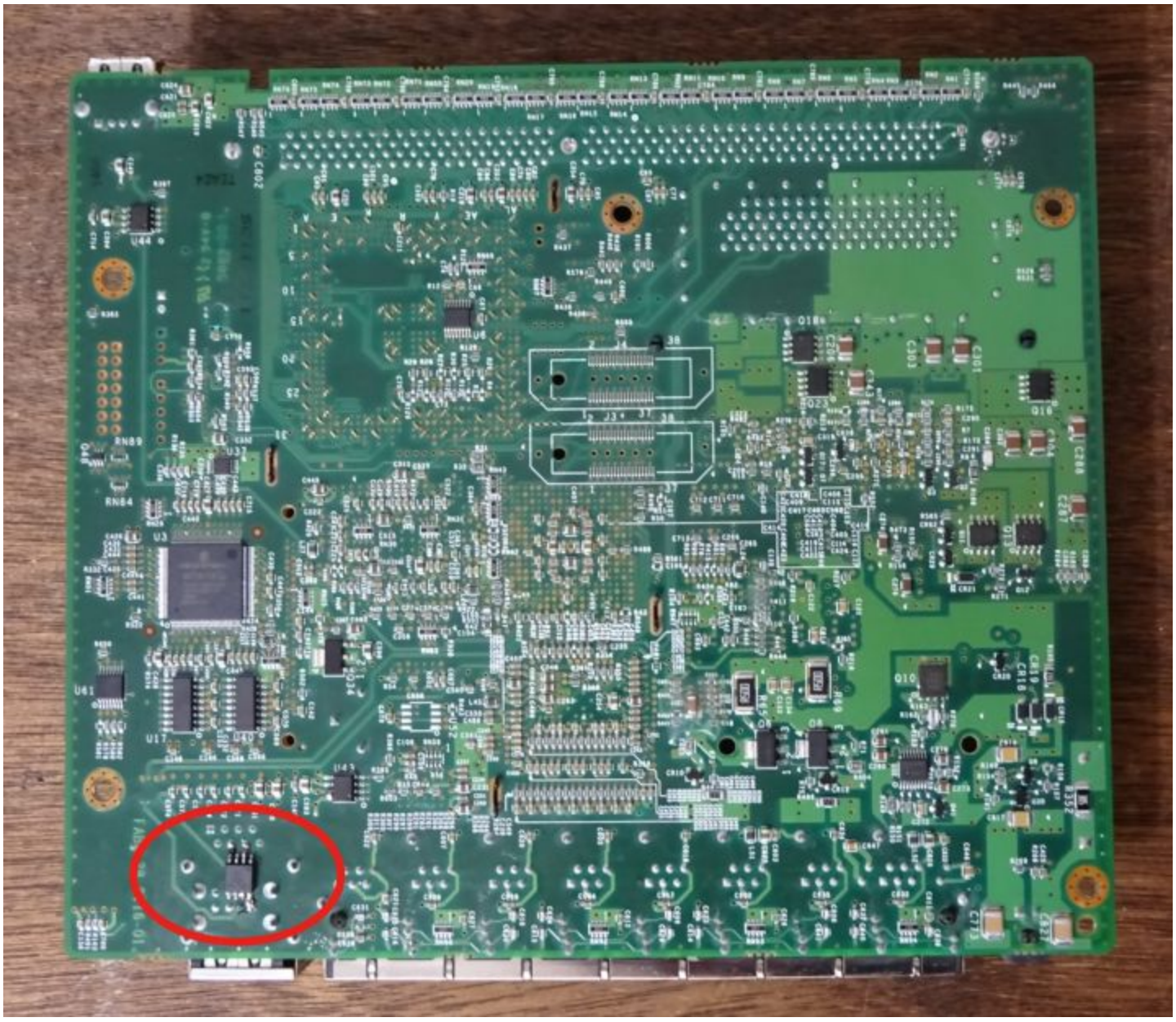
Security Now! #736 - 10-15-19

CheckM8

This week on Security Now!

This week we take a look at a sobering supply chain proof-of-concept attack, an update on the ongoing encryption debate, a blast from the past password decryption, an intriguing security & privacy consequence of today's high-resolution consumer cameras, the sad state of consumer security knowledge, OpenPGP gets a nice boost, Windows Defender gets Tamper Protection and SQRL gets a very nice mention by Google's Cloud Security architects. We'll then share a bit of sci-fi and fun miscellany and conclude by examining the crucially important, widely available and completely unpatchable Apple Boot ROM exploit known as “CheckM8.”

We are operating in a world of pseudo security



Security News

A sobering reminder about supply chain attacks
No, they're not common. No, they won't be employed by random 400 pound anti-social hackers living in their mother's basement. But anyone who completely discounts them and imagines that they are impossible... is fooling themselves.

Andy Greenberg, writing for Wired magazine re-introduced the idea by reminding us:

"More than a year has passed since Bloomberg Businessweek grabbed the lapels of the cybersecurity world with a bombshell claim: that Supermicro motherboards in servers used by major tech firms, including Apple and Amazon, had been stealthily implanted with a chip the size of a rice grain that allowed Chinese hackers to spy deep into those networks. Apple, Amazon, and Supermicro all vehemently denied the report. The NSA dismissed it as a false alarm. The Defcon hacker conference awarded it two Pwnie Awards, for "most overhyped bug" and "most epic fail." And no follow-up reporting has yet affirmed its central premise."

Next week in Stockholm, Sweden, October 21-24, the CS3STHLM security conference will be held. The conference bills itself as the premiere cyber security conference for ICS/SCADA and Critical Infrastructure. During that conference security researcher Monta Elkins who works as the "Hacker in Chief" for the industrial control security firm FoxGuard will be showing off his handiwork.

