
https://arstechnica.co.uk/security/2017/05/the-hijacking-flaw-that-lurked-in-intel-chips-is-worse-than-anyone-thought/

While studying the Intel AMT Implementation and Reference Guide, the researchers learned that various AMT features are available through the AMT Web-panel, which is supported by the integrated Web server, which listens to ports 16992 and 16993.

To protect the AMT from unauthorized access, the Web server provides several methods of authentication and authorization of a remote user. Intel AMT supports both Digest and Kerberos authentication though the Admin account always uses digest authentication.

They wrote: "An admin account which is present by default, and always uses digest authentication, seemed like an interesting thing to dig deeper into.

Digest Authentication:
A simple HTTP Challenge/Response authentication which allows the querying client to prove it shares a secret with the server.

The client first issues an unauthenticated query which is rejected by the server with a "401 Unauthorized" response. (We're all familiar with the "404 Not Found" response.)

But the 401 Unauthorized response includes "realm", "nonce" and other protocol-negotiating values which allow the client to then calculate a valid Authenticated query the second time.

The client reissues the original query, this time returning the "realm", "nonce" values plus a "response" value which was cryptographically determined from the server-supplied data.

MD5 generates a 128-bit hash, which is exactly and always 32 hex digits.

Hash One = MD5(username:realm:password)
Hash Two = MD5(method:digestURI)
Client's Response = MD5(HA1:nonce:HA2)

So where's the bug?

To verify the client's reply, the server internally computes the correct response it's expecting to receive and compares that to the string it actually DID receive from the client.

A comparison of two strings is essentially a comparison of two regions of memory over some number of bytes, where the regions are compared byte-by-byte looking to see whether they differ before reaching the end of the strings.

The most obvious thing for any code to do, which wants to verify an MD5 hash, would be to

verify that the client provided exactly 32 hex characters, or 128-bits. If not, there's a clear protocol error and authentication should fail.

But failing that, properly written code that wishes to compare two strings for equality should at least compare the lengths of the two strings to verify that their lengths are identical, since differing lengths would be an immediate disqualifier for string equality.

But Intel's code doesn't do that. But it's even worse than that. If you're not going to compare the two string lengths, then you at least want to compare the strings through the correct and expected length (of 32 hex characters) which was calculated by the server. But Intel's code doesn't do that either.

Incredibly, the researchers discovered that Intel's AMT code was using the length of the CLIENT's provided string for the comparison! And if that length was ZERO, no comparison would ever be performed, and the strings would be considered to be identical.

What could an attacker could do after gaining an access to the AMT services?

Intel AMT provides the ability to remotely control the computer system even if it’s powered off while electrically connected to power and the network.

Also, Intel AMT is completely independent of OS installed on the computer system. This technology allows OSes to be remotely deleted or reinstalled and there are a number of possible attacks:

KVM (remote control of mouse keyboard and monitor) can be used to remotely perform any common physical actions (with mouse, keyboard) that would be done physically at the computer. So any program could be remotely loaded and executed and any files read or written.

IDE-R (IDE Redirection) allows the boot device to be remotely changed to another device or to a virtual drive image sourced locally or remotely.

SOL (Serial over LAN) allows remote control of power, reboot, reset and more. The BIOS settings can also be accessed and modified.

Remember: Intel's security advisory of last Monday, May 1, 2017 referred to this as a "privilege escalation" vulnerability in AMT.

GRC's "ID Serve" utility:
26 Kbytes, 14 years ago (2003). Downloaded about a million times.
localhost:16992 & localhost:16993

https://www.embedi.com/files/white-papers/Silent-Bob-is-Silent.pdf

Natalie Silvanovich and Tavis Ormandy of Google Project Zero
Tavis: MsMpEng: Remotely Exploitable Type Confusion in Windows 8, 8.1, 10, Windows Server,

SCEP, Microsoft Security Essentials, and more.
https://bugs.chromium.org/p/project-zero/issues/detail?id=1252&desc=5
Tavis Writes:
MsMpEng is the Malware Protection service that is enabled by default on Windows 8, 8.1, 10, Windows Server 2012, and so on. Additionally, Microsoft Security Essentials, System Centre Endpoint Protection and various other Microsoft security products share the same core engine. MsMpEng runs as NT AUTHORITY\SYSTEM without sandboxing, and is remotely accessible without authentication via various Windows services, including Exchange, IIS, and so on.

