Security News Digest
December 19, 2017

Take some time to relax and enjoy the 'Online Shopping Safety' Quiz

This is the final edition of the Security News Digest for 2017!
To all of our Readers: thank you for your continued interest in information security and privacy awareness and education.

Have a Safe and Secure Holiday Season!!
Merry Christmas and Happy New Year!

The Future is Meow: How the Ethereum Blockchain became Overrun with Virtual Cats

https://www.theglobeandmail.com/report-on-business/the-future-is-meow-how-the-ethereum-blockchain-became-overrun-with-virtual-cats/article37376359/

It's the latest twist in the cryptomania saga. **In recent weeks, 160,000 users have spent an estimated $15.5-million (U.S.) worth of cryptocurrency on collectible virtual kittens.** Vancouver-based start-up Axiom Zen launched CryptoKitties – a virtual game that allows users to buy, sell and breed digital cats – in a bid to make blockchain technology less intimidating. After all, anyone who has purchased cryptocurrency such as bitcoin knows that it can be a daunting task. Although the blockchain-based app is intended to be a game, some users may be buying the collectibles with the hopes that the digital cats will appreciate in value, much like the price of many cryptocurrencies has.

The price of bitcoin has been on a tear, rising more than 1,500 per cent since the start of the year. Meanwhile, the market for new virtual currencies has exploded, with early-stage companies raising roughly $3.68-billion through more than 230 new offerings, according to initial-coin-offering tracker Coinschedule. The hype surrounding cryptocurrencies and their underlying blockchain technology has caused a number of critics to sound the bubble alarm.

CryptoKitties is the latest digital sensation to benefit from the growing popularity of cryptocurrencies. In fact, the game has become so wildly popular that it caused a number of delays on the Ethereum network that hosts it – much to the dismay of users of other Ethereum-based apps. Ethereum is a software platform based on blockchain technology that allows developers to create decentralized applications.

At one point, CryptoKitties accounted for roughly 20 per cent of the traffic on the Ethereum network, according to Axiom Zen's founder and chief executive officer, Roham Gharegozlou. Since then, a number of improvements have been made to both the game and the underlying Ethereum platform to get things moving again, Mr. Gharegozlou added.

"We had to do a lot of apologizing, but at the end of the day, it's better for the [Ethereum] network to be tested under real conditions, so that we can improve its utility," he said. Mr. Gharegozlou said CryptoKitties was created to help users understand the benefits that decentralized networks can provide.

"Every time we talk to our friends and our families and try to explain why bitcoin matters and why blockchain matters, their eyes glaze over," Mr. Gharegozlou said. "So we were thinking about the best way to really demonstrate it and make people viscerally feel the value that blockchain can provide to them, and we decided games and collectibles was the most natural choice. If you look at the history of computing, games really drive the adoption of every new platform."

CryptoKitties is centred around collectible digital cats, each one of them unique and possessing its own digital genome. **The so-called "cryptocollectibles" are priced in ether, a form of digital currency used across the Ethereum platform, and transactions are recorded in an unalterable digital ledger. The cost of each CryptoKitty varies, with average coming in at around $91, although a handful have sold for north of $100,000**. Users can also breed CryptoKitties together, with an algorithm

dictating the new kitten's genome and determining its appearance. "If you want an all-white cat, you can breed towards it by selecting cats that look white," Mr. Gharegozlou said.
Toronto resident Kale Parsons owns four CryptoKitties – two that he purchased for a small amount of money and two that he created through breeding. Mr. Parsons stumbled upon the game with a friend and bought the cats mostly as a joke. "We just thought it was hilarious that people were buying digital cats for thousands of dollars," he said. But he soon discovered that doing anything with the cats – even selling them – triggers a fee. "I'm kind of embarrassed that I ever got into it," Mr. Parsons said.
Although CryptoKitties is meant to be a lighthearted introduction to the cryptocurrency space, Mr. Gharegozlou says the game also demonstrates how blockchain technology can be used to record ownership of unique assets such as real estate, art and inventory. **Why did they settle on cats rather than some other virtual animal? "We kept making the joke that cats are the rocket fuel of the internet," Mr. Gharegozlou said. "So for any new platform, you just have to add kitties to it."**

GIVEN THE IMPORTANCE OF NET NEUTRALITY, AND THE U.S. FCC VOTE TO REPEAL NET NEUTRALITY, THE FOLLOWING THREE ARTICLES ARE DEVOTED TO THIS ISSUE, AND ITS POTENTIAL IMPACT FOR CANADIANS.

FCC Repeals Net Neutrality, Eliminating Rules Aimed at an Open Internet Within U.S.