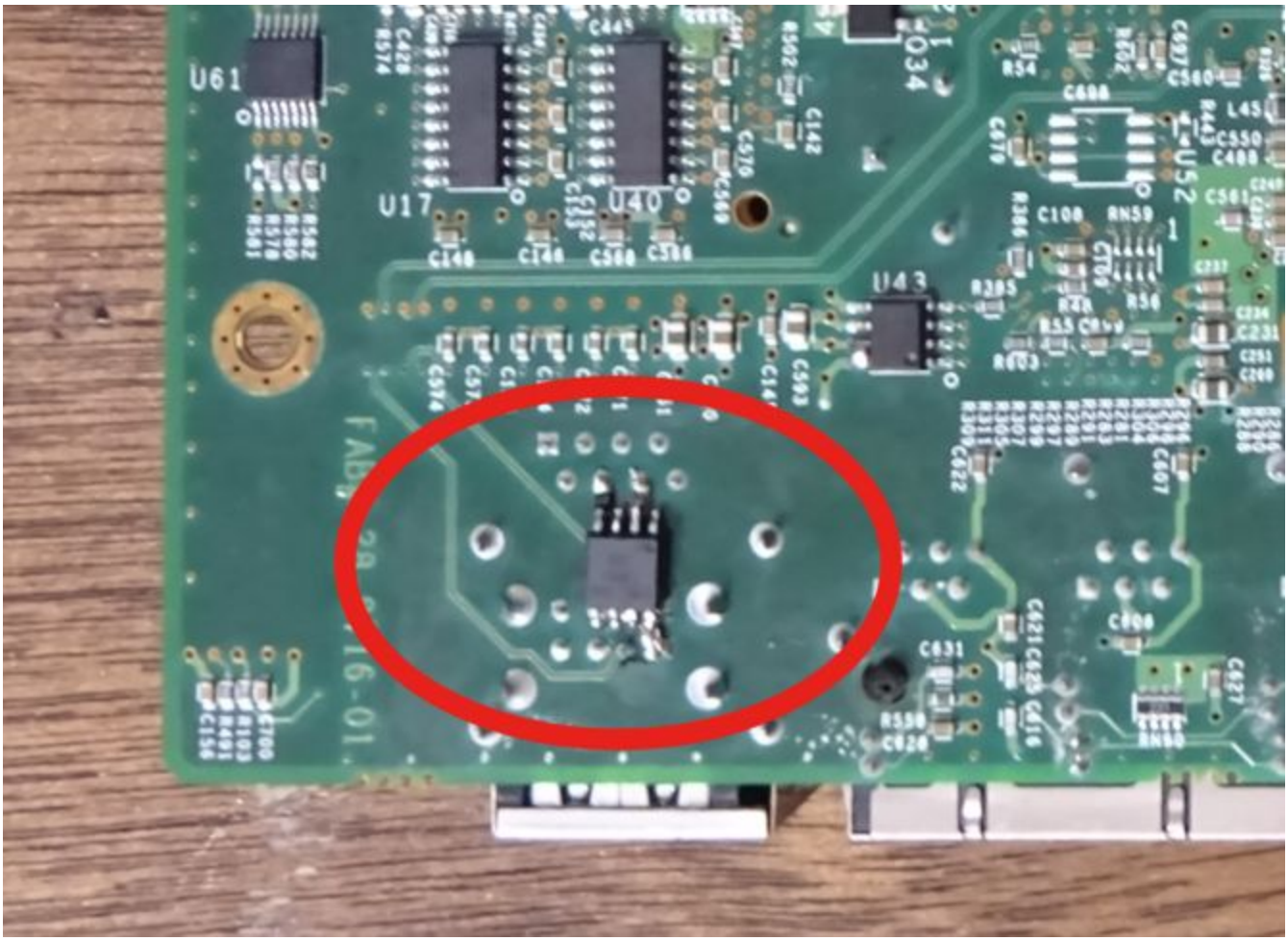
Monta will be vividly demonstrating just how easily spies, criminals, or saboteurs with even minimal skills, working on a shoestring budget, can plant a chip in enterprise IT equipment to create a stealthy backdoor access for themselves. Armed with a $150 hot-air soldering tool, a $40 microscope, and some $2 chips ordered online, Elkins altered a commercial Cisco firewall in a way that he says most IT admins likely wouldn't notice, yet would give a remote attacker deep control.

During his interview with Andy Greenberg, Elkins said: "We think this stuff is so magical, but it's not really that hard. By showing people the hardware, I wanted to make it much more real. It's not magical. It's not impossible. I could do this in my basement. And there are lots of people smarter than me, and they can do it for almost nothing."

So... Elkins used an ATtiny85 chip, it's about 5 millimeters square with four tiny mounting pins on two sides across from each other. He pulled the chip from a $2 Digispark Arduino board. It's not quite the size of a grain of rice, but it's tiny. After writing his code into that chip, Elkins desoldered it from the Digispark board and soldered it to the motherboard of a Cisco ASA 5505 firewall. He found an inconspicuous spot that required no extra wiring and would give the chip access power and to the firewall's serial port.

Our picture of the week shows the chip sitting there among all of the other identical looking chips. There's no way anyone who opened the case of the Cisco firewall to do a physical inspection would notice anything out of the ordinary. "Nothing to see here, move along."

Elkins noted that he could have used an even smaller chip, but chose the ATtiny85 because it was easier to program. He says he also could have hidden his malicious chip even more subtly, inside one of several radio-frequency shielding "cans" on the board, but he wanted to be able to show the chip's placement for the security conference.