On workstations, attackers can access mpengine by sending emails to users (reading the email or opening attachments is not necessary), visiting links in a web browser, instant messaging and so on. This level of accessibility is possible because MsMpEng uses a filesystem minifilter to intercept and inspect all system filesystem activity, so writing controlled contents to anywhere on disk (e.g. caches, temporary internet files, downloads (even unconfirmed downloads), attachments, etc) is enough to access functionality in mpengine. MIME types and file extensions are not relevant to this vulnerability, as MsMpEng uses it's own content identification system.

Vulnerabilities in MsMpEng are among the most severe possible in Windows, due to the privilege, accessibility, and ubiquity of the service.

The core component of MsMpEng responsible for scanning and analysis is called mpengine. Mpengine is a vast and complex attack surface, comprising of handlers for dozens of esoteric archive formats, executable packers and cryptors, full system emulators and interpreters for various architectures and languages, and so on. All of this code is accessible to remote attackers.

NScript is the component of mpengine that evaluates any filesystem or network activity that looks like JavaScript. To be clear, this is an unsandboxed and highly privileged JavaScript interpreter that is used to evaluate untrusted code, by default on all modern Windows systems. This is as surprising as it sounds.

We have written a tool to access NScript via a command shell for testing, allowing us to explore and evaluate it.

...

Before executing JavaScript, mpengine uses a number of heuristics to decide if evaluation is necessary. One such heuristic estimates file entropy before deciding whether to evaluate any javascript, but we've found that appending some complex comments is enough to trigger this.

The attached proof of concept demonstrates this, but please be aware that downloading it will immediately crash MsMpEng in it's default configuration and possibly destabilize your system. Extra care should be taken sharing this report with other Windows users via Exchange, or web services based on IIS, and so on.

As mpengine will unpack arbitrarily deeply nested archives and supports many obscure and esoteric archive formats (such as Amiga ZOO and MagicISO UIF), there is no practical way to identify an exploit at the network level, and administrators should patch as soon as is practically

possible.

We have verified that on Windows 10, adding a blanket exception for C:\ is enough to prevent automatic scanning of filesystem activity (you can still initiate manual scans, but it seems prudent to do so on trusted files only, making the action pointless).

Microsoft Security Advisory 4022344
Security Update for Microsoft Malware Protection Engine
https://technet.microsoft.com/en-us/library/security/4022344#ID0E3AAC
For affected software, verify that the Microsoft Malware Protection Engine version is 1.1.13704.0 or later.

To check your MsMpEng version:
Open Microsoft Security Essentials.
Drop down the Help menu at the upper right.
Choose "About"
See: Engine Version: (Mine was 1.1.13701.0)
After today's Patch Tuesday: 1.1.13704.0)

Microsoft Patch Tuesday
Patching more than 20 vulnerabilities for every platform, of which 4 are rated CRITICAL.

Google Patches 6 Critical Android Mediaserver Bugs in May Security Update
Security patch levels of May 05, 2017 or later address all of these issues.
https://source.android.com/security/bulletin/2017-05-01#announcements
Google has released its May security patches for Android.
This addresses 17 critical vulnerabilities, 6 of which affect Android Mediaserver component that could be used to execute malicious code remotely.
In addition, Google also fixed 4 critical vulnerabilities related to Qualcomm components discovered in Android handsets, including Google's Nexus 6P, Pixel XL, and Nexus 9 devices.
Google wrote: "The most severe of these issues is a Critical security vulnerability that could enable remote code execution on an affected device through multiple methods such as email, web browsing, and MMS when processing media files."

SS7 abused / hacked in Germany to steal money from bank customers.
SMS 2FA is not secure!