http://business.financialpost.com/technology/fcc-repeals-net-neutrality-rules-eliminating-open-internet-within-u-s
The U.S. Federal Communications Commission voted along party lines on Thursday to repeal landmark 2015 rules aimed at ensuring a free and open internet, setting up a court fight over a move that could recast the digital landscape. The approval of FCC Chairman Ajit Pai's proposal marks a victory for internet service providers like AT&T Inc, Comcast Corp and Verizon Communications Inc and hands them power over what content consumers can access.
Democrats, Hollywood and companies like Google parent Alphabet Inc and Facebook Inc had urged Pai, a Republican appointed by U.S. President Donald Trump, to keep the Obama-era **rules barring service providers from blocking, slowing access to or charging more for certain content**. Consumer advocates and trade groups representing content providers have planned a legal challenge aimed at preserving those rules. The meeting was evacuated before the vote for about 10 minutes due to an unspecified security threat, and resumed after sniffer dogs checked the room.
FCC Commissioner Mignon Clyburn, a Democrat, said in the run-up to the vote that Republicans were "handing the keys to the internet" to a "handful of multi-billion dollar corporations." Pai has argued that the 2015 rules were heavy handed and stifled competition and innovation among service providers. "The internet wasn't broken in 2015. We weren't living in a digital dystopia. To the contrary, the internet is perhaps the one thing in American society we can all agree has been a stunning success," he said on Thursday. The FCC voted 3-2 to repeal the rules.
Consumers are unlikely to see immediate changes resulting from the rule change, but smaller start-ups worry the lack of restrictions could drive up costs or lead to their content being blocked. Internet service providers say they will not block or throttle legal content but that they may engage in paid prioritization. They say consumers will see no change and argue that the largely unregulated internet functioned well in the two decades before the 2015 order.
Canada remains a staunch advocate for net neutrality. Unlike its neighbour, federal regulators have always applied common carriage rules to the internet. The Canadian Radio-television and Telecommunications strengthened net neutrality principles earlier this year in a decision that mandated all data be treated equally. Net neutrality has political support from the Liberal government.

An hour after the FCC's repeal, Canadian Heritage Minister Mélanie Joly reiterated Canada's commitment to net neutrality. "We will continue to promote a diversity of voices on the internet," she wrote on Twitter.

Why Canada Firmly Supports Net Neutrality - But It May Not Matter Anyway 

http://business.financialpost.com/telecom/why-canada-firmly-supports-net-neutrality-but-it-may-not-matter-anyway

A telephone network owner can't block the line if they don't like what you're about to say before placing a call across an old copper wire. This principle, called common carriage, is enshrined in telephone services as well as in railroads, airlines and, in countries such as Canada, the internet. **It's the backbone of net neutrality: the idea that all content should be equally treated when it comes to transmission speeds or access. Canada's net neutrality regulations are among the world's strongest** and the federal government has said it plans to keep them that way. But that's about to get harder, experts say, since the United States is preparing to rescind the internet's common carrier status down south.

…. Canada is "very firm about upholding these values no matter what other jurisdictions decide," said Innovation, Science and Economic Development Minister Navdeep Bains. "This is a critical issue of our time, like freedom of the press and freedom of expression centuries ago. I firmly support the basic principles of the internet around openness, fairness and freedom." The government, he added, will look for ways to strengthen net neutrality provisions when it revamps the broadcasting and telecommunications acts and will commit to being an international leader in advocating for an open internet.

…. But even if Canadian rules stay the same, Thomas Kunz, a systems and computer engineering professor at Carleton University in Ottawa, said **killing net neutrality in the U.S. could hurt web users in this country since many of the services they use are based in the U.S. and internet traffic often traverses the border to deliver content from servers**. "It might be that traffic doesn't get shaped in Canada itself," he said. "If it's slow or fast somewhere else, you'll benefit from that." Fees could also go up if telecoms are successful in getting, say, Netflix to pay more for a fast lane, Kunz said. Critically, it could make it harder for innovators if telecoms incent customers to use their own products. "Telcos aren't the most innovative … they haven't been able to successfully fight back against Facebook messenger or WhatsApp," he said, noting how the free apps beat short message service (SMS) offerings and trounced texting as popular means of communication.

The potential to limit innovation has a made-in-Canada example, said Byron Holland, president of the Canadian Internet Registration Authority. He said Netflix's growth may have been stunted without net neutrality since Rogers and Shaw Communications Inc. could have made it more difficult to access it in favour of Shomi, the inferior streaming service they co-owned. Instead, Shomi was shuttered in 2016. "If you own content, but there's a better one out there, all you have to do is slow it down a bit," Holland said. There will be a huge pressure to do the same thing in Canada. Such preferential treatment could have consequences in industries such as financial services or online stock trading. "All it takes is slowing a transaction down … literally seconds, all of a sudden, gives great preference to one platform versus another," he said. "The sky's the limit in terms of how incumbents, large operators, major players can then tweak the system to limit competition."

It costs billions to build networks and providers rightly charge for access, Holland said, but **there's a difference between paying a network owner for access and paying a gatekeeper to select content**. The internet began with walled gardens set up by providers such as AOL that limited who could participate and what content was available. "Do we want to go to a world like that?" Holland said. "Just because we have the internet today doesn't mean we'll get to enjoy that internet tomorrow. Net neutrality is one of the key foundational pillars of the internet as we know it."

Team Internet Is Far From Done: What's Next For Net Neutrality and How You Can Help

https://www.eff.org/deeplinks/2017/12/team-internet-far-done-whats-next-net-neutrality-and-how-you-can-help

About the Electronic Frontier Foundation: The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows.

For Security News Digest readers concerned about the repeal of Net Neutrality in the U.S., which has implications for Canada, here is the introduction to this article:

Defying the facts, the law, and the will of millions of Americans, the Federal Communications Commission has voted to repeal net neutrality protections. It's difficult to understate how radical the FCC's decision was. The Internet has operated under formal and informal net neutrality principles for years. For the first time, the FCC has not only abdicated its role in enforcing those principles, it has rejected them altogether. Here's the good news: the fight is far from over, and Team Internet has plenty of paths forward. [Go to the article to learn more.]

Too Many People Are Still Using 'Password' as a Password

https://motherboard.vice.com/en_us/article/paqd4m/too-many-people-are-still-using-password-as-a-password

For the seventh year in a row, password management security company SplashData has scraped password dumps to find the year's worst passwords. **This year's research was drawn from over five million leaked passwords, not including those on adult sites or from the massive Yahoo email breach**. The passwords were mostly held by users in North America and Western Europe.