So what does this itty bitty chip do? Elkins programmed his tiny stowaway chip to carry out an attack as soon as the firewall boots up in a target's data center. It impersonates a local security administrator who would access firewall's configuration by connecting their computer directly to the firewall's hardware admin port. As at boot, the chip triggers the firewall's password recovery feature to create a new admin account allowing subsequent full remote admin access to the firewall's settings. Elkins noted that he chose Cisco's ASA 5505 firewall for his demo because it was the cheapest one he found on eBay. But he noted that any Cisco firewall that offers that sort of recovery in the case of a lost password should work. He also noted that with a bit more reverse engineering, it would also be possible to reprogram the firmware of the firewall to make it into a more full-featured foothold for spying on the victim's network, though he didn't go that far in his proof of concept.

I wanted to highlight the triviality of this proof-of-concept for our listeners. For non hardware types this sort of thing might seem like exotic Sci-Fi. But it’s really not. It’s extremely possible to hide in plain sight. Think of it like what’s happened with today’s operating systems. The grey beards among us will, probably fondly, recall those days of yesteryear when we knew and could identify every file on our 10 megabyte hard drive. Back then, we thought that’s the way it was

supposed to be. Needless to say, those days are long long gone. Not only do we now have no idea what the hell is loaded onto our multi gig, if not multi-terabyte, drives, but we don't even know what most of the processes running in our machines are doing. Talk about hiding in plain sight.

Similarly, looking at any modern motherboard or security appliance like a firewall, we see a sea of tiny chips. There's literally no way to know whether they are from the factory or not.

Again… I'm not wearing a tinfoil beanie. I know this likely doesn't affect **ANY** of us, and never will. But we do keep seeing that what can be done, is done. And we know that cyber espionage is a real thing. For a nation state actor, intercepting the physical shipment of a device is not difficult. And the payoff from implanting an undetectable hardware backdoor could be significant.

So what would I do if I was really really worried and had to be safe? One possibility would be to ask a favor of a completely unaffiliated company to purchase the hardware on my behalf, then go pick it up myself. Another possibility is to note that these turnkey appliances are typically just offering pre-packaged solutions. Anything they can do can probably be done by gluing some off-the-shelf Linux or Unix apps together in any generic server PC. For example, Linux/Unix firewalls are very capable. So if just roll-your-own, then it is your own.

Facebook's stance on end-to-end encryption raises official protests

As we know, last March 6th, Mark Zuckerberg posted "A Privacy-Focused Vision for Social Networking" wherein he stated:

https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/

> "I believe the future of communication will increasingly shift to private, encrypted services where people can be confident what they say to each other stays secure and their messages and content won't stick around forever. This is the future I hope we will help bring about. We plan to build this the way we've developed WhatsApp: focus on the most fundamental and private use case -- messaging -- make it as secure as possible, and then build more ways for people to interact on top of that, including calls, video chats, groups, stories, businesses, payments, commerce, and ultimately a platform for many other kinds of private services."

Mark's posting was much longer and it covert many points. But, basically, the entire thing was a manifesto for privacy and unbreakable -- by anyone -- encryption.

Predictably, in our current environment where the whole question of government and law enforcement "legal access" to any and all private communications remains very much up in the air and unsettled, several governments have now formally pushed back against Facebook's declared intentions.

https://www.justice.gov/opa/press-release/file/1207081/download

In a two and a half page Open Letter dated October 4th, co-signed by law enforcement authorities in the US, the UK and Australia, Facebook is strongly urged to halt its plans for end-to-end encryption. I won't bore our listeners with the entire letter, but it begins…

> Dear Mr. Zuckerberg,
>
> OPEN LETTER: FACEBOOK'S "PRIVACY FIRST" PROPOSALS
>
> We are writing to request that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to protect our citizens.
>
> In your post of 6 March 2019, "A Privacy-Focused Vision for Social Networking," you acknowledged that "there are real safety concerns to address before we can implement end-to-end encryption across all our messaging services." You stated that "we have a responsibility to work with law enforcement and to help prevent" the use of Facebook for things like child sexual exploitation, terrorism, and extortion. We welcome this commitment to consultation. As you know, our governments have engaged with Facebook on this issue, and some of us have written to you to express our views. Unfortunately, Facebook has not committed to address our serious concerns about the impact its proposals could have on protecting our most vulnerable citizens.
>
> We support strong encryption, which is used by billions of people every day for services such as banking, commerce, and communications.We also respect promises made by technology companies to protect users' data. Law abiding citizens have a legitimate expectation that their privacy will be protected. However, as your March blog post recognized, we must ensure that technology companies protect their users and others affected by their users' online activities. Security enhancements to the virtual world should not make us more vulnerable in the physical world. We must find a way to balance the need to secure data with public safety and the need for law enforcement to access the information they need to safeguard the public, investigate crimes, and prevent future criminal activity. Not doing so hinders our law enforcement agencies' ability to stop criminals and abusers in their tracks.
>
> Companies should not deliberately design their systems to preclude any form of access to content, even for preventing or investigating the most serious crimes. This puts our citizens and societies at risk by severely eroding a company's ability to detect and respond to illegal content and activity, such as child sexual exploitation and abuse, terrorism, and foreign adversaries' attempts to undermine democratic values and institutions, preventing the prosecution of offenders and safeguarding of victims. It also impedes law enforcement's ability to investigate these and other serious crimes.
> 2 Risks to public safety from Facebook's proposals are exacerbated in the context of a single platform that would combine inaccessible messaging services with open profiles, providing unique routes for prospective offenders to identify and groom our children.

It then congratulates Facebook on the number of child sexual abuse cases they help law enforcement with and details one particularly poiniant case involving an 11 year old.