Signalling System 7 (SS7) is used to interconnect more than 800 telecommunications companies.

But... as we have discussed here in the past, the system is very old and lacks any kind of endpoint authentication.

But, despite that fact, we have taken to sending secondary identity authentication factors through the unauthenticated mobile telecommunications system.

And, finally and foreseeably, in January, attackers exploited these well-known SS7 weaknesses

to bypass two-factor authentication banks used to prevent unauthorized withdrawals from online accounts. After first using traditional Banking Trojan implants to perform the first stage of account compromise, and learning the account balances, they then selectively compromised the SS7 system to redirect the text messages banks used to send one-time passwords. Instead of being delivered to the phones of designated account holders, the text messages were diverted to numbers controlled by the attackers. The attackers then used the mobile transaction authentication numbers to transfer money out of the accounts.

The attacks were confirmed by the affected banks.

The Google Doc invite phishing attack.
One podcast listener wrote: Exploit is spreading quick! I've seen it twice today.

Google's Official Statement
Dear G Suite Administrator,

On Wednesday, May 3, we identified, investigated, and resolved an email phishing campaign that affected some accounts in your domain. This issue was addressed within approximately one hour from when Google became aware of it. Please note that we have already taken action to protect all users, and no further action is necessary. To assist you in understanding what happened and better educating your users on email security, we are sharing details on how the campaign worked and how we addressed it. We are also providing a CSV file identifying the users on your domain who were affected.

What happened:

The affected users received an email that appeared to be from a contact offering to share a Google doc. Clicking the link in the attacker's email directed the user to the attacker's application, which falsely claimed to be Google Docs and asked for access to the user's account. If the user authorized the application, it accessed the user's contacts for the purpose of sending the same message to those contacts. This access only retrieved contacts and sent the message onward—customer data such as the contents of emails and documents were not exposed.

Upon detecting this issue, we immediately responded with a combination of automatic and manual actions, including removing the fake pages and applications, and pushing updates through Safe Browsing, Gmail, and other anti-abuse systems.

We have taken the following steps to protect your users:

Disabled the offending Google Accounts that generated the phishing link Revoked any access that the affected users authorized to the attacker Disabled the malicious projects and apps that sought access In addition, Google is taking multiple actions to combat this type of attack in the future such as updating our policies and enforcement on OAuth applications, updating our email filters to help prevent campaigns like this one, and augmenting the monitoring of suspiciously behaving third-party apps that request consent from our users.

As a general precautionary measure, you may choose to take the following actions regularly for your users:

Review and verify current OAuth API access by third-parties. Run OAuth Token audit log reports to catch future inadvertent scope grants and set up automated email alerts in the Admin console using the Custom Alerts feature, or script it with the Reports API. We thank you for your continued business and support. If you have any questions, please let us know by contacting Google Support and referencing the issue number 37950384.

Sincerely,

The G Suite Team

SQRL and Phishing.

"Google My Activity"

- https://myactivity.google.com/myactivity

The emergence of Ultrasonic cross-device tracking

"SilverPush" - Publicly available SDK.
Privacy Threats through Ultrasonic Side Channels on Mobile Devices
The paper was published at the 2nd annual IEEE European Symposium on Security and Privacy and was presented last week in Paris, France.
https://www.sec.cs.tu-bs.de/pubs/2017a-eurosp.pdf
Four German University researchers
Abstract:
Abstract—Device tracking is a serious threat to the privacy of users, as it enables spying on their habits and activities. A recent practice embeds ultrasonic beacons in audio and tracks them using the microphone of mobile devices. This side channel allows an adversary to identify a user's current location, spy on her TV viewing habits or link together her different mobile devices. In this paper, we explore the capabilities, the current prevalence and technical limitations of this new tracking technique based on three commercial tracking solutions. To this end, we develop detection approaches for ultrasonic beacons and Android applications capable of processing these. Our findings confirm our privacy concerns: We spot ultrasonic beacons in various web media content and detect signals in 4 of 35 stores in two European cities that are used for location tracking. While we do not find ultrasonic beacons in TV streams from 7 countries, we spot 234 Android applications that are constantly listening for ultrasonic beacons in the background without the user's knowledge.