SplashData estimates that nearly 10 percent of people have used at least one of the 25 worst passwords on this year's list, and almost 3 percent used the worst password, '123456'. 'Password' was the second most popular password.

Other numeric passwords that weren't new to the list were '12345678' in third place, '12345' at number five, and '1234567' in seventh place. But there were some new, more creative (or, you know, not) variations: '123456789' (in sixth place), and '123123' in 17th. Additional repeat offenders include a handful of very obvious words: 'qwerty,' 'football,' ''admin,' 'welcome,' 'login,' 'abc123,' 'dragon,' 'passw0rd,' and 'master.' But there were some new passwords on the top 25 list this year, including 'letmein,' 'iloveyou,' 'monkey,' 'starwars,' 'hello,' 'freedom,' 'whatever,' 'qazwsx' (from the two left columns on a standard keyboard), and 'trustno1.' The new passwords replaced 2016's '123456790,' 'princess,' '1234,' 'solo,' '121212,' 'flower,' 'sunshine,' 'hottie,' 'loveme,' 'zaq1zaq1,' and 'password1.'

Many people wrongly assume that adding a zero instead of the letter O will make their passwords more secure, but, as SplashData CEO Morgan Slain is quick to point out in a press release, **"hackers know your tricks, and merely tweaking an easily guessable password does not make it secure."**

Additionally, Slain points out that attackers are quick to use common pop culture terms to break into accounts online, in case you thought you were the only *Star Wars* fan.

Password advice hasn't changed any more than people's proclivity for horrible reused passwords, but here's a quick refresher: think complex pass *phrases* rather than simple pass *words*, and **create unique passwords for every account. Reusing passwords on multiple accounts leaves *all* of them vulnerable: if one account is compromised, attackers can test out that password on all of your other accounts**. Memorizing unique passwords for dozens of accounts ain't easy, though, so storing passwords in a password manager will let the tech do the heavy lifting. It won't just make you more secure, it will simplify your life as the manager can fill password forms for you. *[and hey, at home, write them down and hide the list – what are the odds someone will break into your home and find it??]*

…. In addition to using a good passphrase (whether that's a ≥12-character passphrase with various symbols, letters, and numbers or a seven-word diceware phrase), setting up two-factor authentication on your email accounts is a good idea. 2FA will add an extra layer of security by asking for a second factor in addition to a username and password to prove your identity.

Dune! Game App Leaking Sensitive Data of Millions of Android Users

https://www.hackread.com/dune-game-app-on-play-store-leaks-user-data/

Last week HackRead exclusively reported how a Fidget more spin app on Play Store is sending other apps data on an Android device to a server based in China. Now, security firms Pradeo's researchers have identified that a popular game app on Play Store is performing quite a few unfavorable functions than what it is supposed to be.

According to their findings, the app called Dune! is actually plagued with a number of OWASP flaws and is constantly leaking sensitive data. It is also claimed that Dune! can facilitate the execution of denial of service attacks and can also perform data corruption. **It is rather unfortunate that Dune! has been downloaded 5 to 10 million times only in the past few weeks and currently is it listed in the Top Apps category of the Play Store**. The app can leak critical private data including country code, device manufacturer, server provider, device's commercial name, type of telephone network, battery level, device model number and operating system. Furthermore, **it can also geolocate the device user**

although it is a gaming app and this sort of functionality is not required for the execution of the game.
It was noted that **the stolen data is sent to 32 servers** and due to the presence of 11 OWASP vulnerabilities including those that provide permission to other apps for bypassing security access, it is possible for third parties to collect sensitive data. Moreover, the app contains an excessively high number of external libraries and half of them are enabled with the capability of tracking users and obtaining as much information as possible.
In their official blog post, the researchers wrote that the app has 20 libraries, which is an above average number, and these libraries silently connect the device to unknown servers and perform data leakage. Then there are the Broadcast-Service and Broadcast-Receiver vulnerabilities that also allow data leakage and denial of service attack to be executed. Also present is the URL canonicalization vulnerability that eventually paves way for directory traversal vulnerability and the X.509Trustmanager bug allows an attacker to access and read transmitted data as well as modify it on HTTPS connection.
It is evident that this app can be really dangerous for users especially government employees because sensitive data will be leaked without the knowledge of the user. An attacker can easily get to know the exact location of the user and use the information while performing other attacks.