The letter concludes with:

> Equally important to Facebook's own work to act against illegal activity, law enforcement rely on obtaining the content of communications, under appropriate legal authorisation, to save lives, enable criminals to be brought to justice, and exonerate the innocent. We therefore call on Facebook and other companies to take the following steps:
>
> - Embed the safety of the public in system designs, thereby enabling you to continue to act against illegal content effectively with no reduction to safety, and facilitating the prosecution of offenders and safeguarding of victims;
>
> - Enable law enforcement to obtain lawful access to content in a readable and usable format;
>
> - Engage in consultation with governments to facilitate this in a way that is substantive and genuinely influences your design decisions; and
>
> - Not implement the proposed changes until you can ensure that the systems you would apply to maintain the safety of your users are fully tested and operational.
>
> We are committed to working with you to focus on reasonable proposals that will allow Facebook and our governments to protect your users and the public, while protecting their privacy. Our technical experts are confident that we can do so while defending cyber security and supporting technological innovation. We will take an open and balanced approach in line with the joint statement of principles signed by the governments of the US, UK, Australia, New Zealand, and Canada (the Five Eyes) in August 2018 and the subsequent communique agreed in July this year. As you have recognised, it is critical to get this right for the future of the internet. Children's safety and law enforcement's ability to bring criminals to justice must not be the ultimate cost of Facebook taking forward these proposals.

Facebook, for its part, replied with a reiteration of some of its previous statement by stating:

> We believe people have the right to have a private conversation online, wherever they are in the world. As the US and UK governments acknowledge, the CLOUD Act allows for companies to provide available information when they receive valid legal requests and does not require companies to build back doors.
>
> We respect and support the role law enforcement has in keeping people safe. Ahead of our plans to bring more security and privacy to our messaging apps, we are consulting closely with child safety experts, governments and technology companies and devoting new teams and sophisticated technology so we can use all the information available to us to help keep people safe.
>
> End-to-end encryption already protects the messages of over a billion people every day. It is increasingly used across the communications industry and in many other important sectors of the economy. We strongly oppose government attempts to build backdoors because they would undermine the privacy and security of people everywhere.

Tech companies are happily implementing unbreakable end-to-end encryption. As we know, it's not difficult -- ransomware does it night and day. And customers love the idea of unbreakably encrypted privacy. However, our companies are ultimately subject to the laws of the countries within which they operate. And there's no way that Apple, Facebook and Google will be outlaw

organizations. So eventually they will be forced to compromise. That's the only way this drama is going to play out. I hope I'm would. And the US Congress, where any such legislation would need to originate, does seem to be a bit timid about this. But the UK seems much less so. So I would expect the US to follow rather than lead in such legislation.

[And on the lighter side in a fun bit of news…]

UNIX's Co-Creator Ken Thompson's BSD UNIX Password Has Finally Been Cracked
(And it was a pretty good password, too.) So, yes... after 39 years, the elusive password used by Ken Thompson, who was, of course, the co-creator of UNIX, has finally been cracked.

The story begins five years ago, when developer Leah Neukirchen spotted an interesting "/etc/passwd" file in a publicly available source tree of historical BSD version 3 from 1980, which includes hashed passwords belonging to more than two dozens Unix luminaries who worked on UNIX development, including Dennis Ritchie, Stephen R. Bourne, Ken Thompson, Eric Schmidt, Stuart Feldman, and Brian W. Kernighan.

Since those early passwords were protected using the long since depreciated DES-based descrypt -- aka crypt(3) -- algorithm, and were limited to at most 8 input characters, Leah decided to brute-force them for fun. She successfully cracked the passwords for most of the UNIX luminaries using password cracking tools like "John the Ripper" and "hashcat".

But the toughest one's to crack -- which she was unable to crack -- belonged to Ken Thompson and five other contributors who helped build the Unix system, including Bill Joy, who, as we know, later co-founded Sun Microsystems and designed Java.

She wrote in a blog posting last Wednesday: "Ken's password eluded my cracking endeavor. An exhaustive search back in 2014 through all lower-case letters and digits took several days and yielded no result. She notes that compared to other password hashing schemes (such as NTLM), descrypt turns out to be quite a bit slower to crack."

Earlier this month, Neukirchen posted all her findings on the Unix Heritage Society mailing list and requested help from other members to crack the remaining passwords. And just 6 days later, Australian engineer Nigel Williams responded with the plaintext password used by Ken Thompson, which he cracked after 4 days using "an AMD Radeon Vega64 running hashcat at about 930MH/s."

Thompson's password has been revealed as "p/q2-q4!" — which is chess notation describing the move "pawn from Queen's 2 to Queen's 4." Ken Thompson, who is now at Google where he developed Google's "Go" programming languages responded with another short 8-characters, saying: "Congrats"

And the next day, another mailing list member, Arthur Krewat, successfully cracked and provided the passwords for four more remaining uncracked hashes.

- Ken Thompson, co-inventor of Unix: p/q2-q4!
- Dennis Ritchie, co-inventor of BSD and creator of the C programming language: dmac

- Brian W. Kernighan, Canadian computer scientist and Unix contributor: /.,/.,
- Stephen R. Bourne, creator of the Bourne shell command line interpreter: bourne
- Eric Schmidt, an early developer of Unix software and Former Google CEO: wendy!!!
- Stuart Feldman, author of Unix automation tool make and the first Fortran compiler: axolotl

Consequences of Consumer High Resolution Cameras

- Photos of keys at a distance
- Bouncing a laser off a window to pick up the window pane vibrations.
- Distant photos of the vibrations of a balloon to pick up the conversations.

Now we have... Stalkers locating celebrities by examining the reflections picked up in their eyes' irises.