With the headline "Hundreds of privacy-invading apps are using ultrasonic sounds to track you" ZDNet summarizes it like this:

A new privacy-busting technique that tracks consumers through the use of ultrasonic tones may have once sounded like the stuff of science fiction novels, but today it's reality.

These near-silent tones can't be picked up by the human ear, but there are apps in your phone that are always listening for them. This technology is called ultrasonic cross-device tracking, and it works by emitting high-frequency tones in advertisements and billboards, web pages, and across brick-and-mortar retail outlets or sports stadiums. Apps with access to your phone's microphone can pick up these tones and build up a profile about what you've seen, where, and in some cases even the websites you've visited.

The technology is still in its infancy, but it's growing in popularity.

In the past year, researchers found 234 Android apps that include the ability to listen for ultrasonic tones without the user's knowledge. And these are not all obscure apps since, numbered among them are McDonalds and Krispy Kreme.

NONE of the 234 Android applications disclose their tracking capabilities in their privacy policies.

And we know it possible, with some limitations. Leo: You know that cool little EKG monitor? It's using frequency-modulated ultrasonics to link itself to your phone.

In their coverage of this, ArsTechnica wrote:
A Google representative said that the privacy policies enforced on all apps available in the Play market require developers to "comprehensively disclose how an app collects, uses and shares user data, including the types of parties with whom it's shared." The representative didn't respond to a follow-up question asking why none of five apps cited in the research findings disclosed the SilverPush functions. At the time this post went live, all five apps remained available in Play.
https://arstechnica.com/security/2017/05/theres-a-spike-in-android-apps-that-covertly-listen-for-inaudible-sounds-in-ads/

Amazon releases Echo data in murder case, dropping First Amendment argument
http://www.pbs.org/newshour/rundown/amazon-releases-echo-data-murder-case-dropping-first-amendment-argument/
Amazon has agreed to release any data obtained by the Arkansas defendant in that bizarre hot tub homicide after the defendant voluntarily agreed to have Amazon release the data. Prior to this, Amazon was refusing on 1st amendment grounds.

Miami Judge Says Compelling Password Production Isn't A Fifth Amendment Issue
https://www.techdirt.com/articles/20170503/15582137298/miami-judge-says-compelling-password-production-isnt-fifth-amendment-issue.shtml
TechDirt reports: Miami Judge Says Compelling Password Production Isn't A Fifth Amendment Issue

Another small dart has been lodged in the thigh of the Fifth Amendment by the courts. A Miami, FL federal judge has ruled that defendants in a sex video extortion case must turn over their phones' passwords.

In a case being closely watched in legal and tech circles, Miami-Dade Circuit Judge Charles

Johnson ruled that Hencha Voigt, and another man charged with being her accomplice, must unlock phones police believe were used in a plot to extort a social-media celebrity.

He ruled that unlocking their phones would not violate their constitutional right against self-incrimination.

The jurisprudence related to passwords and the Fifth Amendment is all over the place, but it seems to be leaning towards treating device passwords and pins as "non-testimonial." Other decisions have resulted in the indefinite jailing of defendants on contempt of court charges for refusing to turn over passwords. Arguing against self-incrimination hasn't found many judicial supporters, but the issue is far from settled.

Indefinite jailing may be on tap for these defendants as well. They've been given two weeks to comply with the order, with the "or else" being a stay of indeterminate length at the local lockup. The Miami judge appears to be following state precedent, citing an earlier case where the state appeals court ruled in favor of the government, ordering an upskirt photographer to turn over his password to prosecutors.

This decision will be appealed. But the decision cited by this judge appears to indicate this will only delay the inevitable. Sooner or later, this issue will have to be addressed by the Supreme Court, but I wouldn't hold my breath waiting for it to happen. The Supreme Court frequently takes a pass on timely issues, leaving circuit appeals courts to do most of the heavy lifting. There have not been sufficient Fifth Amendment cases of this type in federal appeals courts to press the issue. So far, the only thing that's been made clear in multiple cases is fingerprints are worse than passwords when it comes to locking law enforcement out of phone contents.