Mozilla Backpedals After Mr. Robot-Firefox Misstep

https://www.cnet.com/news/mozilla-backpedals-after-mr-robot-firefox-misstep/

It sounded like a good idea at Mozilla - promote computer security and privacy awareness using a tie-in with an online game from the popular Mr. Robot hacker TV series. But almost immediately, the plan started backfiring. On Wednesday, Firefox users started complaining that a cryptic extension had been installed in their browser with no explicit permission or explanation of what it does - only a description that read "MY REALITY IS DIFFERENT THAN YOURS." People ripped into Mozilla in a Reddit discussion after one Firefox user fretted, "I have no idea what it is or where it came from. I freaked out a bit and uninstalled it immediately."
Mozilla had installed the Looking Glass extension remotely on their machines this week through a partnership with Mr. Robot, but it stopped doing so when people started giving them an earful, the nonprofit organization said. "Suffice to say, we've learned a good deal in the last 24 hours ... Although we always have the best intentions, not everything that we try works as we want," said Jascha Kaykas-Wolff, Mozilla's chief marketing officer. "Within hours of receiving feedback," Mozilla moved Looking Glass to its Firefox add-on store, where people will be able to get it if they want it as it becomes available this weekend.
The issue shows just how much control outside organizations have over our computing hardware and software - even well-meaning organizations devoted to online privacy and to making us all "empowered, safe and independent." "Mozilla should have known better," said computer security and privacy researcher Bruce Schneier.
Like Apple's U2 moment. Schneier likened the situation to Apple sending iPhone users U2 music [in 2014] even if they hadn't asked for it and Amazon remotely removing a copy of George Orwell's "1984" [in 2009] from people's Kindle e-book readers. "These companies have control, and you don't," Schneier said. "They can do things against your interest all the time."
To check to see if you got the extension, type "about:addons" into Firefox's address bar; then click "extensions" on the left side of the page. If "Looking Glass" is there, you can click the "remove" button.
The faux pas comes at a bad time. With its new Quantum version of Firefox years in the making and released a month ago, Mozilla is trying to win back users from Chrome with faster performance and software that's designed to benefit you, not a powerful corporation. It's also jabbing Google with an ad campaign that says, "Big browser is watching you." Mozilla is trying to get people to use Firefox to protect their privacy, taking a potshot at Google Chrome in [this] ad on Facebook. But the Mr. Robot extension damaged trust for some.
….To install the extension, Mozilla had used a tool that lets it test Firefox features. Several on the Reddit discussion said they're disabling that ability, another sign of damaged trust. … **Mozilla distributed the extension only to people in the United States, the organization said, adding that it checked the extension to make sure it didn't collect any user data**. Mozilla wasn't paid for the Mr. Robot tie-in, Kaykas-Wolff said. "We've enjoyed a growing partnership with the show and the show's audience," he said. The extension was part of a Mr. Robot alternate-reality game that offers players clues and puzzles.

"We've found the audience of the show and our users have many points of alignment. This was not a paid promotion but rather a collaboration that was intended to be fun."

Chinese Woman Unlocks Colleague's iPhone X through Face ID

https://www.hackread.com/chinese-woman-unlocks-colleague-iphonex-using-face-id/

Like other Apple devices, iPhone X is also a sleek product that is equipped with Face ID facial recognition system. Upon its launch, the company claimed its Face ID is so secure that even high-quality masks such as those used in Hollywood movies couldn't trick its security system. But then, we witnessed Face ID system getting breached with a messed up looking mask, and a kid using his face to unlock mom's iPhone X with Face ID. Now, iPhone X and its Face ID is back in the news for yet another wrong reason. According to *Jiangsu Broadcasting Corp,* Apple Store in China was left with no option but to issue two refunds to a Chinese woman after she complained that her colleague was able to unlock her iPhone through Face ID facial recognition system.

The woman who has been identified by her last name Yan first contacted Apple when her colleague unlocked her iPhone using her face even though the Face ID was configured and activated by Yan for herself. Initially, store employees refused to believe Yan's story and stated it was "impossible", but when she along with her friend went to the store and demonstrated the issue Yan got a refund while the store claimed it might be some issue with the camera. *South China Morning Post* reports that Yan then bought another iPhone X and it turned out her colleague was able to unlock the device once again, prompting the shop to offer another refund.

At the time of publishing this article, there was no official statement by Apple however it told HuffPost it is possible that "both women may have used the phone during its "passcode training" and that the phones may have been essentially "taught" to recognize both faces." Whether it was during "passcode training" or otherwise it is quite a glitch and it is time for Apple to either secure its Face ID feature or come up with a proper explanation.

User 'Gross Negligence' Leaves Hundreds of Lexmark Printers Open to Attack

https://threatpost.com/user-gross-negligence-leaves-hundreds-of-lexmark-printers-open-to-attack/129187/

Researchers at NewSky Security have found hundreds of Lexmark printers misconfigured, open to the public internet and easily accessible to anyone interested in taking control of targeted devices. Researchers identified 1,123 Lexmark printers traced back to businesses, universities and in some cases U.S. government offices. Adversaries with access to those printers can perform a number of different malicious activities ranging from adding a backdoor to capturing print jobs, taking a printer offline or printing junk content to physically disrupt a printer's operation.

Vulnerable Lexmark printers identified by researchers, using a custom Shodan search technique, lacked an administrative password. "We focus on printers which can be controlled by anyone without hacking skills because of gross negligence of the users," said Ankit Anubhav, researcher with NewSky Security in an interview with Threatpost.

Attacks on printers are far from new and have ranged from cross-site printing attacks, RAW printing on port 9100 or exploiting known printer IP addresses for networked devices. For its investigation, NewSky Security focused on printers with no security. "While many people have awareness to change router passwords, **printer security is still neglected at large**. On similar lines, we observed that more than a thousand Lexmark printers are up for grabs for attackers, because they simply have no password," according to NewSky Security that published its findings Monday.

Nigerian Man Jailed for Role in Global Email Scams

https://www.theguardian.com/world/2017/dec/15/nigerian-man-jailed-for-role-in-global-email-scams

A Nigerian man has been sentenced to three years and five months in prison by a US judge after he pleaded guilty to taking part in email scams to defraud thousands of victims around the world of millions of dollars, US prosecutors said. David Chukwuneke Adindu, 30, was sentenced by District Judge Paul Crotty in Manhattan.