A Japanese stalker has confessed to stalking and attacking a young Japanese pop star by zooming in on the reflections in her eyes from photos she posted on social media. After the assult a 26-year-old man by the name of Sato was arrested and confessed to police that he'd used the star's selfies to figure out where she lived. Each of her pupils reflected the nearby streetscape, which he plugged into the street map function of Google Maps to locate matching bus stops and scenery. Je also confessed to observing other reflections in Matsuoka's eyes: curtains, windows, and the angle of the sun. That enabled Sato to guess which floor she lived on in the building.

This case demonstrates that with the ever-higher resolution of cameras, the high-definition selfies we post online disclose actionable intelligence about who – and exactly where – we are. Eliot Higgins, the founder of investigations site Bellingcat, which has pioneered online investigative techniques, told the BBC that the better quality the image, the more potential there is for it to be used in geolocating us. He said:

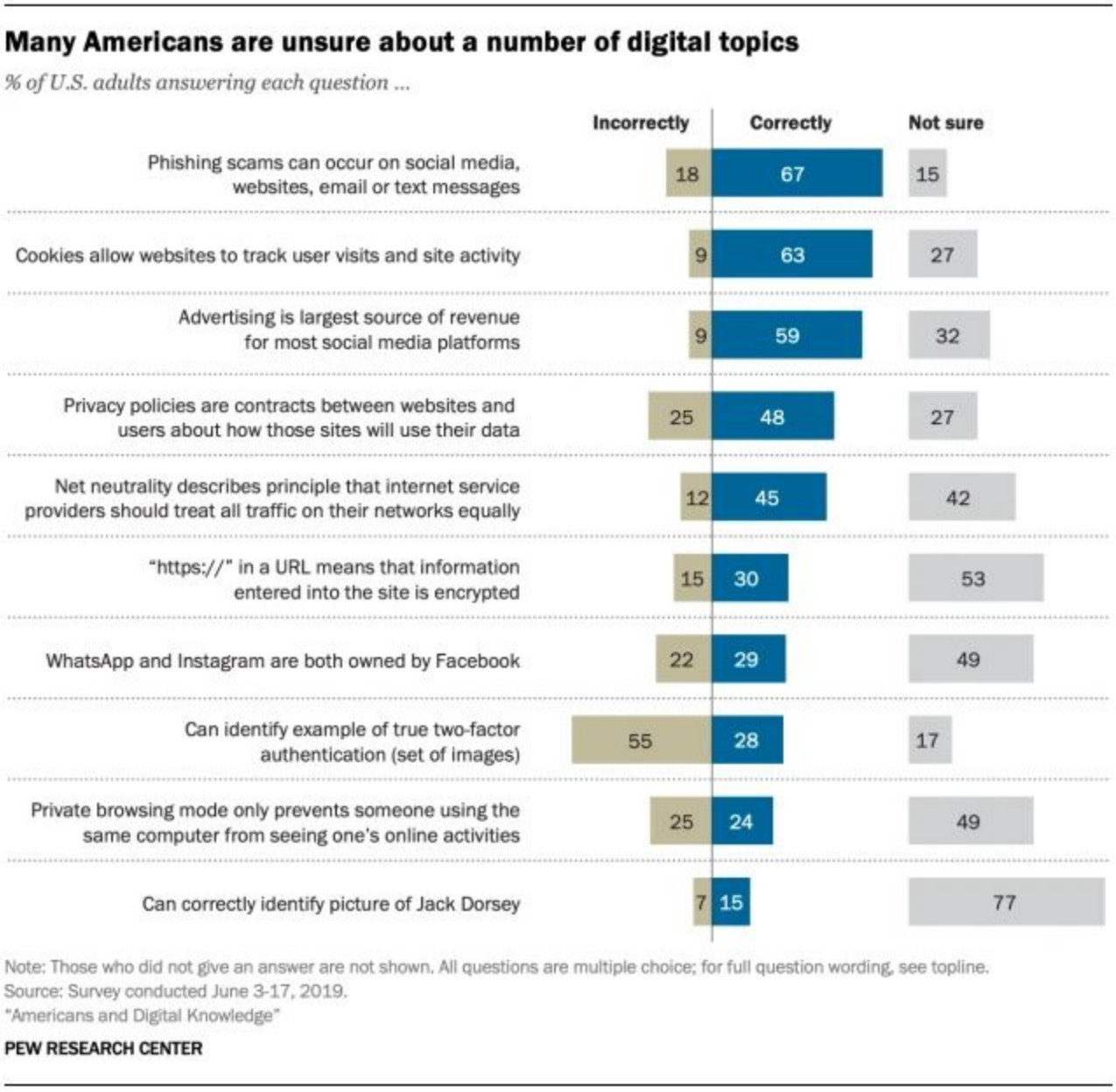
> Higher quality images allow for more details to be identified that can help with geolocation, and the more reference imagery there is from services like Google Street View, the greater the chance of determining a location. Even the tiniest of details can reveal a lot of information about where a photograph is taken, and information about the individuals in the photograph.

It's worth noting that location-reflecting eyeballs in high-resolution photos are not the only way for gelatin data to leak. Photo EXIF data, which may include the GPS coordinates of a photo, may do the same thing. Also, Google's computer vision specialists have worked to train deep-learning machines to determine the location of almost any photo just by using its pixels and relying on image retrieval. This is enabled since Google has an extraordinary number of images to train it on.

So now we have one more thing to consider when posting out photos online. The best advice for celebrities, dissidents, and other person's of interest would be to make their posting locations explicitly known, then conduct themselves accordingly -- with the knowledge that everyone knows where they are. If that's a problem, then take other protective measures. That's a safer course of action than assuming that you're always able to keep your location secret... since that's clearly becoming less and less true.