Plans for Increased Internet Surveillance Revealed in Leaked Documents
Newsweek reports: According to leaked documents, the U.K. government plans to ask for powers allowing intelligence agencies to spy on people in real-time by introducing encryption ‘back doors’ to communications firms.

Privacy advocacy organization Open Rights Group obtained a leaked copy of the government’s draft technical capability notices (TCNs) regulation, which it has published in full on its website. The document forms part of a “targeted consultation” into the Investigatory Powers Act, which was brought into law last year, meaning it has not been publicized to the tech industry or the public.

Under the proposals, all communications companies—including internet providers, messaging apps and phone networks—would be forced to provide police with real-time access to a person’s web browsing with one day’s notice.

Jim Killock, executive director of Open Rights Group, said in an emailed statement to Newsweek: “These powers could be directed at companies like WhatsApp to limit their encryption… but if the powers are exercised, this will be done in secret.”

Killock previously described the Investigatory Powers Act—referred to widely as the ‘Snooper’s Charter’—as the “most extreme surveillance law ever passed in a democracy. Writing an opinion

piece for Newsweek last year, Killock said: “[The Investigatory Powers Act] mostly permits and codifies all the illegal practices revealed through whistleblowing and court action.”

Meanwhile, here in the US: FBI director James Comey says that his organization is unable to access half of mobile devices, and supports new legislation...
During senate testimony last Wednesday, Senator Chuck Grassley (R-IA) asked whether the FBI director still believed that it was not necessary to push for a law to solve the so-called "Going Dark" problem.

Comey replied: "It may require a legislative solution at some point", adding "I could imagine a world that ends up with legislation saying if you are going to make devices in the United States you figure out how to comply with court orders."

"The shadow created by the problem called going dark continues to fall across more and more of our work." and blamed the "ubiquitous default full disk encryption on devices."

https://9to5mac.com/2017/05/04/fbi-unable-to-access-half-of-mobile-devices-comey-legislation/
The FBI Director Thinks a Law Against Encryption Is Possible Under Trump
https://motherboard.vice.com/en_us/article/fbi-director-comey-law-against-encryption-trump

Man: Border agents threatened to “be dicks,” take my phone if I didn’t unlock it
https://arstechnica.com/tech-policy/2017/05/man-border-agents-threatened-to-be-dicks-take-my-phone-if-i-didnt-unlock-it/
Ars: “I believe strongly in the Constitution and in my right to privacy.”

ALBANY, California—As he sat in a darkened corner of a neighborhood bar, Aaron Gach, an artist and lecturer at a local art college, told Ars about what happened to him in a February 2017 episode at San Francisco International Airport, where he agreed to unlock his iPhone and have it be searched by border agents rather than risk being detained and delayed further.

A US Citizen, reentering the county at SFO International Airport, is harassed without cause and detained for interrogation until he finally relents and unlocks his phone so that the customs inspectors can rifle through it.

"Can we check your phone to verify the info you provided?"

This is where I began asking lots of questions. I also asked to see the written policies authorizing their actions and we waited while they went to get a “tear sheet”. Following are some of my questions and their answers:

Is there a problem with my travel arrangements? (A: “I’m sorry but I can’t provide any details.)”

Is there a concern about the arts venue? (A: “I can’t really say at the moment.”)

What is it you want to check on my phone? Is it something in particular that I can just show you? (A: “We’re looking for information pertinent to our investigation.”)

Do I have a choice in the matter? What are my rights in this situation? As a US citizen, don't I have equal protections under the Constitution regardless of whether or not I am in an airport or outside of one? (A: "I understand your concerns, and I'm hoping we can get you on your way as soon as possible. Of course you have a choice, but we can also be dicks and just take your phone as part of our investigations if we see fit. Your phone and its contents are part of your personal effects which are subject to examination when crossing any border into the US.")