Prosecutors said in a court filing on Tuesday that Adindu tricked victims into wiring more than $25m into bank accounts he opened in China, where they said the funds would be difficult for victims in the United States to recover. Gary Conroy, a lawyer for Adindu, said the Nigerian's role consisted mostly of setting up bank accounts in China and Hong Kong. He noted that the sentence was substantially less than the

97 to 121 months called for by federal guidelines. “I think the judge accurately assessed his relatively minor role in this conspiracy,” Conroy said.

Adindu defrauded his victims by impersonating executives or vendors of companies, prosecutors said, directing employees of those companies to make large wire transfers. Such scams are known as “business email compromise”. Prosecutors said in Tuesday’s court submission that the FBI had found that business email compromise scammers often used Chinese bank accounts. Adindu was arrested at a Houston airport in 2016. Prosecutors said in an indictment that Adindu, who during the period in question resided in both Guangzhou, China, and Lagos, Nigeria, worked with others to carry out business email compromise scams from 2014 to 2016.

Prosecutors said the scammers’ targets included an unnamed New York investment firm, where an employee received an email claiming in June 2015 to be from an investment adviser at another firm asking for a $25,200 wire transfer. The employee later learned the email was not actually sent by that adviser and as a result did not comply with a second wire transfer request for $75,100, according to the indictment.

Most of us have devices equipped with Bluetooth. With Christmas and Hanukkah gift-giving, and the need/desire to have the latest gadgets, many people will be bringing Internet of Things devices, and Bluetooth devices, into their homes and lives. If this includes you – then you need to know about BlueBorne!

BlueBorne Attack Highlights Flaws in Linux, IoT Security

http://www.darkreading.com/iot/blueborne-attack-highlights-flaws-in-linux-iot-security/d/d-id/1330649

Bluetooth vulnerabilities let attackers control devices running Linux or any OS (operating system) derived from it, putting much of the Internet of Things at risk, including popular consumer products.

Popular consumer "smart" products, including Amazon Echo, Google Home, and Samsung's Gear S3, are dangerously exposed to airborne cyberattacks conducted via Bluetooth. Researchers at IoT security firm Armis earlier this year discovered **BlueBorne, a new group of airborne attacks**. The vulnerabilities let attackers take full control of any device running Linux, or OS derived from Linux, putting the majority of IoT devices at risk of exposure. The researchers discussed and demonstrated their latest findings at Black Hat Europe 2017, held last week in London.

Vulnerabilities in the Bluetooth stack have been overlooked for the past decade, they explained. Bluetooth, often perceived as peripheral, could benefit attackers if they successfully break into a high-privilege device. As the researchers demonstrated, **one compromised product can spread its attack over the air to other devices within Bluetooth range. "These attacks don't require any user interaction or any authentication,"** said Armis head researcher Ben Seri in their presentation. Armis **experts found 5.3 billion devices at risk and eight vulnerabilities, four of which were classified as critical. These flaws enable attackers to bypass and break into a device without its owner knowing what happened, he explained.**

Each vulnerability across the Bluetooth stack is "a testament to the fact that no specific part is vulnerable, but Bluetooth implementations have not been audited enough," he continued. In general, these implementations are complex and unexamined. Bluetooth has a large attack surface, Armis researcher Gregory Vishnepolsky said. **When Bluetooth is enabled, a device may not be discoverable but it is always listening for incoming connections. Hackers don't need a device to be discoverable in order to break in, he noted**. *[security best practice – if you are not using Bluetooth for your device, even an iPod Touch, go to Settings and disable it because it is usually on by default – you can turn it on again if needed.]*

Bluetooth devices transmit parts of their MAC addresses over the air. If an attacker is close enough to sniff radio between two communicating Bluetooth devices, they can get 80% of the address from a single packet and brute-force the rest. Open-source hardware tools can do this for as little as $100, he said. Attackers put these devices on networks to listen for packets.

Many OEMs use adjacent MAC addresses for Wi-Fi and Bluetooth. Wi-Fi monitor mode detects nearby Bluetooth devices. Seri explained how L2CAP, the Bluetooth equivalent of TCP, is implemented in the kernel. Connecting to an open port doesn't require authentication, and further, many obscure quality of service features increase the amount of code - and as a result, the attack surface.

To illustrate the vulnerability of Bluetooth, the researchers presented examples of everyday devices that can be compromised. One was the Amazon Echo, which is not equipped with expected stack overflow

mitigations KASLR, stack canaries, Fortify_source, NX Bit, or Access Control. With no NX Bit, for example, an attacker can just jump to the shell code in the stack and overflow it.
The researchers did a live demo in which they hacked a Samsung S3 Gear smartwatch, which over Bluetooth hacked a Google Home, which used a Bluetooth connection to break into the Amazon Echo. "No security mechanisms today are actually looking at Bluetooth communications or non-Wi-Fi protocols," they explained. "This needs to be fixed."