Americans and Digital Knowledge
Last Wednesday, the well known US Pew Research Center shared the results of their survey of American's understanding of technology-related security issues. They found, not surprisingly, that a majority of U.S. adults were able to answer fewer than half of the survey's digital knowledge quiz questions correctly, and that many struggle with cybersecurity and privacy questions.

https://www.pewinternet.org/2019/10/09/americans-and-digital-knowledge/



Amerians' knowledge would best be described as a bit spotty: While a majority of U.S. adults can correctly answer questions about phishing scams or website cookies, other items are more challenging. For example, just 28% of adults can identify an example of two-factor authentication. And only about one in four Americans (24%) know that private browsing hides browser history from other users of that computer, while roughly half (49%) say they are unsure what private browsing does.

Pew's survey consisted of 10 questions designed to test Americans' knowledge of a range of digital topics, such as cybersecurity or the business side of social media companies. The median number of correct answers was four. Only 20% of adults answered seven or more questions correctly, and just 2% got all 10 questions correct.

As was true in a previous Center survey, Americans' knowledge of digital topics varies substantially by educational attainment as well as by age. Adults with a bachelor's or advanced degree and those under the age of 50 tend to score higher on these questions. Pew surveyed 4,272 adults living in the United States conducted June 3-17, 2019.

Pew found that Americans' understanding of these topics varies drastically across the 10 questions presented. For example, only three questions were answered correctly by a majority of adults:

- About two-thirds of U.S. adults (67%) know that phishing scams can occur across multiple platforms, including email, text messages, social media or websites.

- 63% of Americans understand that cookies are text files that allow websites to track users' site visits and activities.

- Similarly, 59% know that advertising is the largest source of revenue for most social media sites, rather than things such as exclusive licensing deals (4%) or corporate consulting (2%).

Additionally, 48% of adults correctly answered that a privacy policy is a contract between websites and users regarding how their data will be used, while 45% know that net neutrality refers to the principle that Internet service providers should treat all traffic on their networks equally.

Other concepts in the survey are far less familiar to the public. Only three-in-ten adults correctly answered that starting a URL with "https://" means that the information entered on that site is encrypted (30%). A similar share (28%) accurately identified an example of two-factor authentication. A somewhat smaller share – 24% of Americans – is aware that "private browsing" or "incognito mode" only hides online activity from other individuals using the same computer.

Americans' knowledge of the business side of social media companies is also relatively low. Just 29% of Americans correctly named WhatsApp and Instagram as two companies owned by Facebook. And when presented with a photo of Twitter co-founder and CEO Jack Dorsey, only 15% of adults correctly identified him. (I'm pretty sure I wouldn't recognize his photo.)

What deeply annoys me about this Pew Research survey is that these questions are even an issue. Our moms should NEVER have to know any of this stuff. This is deeply abusive. This whole mess that we call The Internet was created by techies for techies... but most of the world are NOT techies.

Back in the early days of automobiles the darned horseless carriages were breaking down all the time. The confounded machines were unreliable and finicky as hell. So anyone driving one needed to be a bit of an auto mechanic. And that was part of the fun, because those early autos

were simple and understandable. My own first car was a burgundy FIAT 850 Spider. I completely took it apart in our garage and rebuilt it from the ground up. I knew and loved that car inside and out. And if something broke I knew what and where and I could go get the part and fix it myself. But not any more. The car I'm driving today is not, as they say "user serviceable." But what it is, in return for being a black box, is, all things considered, incredibly reliable. I get in and turn the key and it goes. It does what it's supposed to do.

We're not quite there yet with today's computers. But I think that needs to be our target. Over time they are going to become less and less comprehensible and more and more "black boxes." And I think that's fine if, in return, they deliver reliability and security.

OpenPGP being built into Mozilla's Thunderbird eMail client

Thunderbird currently has a 3rd-party plug-in "Enigmail", but it requires users to install additional third-party software like GnuPG or GPG4Win before installing Enigmail itself. And the licenses governing those libraries are incompatible with Thunderbird's -- MPL version 2.0 vs. GPL version 3+. So the Thunderbird folks will need to find a compatible library.

But, starting with Thunderbird 78, scheduled for release in the summer of 2020, OpenPGP will be built-in and filly supported natively.

Windows 10 Tamper Protection being enabled by default

It really doesn't do much good to have Windows Defender watching the store if it can simply be turned off by sufficiently clever malware. And there have been increasing reports of exactly that happening.

So yesterday Microsoft announced that the new Windows 10 Tamper Protection security feature, which was added to Windows 10 1903, the May 2019 update, is now officially available for both Enterprise and consumer users. Along with this announcement, Microsoft will be enabling this security feature on all Windows 10 devices by default.

When enabled, as it will be, Tamper Protection prevents Windows Security and Windows Defender settings from being changed by programs, Windows command line tools, Registry changes, or group policies. Moving forward, the only way to configure it and/or modify its settings will be directly through the Windows 10 user interface or with Microsoft enterprise management software, such as Intune.

I checked my Win10 machine that I just fired up for this Skype session and Tamper Protection was not currently enabled. But the switch was there... so I manually flipped it to "on". Given Microsoft's confidence that nothing will break, I think it's probably a safe thing for others to do.

Sci-Fi & Fun

- "Ad Astra" - Brad Pitt wanders around through outer space
- El Camino - What happened to Jesse Pinkman?

SQRL

Modern password security for system designers
What to consider when building a password-based authentication system
By Ian Maddox and Kyle Moschetto, Google Cloud Solutions Architects

https://cloud.google.com/solutions/modern-password-security-for-system-designers.pdf

Alternatives to passwords / SQRL (Page 18)

The Secure Quick Reliable Login protocol is a recent addition to the security space. It is designed for end-user authentication to websites and applications. SQRL users run a small client application on their Modern password security for system designers computer or in their browser. Instead of giving servers a password that they must keep secret, the client provides a public key that is unique to the application or domain the user wants to authenticate to. The server provides a unique value to the client, and the client must then use their private key to sign and return that secret. The server verifies the signature by using their public key and authenticates the user. Most importantly, a compromised site or service cannot expose its users' credentials in a way that impacts any other site or service.