That doesn't sound like much of a choice. What happens if I choose not to unlock my phone? (A: "We can detain your phone and any personal effects needed to assist in our investigation.")

For how long? (A: "Not long. Just until we're done with it and then we would ship it back to you.")

How long would that be – days, weeks, or indeterminate? (A: Indeterminate)

But I could leave? (A: As soon as we're done.)

Am I also being detained then? (A: "No, we're not detaining you just your personal effects.)

So I can leave then? (A: "As soon as we're done here. Hopefully we can get you on your way shortly.")

Can I be present when you search my phone? (A: "No, I'm afraid not. But for this investigation I can tell you that we are only conducting a manual search and not a digital extraction. However, I can tell you from others that have refused to unlock their phones that I can't make the same claim and your information may be copied for later review.")

*Is there any reason in particular why you don't want to turn over your phone? (A: I believe strongly in the Constitution and in my right to privacy. I have nothing to hide but the only way I know if I actually have any rights is if I try to exercise them. But it sounds like I don't actually have those protections in this situation.)

https://docs.google.com/document/d/1VCMaNvsqsI7g6u2avjKK7hkJly9-FuQUptveLyXUSdo/edit#

Techdirt: New Tools Allow Voice Patterns To Be Cloned To Produce Realistic But Fake Sounds Of Anyone Saying Anything
https://www.techdirt.com/articles/20170425/07092537229/new-tools-allow-voice-patterns-to-be-cloned-to-produce-realistic-fake-sounds-anyone-saying-anything.shtml
Voice Cloning technology has been in the works for several years and before long, just as "photoshopping" an image has become "a thing" -- so, too, will the ability to impersonate anyone saying anything.

Traditionally, playing back a compromising recording of someone saying something has been regarded as strong evidence of wrongdoing -- and created a strong belief that the subject in question had actually uttered those phrases. But that assurance will soon be disappearing.

Mac users installing popular DVD ripper (Handbrake) get nasty backdoor instead
https://arstechnica.com/security/2017/05/mac-users-installing-popular-dvd-ripper-get-nasty-backdoor-instead/
"Handbrake needs to install additional codecs. Enter your password to allow this."

Hackers compromised a download server for the popular media-encoding software, Handbrake, and used it to push stealthy malware that stole victims' password keychains, password vaults, and possibly the master credentials that decrypted them.

Over a four-day period ending Saturday, a download mirror located at download.handbrake.fr delivered a version of the DVD ripping and video conversion software that contained a backdoor known as Proton. At the time that the malware was being distributed to unsuspecting Mac users, none of the 55 most widely used antivirus services detected it.

Anyone who has installed version 1.0.7 should check the SHA1 checksum of the installation file.

This can be done by opening the Mac terminal and typing:
"shasum /path/to/HandBrake-1.0.7.dmg" where "path/to" is the folder location where the installation file is found.

Or type "shasum" in the Terminal and drag the installation file into the Terminal window.

If the sum that's returned is "0935a43ca90c6c419a49e4f8f1d75e68cd70b274," the file is malicious.

Errata

- Typical comment: Great video, but that's not Cookie Monster: Cookie Monster is blue (not green), has no teeth, and lives on Sesame Street, not the Muppet Show.

- Yellow Smurfs... NOT!
  What I meant was that the Emoji images seem inherently smurfy, thus my description as "Yellow Smurfs." But a number of listeners took issue with this, noting that The Simpsons are yellow and Smurfs are blue.

Miscellany

- Not all memory leaks are important

- Explicit memory allocation / Automatic (dynamic) allocation.

- Posted to USENET's comp.lang.ada forum on March 31st, by Kent Mitchell who was consulting to Rational Software Corp. in reference to previous postings by Mitre Corp. and IBM's Watson Research Center.