5 Computer Security Facts that Surprise Most People

https://www.csoonline.com/article/3239644/data-breach/5-computer-security-facts-that-surprise-most-people.html
[By Roger A. Grimes, Columnist, CSO] The five statements below are the causes behind a lot of computer security risk and exploits. If you understand them well enough today, you will be ahead of your peers.
1. Every company is hacked. When the world hears about the latest big breach, people probably think that the company involved must be bad at computer security. The next time a big hack occurs that results in millions of customer records stolen or millions of dollars in losses, what you should think is "Every company is hacked. This is just the one the media is talking about today."
Every company is completely and utterly owned by a nefarious hacker or easily could be. That's just a fact. I'm not including top secret military installations that don't have Internet and require that their hard drives be placed in a locked safe at the end of every day. I'm talking about the average corporate company or small business. I've never consulted at a company (and I've consulted at hundreds) where I didn't find at least one hacker hidden somewhere when asked to do so. In most cases, especially over the last decade, I found multiple groups that had been in for years. My personal record was eight different hacking groups, with some in as long as ten years. That one was interesting because one of the reasons they called me was that a software patch that they didn't want applied was applying no matter what they did. The hacker groups were tired of waiting for the victim company to make its environment more secure, because more and more hacking groups kept breaking in. It's a problem when the hackers are more security conscious than you are.
As a part-time penetration tester, I've often been asked to break into companies (after getting legitimate authority). It's never taken me more than an hour to do so, except for one company that took me three hours, and then only because they had already followed my advice after my previous paid break in. I'm only an average penetration tester. The people I admire get in even faster. I'm not even including all the world's nation-states, which are sitting on tons of zero days.
The world's computers are very poorly secured. You don't need zero day exploits. You just need to look around a bit to find an easy weakness. Most companies aren't doing nearly enough to secure their computers. Most talk a good game, but when it comes to really doing what's needed to keep good hackers out (e.g., perfect patching, application control programs, and no Internet), they aren't willing to do what needs to be done - at least not yet.
2. Most companies don't know the way they are successfully attacked the most. This is something I've only learned, and tested, in the last five years. I've yet to meet an IT security employee who can tell me the number one way their company is exploited the most on a routine basis. Well, that's not fair. Five to 20 percent of the employees guess the right answer, but can't point to any data to back up the claim. That means 80 percent at best of the IT security staff thinks it's something else. The rest of IT and the rest of the company is clueless. If most of the company doesn't agree on what the biggest threat is, how can they effectively fight it? The data to show the biggest threat is non-existent. You would think after spending millions of dollars to collect bazillions of events into fancy event log management systems that this question would be the easiest to answer. It's not. It might never be, especially if you aren't even asking the question.
3. A criticality gulf exists between real and perceived threats. There is a huge gulf between your biggest potential threats and your biggest actual exploits. Security defenders who understand the difference are worth their weight in gold. Each year 5,000 to 7,000 different new exploits appear. (This has been fairly consistent for over a decade.) One-fourth to one-third of them are marked with the highest criticality. This means when you run vulnerability scanning software or look at a patch management report, you'll always have a ton of "top priority" things to fix. You can't concentrate and fix more than a few things at once. So, if your report has 20 number-one priorities you need to correct, what do you do?
Start by fixing the critical things that are causing the most damage in your environment today, followed by the most likely culprits after that. It could be that the top culprits aren't even the highest ranked

vulnerabilities. Doesn't matter. Criticality rankings are done on potential to do harm. Real harm, and most likely future harm, trumps guesses. Understanding this lesson should change a lot of what you do as a computer security defender.

4. Firewalls and antivirus software aren't that important. Most of today's threats are client-side threats, initiated by the end-user. This means they are already past all the firewalls (e.g., network or host) that were put in their way to prevent them from reaching the user's desktop. Once a threat is there, firewalls provide very little value.

A traditional firewall's main value is preventing an unauthorized connection attempt to an existing vulnerable service. If your service isn't vulnerable, then a firewall probably isn't providing a lot of value. This is not to say that they don't provide any value. They can and do, especially intelligent, deep-packet inspecting firewalls. It's just that most threats aren't the things they stop anymore, so the big value they used to provide just isn't there.

Antivirus software isn't valuable because it's very difficult for any AV product to be 100 percent effective against all the newly emerging malware. Anytime you see a "100 percent" rating, don't believe it. Those tests are conducted under controlled conditions where the malware is not getting updated nearly as much as in the real world. In the real world, the first malware program you are likely to encounter is simply a downloader that downloads brand new malware programs, updated to bypass all AV software.

5. Two problems are almost 100 percent of the risk. It's been true for over a decade that the two most likely reasons you will get exploited is due to unpatched software or a social engineering event where someone is tricked into installing something they shouldn't. These two issues account for nearly 100 percent of the risk. It would be a stretch to claim every other exploit type in the world, added together, would account for 1 percent of the risk. **Put another way, if you don't fix the two top problems, then the rest do not matter. A single unpatched software program has at times accounted for over 90 percent of the web-based exploits. Social engineering gobbles up most of the rest. Make sure you concentrate on the right problems!**

Twitter Suspends Britain First Account that Trump Retweeted

http://money.cnn.com/2017/12/18/technology/twitter-britain-first-jaydabf/index.html

Twitter has suspended at least three accounts tied to far-right group Britain First, including one that had been retweeted by President Trump. Trump retweeted three inflammatory videos posted by Britain First deputy leader Jayda Fransen in November, setting off a political firestorm that strained relations between London and Washington. Her verified account was suspended on Monday, along with that of Britain First leader Paul Golding, and the group's main account, @BritainFirstHQ.

Asked why the accounts had been suspended, Twitter said it would not comment on individual accounts for privacy and security reasons. **But the social media firm did publish a blog post on Monday saying that it would start enforcing rule updates that are designed to reduce "hateful and abusive" content**. The policies prohibit accounts that "affiliate with organizations that use or promote violence against civilians to further their causes." They also ban content that "glorifies violence or the perpetrators of a violent act." Representatives from Britain First could not immediately be reached for comment.