Users can expect to see the option for SQRL login to appear in more places in the coming years. Developers and software architects will appreciate the deep level of technical detail written with an eye toward an evolving security landscape and the way real humans interact with security controls.

And a thanks to "Compilenix @Compilenix" for the heads-up about SQRL's inclusion in the guides.

CheckM8

"CheckM8" is a recently discovered, unpatchable, iOS Boot ROM. What does it mean for us? https://www.sentinelone.com/blog/checkm8-5-things-you-should-know-new-ios-boot-rom-exploit/

Two weeks ago the iOS jailbreaking community received a welcome surprise when a security researcher axi0mX dropped what's been described as a 'game changing' new exploit affecting Apple's mobile platform. He calls it 'checkm8'. It's a Boot ROM exploit being widely proclaimed the most important single exploit ever released for iPhone, iPad, Apple TV and Apple Watch devices. So... what does that actually mean for the security of the millions of affected iOS devices out there, in use in both personal and enterprise environments?

Are iOS Devices Now Insecure Because of checkm8?

No. CheckM8 will mostly, at least initially and directly prove to be a massive boon for security researchers who wish to peek under the hood despite Apple's every attempt to prevent that. The only real threat to end users might be that by allowing researchers and hackers to get in under the hood, it could facilitate the discovery of other weaknesses… which is, as we know, all too possible, since Apple **IS** constantly patching other discoveries.

But for now at least, Checkm8 doesn't directly affect end users. For one thing, there is no remote execution path. An attacker cannot use checkm8 to compromise an untethered device. That means anyone wanting to use this exploit without having the target device physically in their possession is out of luck.

Second, checkm8 does not allow a threat actor to bypass a device's TouchID or PIN protections. In other words, it does not permit any compromise of the Secure Enclave. So the user's personal data remains safe from attackers who are lacking the device's unlock credentials, notwithstanding the possibility of other zero days. This is, in itself, a testament to Apple's multi-layered security design philosophy. The idea that a full Boot compromise -- which is that CheckM8 enables -- would still leave the user's private data secure should be comforting to all Apple device users.

Also, there is no persistence mechanism. If an attacker were to gain physical access to an affected device and used the Boot ROM exploit to compromise it, re-booting the device would restore its normal Boot-Chain security. And any changes made by the attacker would be lost as Apple's security checks would either delete any files modified by the attacker or refuse to run them.

So the big question is... which iOS Devices Are Affected by checkm8?

Though not every iOS device is affected by checkm8, the vast majority in use are. On the most recent devices -- an iPhone XR, XS, XS Max or any of the iPhone 11 series, all of which use the A12 Bionic or later chip -- the Boot ROM exploit will not work on it. That's because the use-after-free vulnerability that axi0mX found appears only in devices using A11 chips or earlier,

which includes from iPhone 4S -- which uses the A5 chip -- through the iPhone 8 and X models, as well as any iPad, Apple TV or Apple Watch device using A11 or earlier chips. Therefore, most generations of iPhones and iPads are vulnerable.

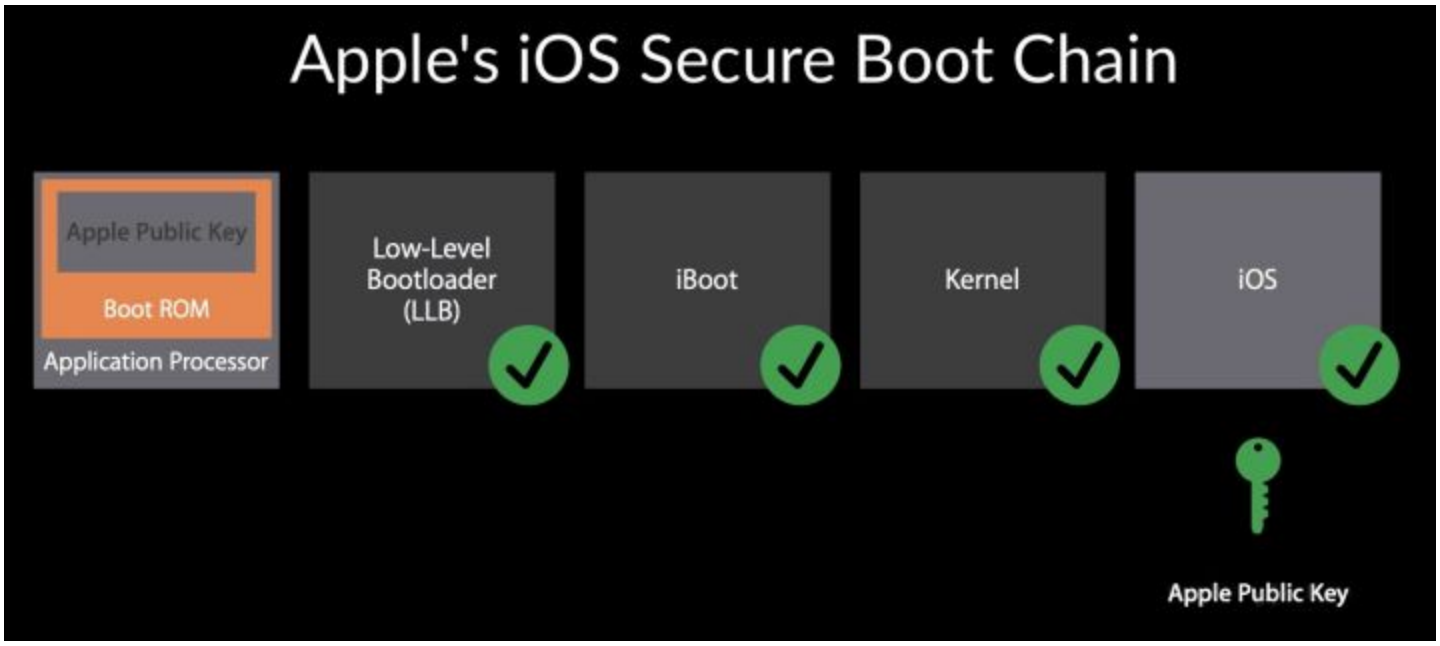
On September 27th, axi0mx tweeted...