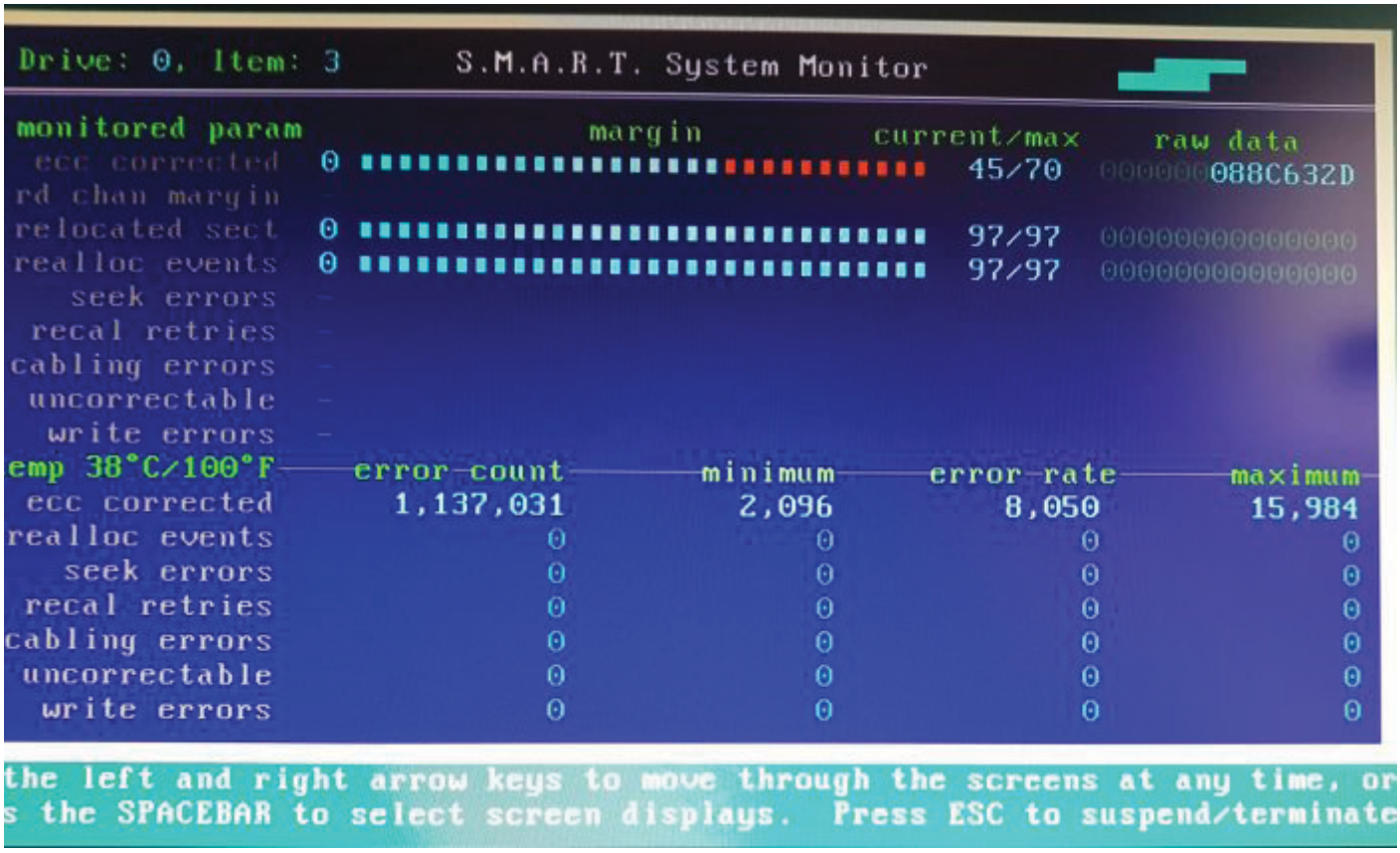
Subject: Re: Does memory leak?

"I was once working with a customer who was producing on-board software for a missile. In my analysis of the code, I pointed out that they had a number of problems with storage leaks. Imagine my surprise when the customers chief software engineer said "Of course it leaks". He went on to point out that they had calculated the amount of memory the application would leak in the total possible flight time for the missile and then doubled that number. They added this much additional memory to the hardware to "support" the leaks. Since the missile will explode when it hits it's target or at the end of it's flight, the ultimate in garbage collection is performed without programmer intervention."