Currency-Mining Android Malware is So Aggressive It Can Physically Harm Phones

https://arstechnica.com/information-technology/2017/12/currency-mining-android-malware-is-so-aggressive-it-can-physically-harm-phones/

A newly discovered piece of Android malware carries out a litany of malicious activities, including showing an almost unending series of ads, participating in distributed denial-of-service attacks, sending text messages to any number, and silently subscribing to paid services. **Its biggest offense: a surreptitious cryptocurrency miner that's so aggressive it can physically damage an infected phone**. **Trojan.AndroidOS.Loapi is hidden inside apps distributed through third-party markets, browser ads, and SMS-based spam**. Researchers from antivirus provider Kaspersky Lab have dubbed it a "jack of all trades" to emphasize the breadth of nefarious things it can do. Most notably, Loapi apps contain a module that mines Monero, a newer type of digital currency that's less resource intensive than Bitcoin and most other cryptocurrencies. The module allows the malware creators to generate new coins by leaching the electricity and hardware of infected phone owners.

But the lower demands of Monero mining by no means stop Loapi from straining infected phones. Kaspersky Lab researchers tested Loapi in a lab setting. After two days, the mining caused the battery in the phone to bulge so badly it deformed the cover. The researchers provided pictures as evidence.

Drive-by currency mining on the rise. Over the past few months, a surge of sites and apps have been caught draining people's CPUs and electricity as they run resource-intensive cryptocurrency mining code. In a handful of cases, the apps or sites disclose what's happening, throttle down the mining, and ask users to participate as a form of payment. In the vast majority of cases, however, the mining is only discovered when users open monitors that track all processes or apps running on a device. On Tuesday, officials at AV provider Sophos formally labeled all cryptocurrency mining without user consent as parasitic.

Loapi is a nuisance in other ways that go beyond covert coin mining. It sends an unending barrage of prompts for users to assign it administrator permissions. Once granted permission, Loapi makes it hard for victims to install security apps that can help disinfect the phone. It can subscribe a phone to costly premium services and even covertly send codes in SMS messages to confirm the request. It allows attackers to use infected phones as foot soldiers in DDoS attacks. And it displays a constant stream of ads. **There are no indications Loapi apps have ever been available through Google Play**. "We've never seen such a 'jack of all trades' before," Kaspersky Lab researchers wrote. Later in the post, they added: "The only thing missing is user espionage, but the modular architecture of this Trojan means it's possible to add this sort of functionality at any time."

And Now, This:

Former Pentagon Official Part of Secret Project Claims Aliens Visited Earth

http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=11963001

[This very lengthy article is presented here in its entirety, for your reading enjoyment.] A former Pentagon official who led a secret government programme to combat UFO attacks says he believes aliens have visited Earth. Luis Elizondo previously ran the Advanced Aerospace Threat Identification Program, which leaked records show investigated reports of clashes with unidentified aircraft.

The former chief of the US$22 million ($31.4m) project says he thinks "we may not be alone", based on numerous reports he read on encounters with the flying craft, according to the Daily Mail. Many reportedly displayed out of this world capabilities in terms of both speed and manoeuvring. **News of the off-the-books Department of Defense (DoD) programme emerged over the weekend.** It sought to identify what had been seen, either through tools or eyewitness reports, and then "ascertain and determine if that information is a potential threat to national security". Elizondo resigned from the DoD in October in protest over what he has termed excessive secrecy and internal opposition to the project, whose funding was cut in 2012.

He has now said there is evidence which leads him to believe alien aircraft have visited the planet. Speaking to CNN, he said: "My personal belief is that there is very compelling evidence that we may not be alone. "These aircraft - we'll call them aircraft - are displaying characteristics that are not currently within the US inventory nor in any foreign inventory that we are aware of. "Things that don't have any obvious flight services, any obvious forms of propulsion, and maneuvering in ways that include extreme manoeuvrability beyond, I would submit, the healthy G-forces of a human or anything biological."

Among the sightings were reports from pilots of two US Navy Super Hornet fighters who spotted a UFO on a training mission. They were 160km from San Diego in the Pacific when a call on their radios asked if they were carrying weapons. The unusual request, that day in 2004, came from a naval cruiser, the Princeton, that had spent two weeks tracking unidentified aircraft. Commanders David Fravor and Jim Slaight had only dummy missiles, but were directed to investigate objects that appeared suddenly at an altitude of 80,000ft, then plunged towards the sea. At 20,000ft, they stopped and hovered before disappearing out of radar range or shooting up again. The pilots could see nothing at first and then Fravor looked down to the sea. The water in one place was being churned by something just below the surface. Hovering erratically 15m above that spot was some sort of flying craft, around 12m long, oval-shaped and whitish.

As the pilot descended towards it, it rose to meet him, but suddenly peeled away at an immense speed that he admits left him feeling "pretty weirded out". The craft "had no plumes, wings or rotors" but, seemingly travelling at a mile a second, easily outran America's fastest military jets. Fravor's comrades made fun of him when he described the encounter, but others in the US military, we now know, took him seriously.

For the episode was one of scores of unexplained encounters between military personnel and UFOs that were investigated by a top-secret, multimillion dollar programme run by the Pentagon. Although it was set up in 2007, the existence of the Advanced Aviation Threat Identification Programme

(AATIP) has only now emerged thanks to its former boss. Its US$22 million of funding - so-called "black money" for secretive projects - was known only to a few outsiders. UFO enthusiasts have argued for decades that the US Government has been covering up the existence of unidentified craft containing alien visitors.