What should end-users do?

First... not worry much about this. Apple is definitely NOT happy whereas researchers and hackers are dancing a jig.

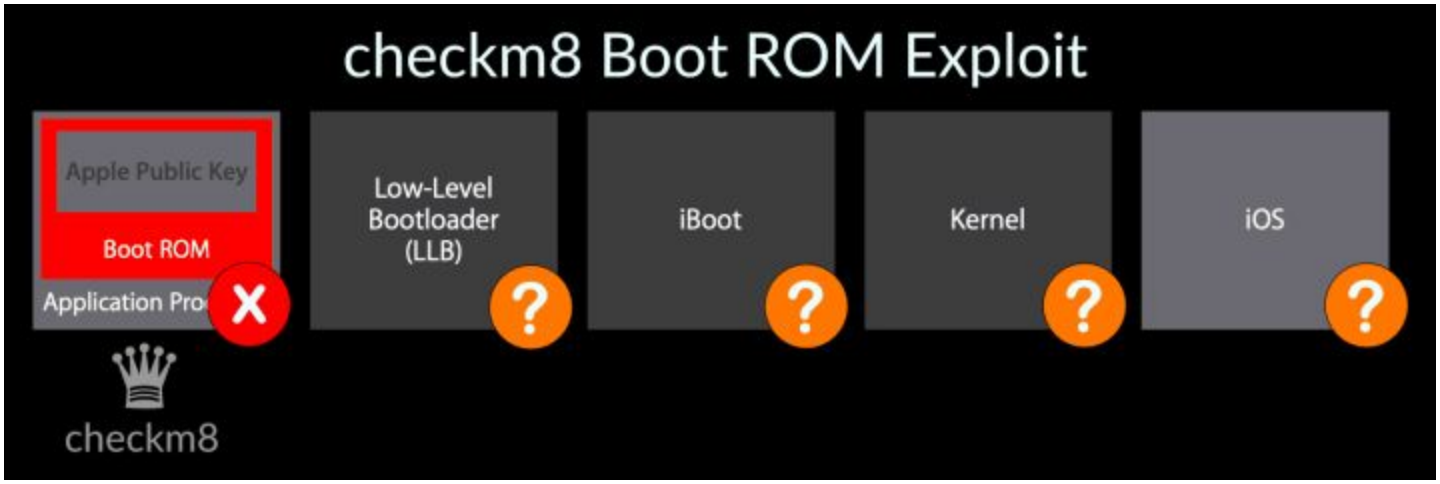
But, that said, if a paranoid person (or perhaps someone who might be explicitly targeted) wants some takeaways, the only risk is if an affected device is outside of one's presence and control. In such a case it would be possible for the phone to be jailbroken and for TRANSIENT surveillance malware to be loaded into RAM. So... if you've left your iPhone unattended and powered-on in your hotel room, for example, or on a desk in a shared office environment, or had it temporarily confiscated by border security guards, you might consider rebooting the iOS device once it's back in your possession. And for good measure, you should probably do a force restart to ensure that malware hasn't found a way of simulating a fake reboot.

We've previously discussed the concept of secure boot chains. This graphic from Apple's 2016 WWDC presentation shows the flow of the secure boot chain from power on, from left to right, on an uncompromised device.



According to the iOS Security Guide: "Each step of the startup process contains components that are cryptographically signed by Apple to ensure integrity and that proceed only after verifying the chain of trust…This secure boot chain helps ensure that the lowest levels of software aren't tampered with."

What makes checkm8 so devastating is that it exploits a flaw that exists at the root of this process and it therefore undermines ALL subsequent checks made by subsequent steps in the chain.



So what does this mean for iOS Security?

It's TRULY a big deal. Though it has little immediate impact for most users, this exploit really is a game changer for Apple researchers and hackers because this exploit IS UTTERLY UNPATCHABLE on any A11 and earlier devices. It CANNOT BE FIXED. The Boot ROM really is a ROM... and there's a bug in it. So now **anyone** will **always** be able to jailbreak **any** of these Apple-supported devices to dump and fully and deeply inspect Apple's proprietary code... which they have desperately worked to keep away from prying eyes. Those days are truly over.

And who knows what will be found? This also applies to any and all future updates to Apple's code moving forward, so long as the most recent A11 devices are supported with updates. It will now be much easier for researchers and attackers to reverse-engineer any changes Apple makes when patching vulnerabilities... to rush exploits into the wild before devices are updated.

Note that this also means that researchers will not need to depend upon Apple’s generosity in handing out special “research” phones to a select few hand-picked researchers who wish to explore iOS for bugs and security flaws. The iOS Security Research Device program was slated to begin next year in 2020. But that now appears to be effectively redundant.

As a result of checkm8, there will be a massive increase in the number of people actively investigating iOS security -- for better or for worse. Checkm8 brings the inner workings of iOS into the light for inspection by anyone, not just a handful of chosen researchers.

The Boot ROM exploit was well named.