SpinRite

- Steven (@Dillinger65) -- 5/6/17, 8:04 AM
  @SGgrc Hi Steve I needed to pirate a copy of SpinRite, fixed income & all.
  SpinRite saved my old laptop's HDD. One day I'll pay for a copy.

- Javier Figueiredo (@jfigueOK) -- 5/6/17, 8:09 AM
  @SGgrc SpinRiting at level 2, a 2-year old Kingston SSD.
  Does this image look like a healthy disk? pic.twitter.com/Oqg8RunCwz



- No! Those red squares show that the drive's own self-reported health is dropping under stress!! That would never happen!!

- Keith Pottratz (@KeithPottratz) - 5/8/17, 9:08 AM

@SGgrc Ran SpinRite on two computers that were not running slow. SpinRite revealed that BOTH drives were failing! Saved the day!

Go FCC Yourself
Thanks to HBO's "Last Week Tonight with John Oliver."
http://www.gofccyourself.com/ (will redirect to secured page)
https://www.fcc.gov/ecfs/search/proceedings?q=name:((17-108))

The Hill: FCC site crashes after John Oliver segment
http://thehill.com/policy/technology/332342-john-oliver-roasts-the-fccs-plan-to-curb-net-neutrality

To see existing results, click the 17-108 on the left.
To add your own short "Express" comment, click on "+ Express" on the right.

EFF: https://dearfcc.org/

Dear FCC,
The FCC has asked for public comment on new rules about net neutrality. Use this form to submit a comment to the FCC. Learn more about the FCC rulemaking process.
A nice "fill in the blanks" form letter that the EFF's new site will eMail to the FCC for us.

Closing the Loop with our Listeners

- Sable (@sablecantus) -- 5/3/17, 11:25 AM
  Hey @SGgrc - I didn't catch which iOS FTP server app is your preferred one?
  Good enough to recommend?

FileApp:
https://itunes.apple.com/us/app/fileapp-file-manager-document-reader/id297804694?mt=8

Description
FileApp is a file and documents manager for iPhone, iPad and iPod touch.
FileApp reads many files types such as PDF, Microsoft Office documents and plays multimedia contents.
FileApp will let you store files and folders on your iOS device just like Windows Explorer or the Finder on the Mac.

FILE STORAGE & TRANSFER
- USB file transfer to Mac and PC using DiskAid or iTunes File Sharing
- Robust wireless file transfer to computer via Wi-Fi (HTTP, FTP)
- Stores any file sent from any third party app (Mail, Safari...)
- Allows to "Open In..." any compatible app (Pages, Numbers, iBooks...)
- Secure folder protects files when the device is locked with a passcode

DOCUMENTS & FILES
- System-wide Pasteboard - copy text and images, paste them to FileApp to create a file automatically!
- Powerful PDF Editor with annotation, edition, comments and bookmarks support
- Create and edit text files (.txt, .html, .xml …)
- Microsoft Office documents (Word, Excel, Powerpoint), all formats supported
- RTF and Plain Text
- iWork documents (Pages, Numbers and Keynote)
- HTML files
- Safari Web Archives
- ZIP (Uncompress zip archives)
- Send documents via email attachments
- Open attachments from "Mail" app

IMAGES
- Built-in image editor with many filters and enhancements
- Import pictures and movies both from Camera Roll and Photo Library
- Take pictures within FileApp

SECURITY
- File encryption with iOS Data Protection
- Passcode to protect FileApp at startup
- Wireless transfer Password if needed

Adam Rixey (@arixey) -- 5/5/17, 3:50 PM

- @SGgrc? Does the inherent SNI domain leak make DNS Crypt fairly useless? #sn610

John Sey (@jseyb4t) -- 5/7/17, 12:07 PM

- @SGgrc What do you use for Windows 7 backup & recovery?
  Sure I heard on Security Now but can not find reference.