The idea that a hush-hush Government outfit was investigating sightings and other bizarre phenomena famously provided the basis for TV drama series *The X-Files.* Now, it seems the cult series wasn't such a flight of fancy after all. The shadowy programme's existence was intentionally buried in the defence department's US$600 billion annual budget, as were its headquarters, deep within the labyrinthine Pentagon building. Based on the fifth floor of C Ring, the secret department has spent years investigating reports of unidentified flying objects. Although the Pentagon officially stopped funding the project in 2012, insiders told the *New York Times* it was still operating.

And, more tantalisingly, intelligence experts who ran it, and politicians who backed it, insist its research has not been fruitless. Having investigated myriad reports from US servicemen of encounters between unknown objects and military planes, they are convinced that nothing in this world can explain them. "If anyone says they have the answers now, they're fooling themselves," said Harry Reid, the US Senate Democrat leader for 12 years and the project's most powerful supporter. "We do not know." Reid, who retired recently as senator for Nevada, first directed the Pentagon to investigate the "unidentified aerial phenomena" repeatedly identified.

In each case, the servicemen were convinced that what they saw was vastly more technologically advanced than anything in US or foreign arsenals. The man who inspired this "X-Files department", Reid, had the support of two other senior senators, both members of a defence spending sub-committee, who feared a threat to national security behind these chilling sightings. Their rationale was that if the mysterious craft were not aliens, then perhaps Russia or China had developed advanced technology to threaten the West.

Reid's interest in UFOs had originally been pricked by his friend Robert Bigelow, a billionaire hotel tycoon and government contractor who is investing millions in space projects such as inflatable modules for living on the Moon. Bigelow, who became convinced extra-terrestrials exist after his grandparents said they saw a UFO, has been investigating the paranormal for decades and bought a Utah ranch known for UFO sightings in the skies above. The Pentagon UFO programme paid Bigelow's Las Vegas-based aerospace research company to do most of its work.

Reid says he was also influenced by the veteran astronaut John Glenn, who had told him years earlier that the Government should be seriously looking into UFOs and talking to military people who claimed to have seen them. Too often, their claims were not being passed up the chain of command because servicemen feared they would be ostracised. The Pentagon programme investigated scores of reported encounters - in some cases, such as Fravor's, backed by video or audio evidence. Newly released tapes make for disturbing listening. In another incident involving a US Navy Super Hornet jet chasing a UFO that emitted a "glowing aura travelling at high speed and rotating as it moves", a pilot is heard exclaiming: "There's a whole fleet of them . . . My gosh, they're all going against the wind. The wind is 120 knots to the west."

Suspiciously, sightings were often near nuclear facilities, be they ships or power plants. In many cases they involved aircraft that appeared to defy the laws of physics in their speeds and manoeuvrability. Often, they were able to move or hover with no visible means of propulsion or lift. Seeking explanations, the Pentagon focused attention on other phenomena that sound as if they've come from a sci-fi convention. They included warp drives (faster than light spacecraft propulsion), and wormholes (theoretical passages in space-time that could create shortcuts).

Researchers also analysed people claiming to have experienced physical effects from encounters. The Pentagon investigators are likely to have talked to some of the 120 retired military personnel who - according to UFO researchers - have described encounters near nuclear missile bases. Some believe aliens were monitoring them to ensure humanity didn't blow itself up by accident. They include Air Force captain Robert Salas, an intercontinental ballistic missile launch officer on duty at Malmstrom Air Force Base in Montana one night in 1967. He says he was warned by his men "screaming into the phone" that a mysterious "glowing red object" had been spotted over their missile silo, which was 18m underground. Moments later, they discovered that all 10 Minuteman missiles had been deactivated.

Robert Jamison, the base's targeting officer, confirmed the report and said he heard about a UFO landing in a "deep ravine" nearby. He said he spoke to a security guard, who described "two small red lights off at a distance" that began to close in. The guard then broke down and started crying.

More recently, the department has assessed the threat posed by UFOs and Bigelow has modified some of his company's buildings to store materials reportedly recovered from the scene of UFO sightings.
Those involved insist they made progress. In 2009, Reid wrote to then deputy defence secretary William Lynn requesting heightened security to protect the programme. "Much progress had been made with the identification of several highly sensitive, unconventional aerospace-related findings," he said. At the same time, a Pentagon briefing by Elizondo claimed that "what was considered science fiction is now science fact", says the *New York Times*.
He warned that the US was incapable of defending itself against the technologies that had been discovered, although he conceded none of the UFOs showed "overt hostility". A project insider told the website Politico, however, that the programme couldn't justify using taxpayers' money. It lost its funding. Elizondo quit in October, in protest at what he said was excessive secrecy and internal opposition to his work. But the Pentagon insisted it would act "whenever credible information is developed".
The US has investigated UFOs before, notably in 1949 when it launched a 20-year study - Project Blue Book - into more than 12,000 sightings. Although 701 were never explained, the report attributed most to people seeing conventional aircraft or spy planes, stars and clouds. Many will laugh at the US Government wasting so much time and money on them. But others think they were on to something.
The Navy pilot who says he saw that astonishing craft off San Diego, Fravor, told ABC News yesterday: "I can tell you, I think it was not from this world. I'm not crazy, haven't been drinking. After 18 years of flying, I've seen pretty much about everything I can see in that realm, and this was nothing close. "I have never seen anything in my life, in my history of flying that has the performance, the acceleration - keep in mind this thing had no wings".
And Reid is sticking to his guns. "I'm not embarrassed or ashamed or sorry I got this thing going. I've done something that no one has done before," he said. As news of his UFO secret emerged, he even borrowed *The X-Files*' famous catch-line, tweeting: "The truth is out there."