# Security Now! #587 - 11-22-16

## Mobile & IoT Nightmares

## This week on Security Now!

- This week’s Dynamic Duo: Samy Kamkar is back with a weaponized $5 RaspberryPI and "El Cheapo" Android phones bring new meaning to "Phoning it in" !!
- And another big, unrelated, Android problem.
- Watching a webcam getting taken over
- Bruce Schneier speaks to Congress about the Internet,
- A(nother) iPhone Lockscreen Bypass and another iPhone lockup link.
- Ransomware author asks a security researcher for help fixing their broken crypto.
- Britain finally passed that very extreme surveillance law,
- Some more fun miscellany… and more!

## Last Week's awful audio...

- AS8075 Microsoft Corporation / Redmond, Washington, United States
  160.699 K / 219.865 K     60.23 MiB / 83.91 MiB
- AS7738 Telemar Norte Leste S.A. / Rio de Janeiro, Rio de Janeiro, Brazil
  187-14-192-114.user.veloxzone.com.br
  5 / 5     230 B / 270 B
- AS8075 Microsoft Corporation / Washington, Virginia, United States
  1 / 1     62 B / 48 B
- AS8075 Microsoft Corporation / Chicago, Illinois, United States
  1 / 1     62 B / 48 B

## Security News

### The Horror of LessPass

- https://www.youtube.com/watch?v=sdlGy3kg2lM

- @numerodix, a listener, tweeted:
  - @guillaume20100 @SGgrc That's the first time I've seen a code review in a podcast. Pretty cool :)

- Vincent Guillaume:
  - @numerodix @SGgrc yes I'm obviously not happy with this video, but I'm glad that people are studying the code in depth.

- Discussion about the Horror of #LessPass
  The Horror of LessPass - TWiT Netcast Network
  https://github.com/lesspass/lesspass/issues/88 cc @SGgrc

- <quote>
  The interview went to says:

  - Your goal is to make your password as random as possible, so anything that reduces randomness or entropy is going to reduce the effectiveness of your password

  - Is going to increase its bruteforceability

- **Understanding our mistakes**

- We use patterns to create passwords with complex rules like no consecutive vowels or can't start with a number.

- We made two mistakes:
  - First, we did not understand at the beginning that the entropy of the generated password increase the bruteforceability of the master password. I took the idea of password templates from masterpassword algorithm. We misunderstood and took for granted what we read.
  - Then, it was to define cvCVns as template by default (consonms, vowels, etc.) instead of a more random one as x (full characters set).

- On Open Source
  And for anyone who thinks they do well at first, or who think that Open Source does not help. On the contrary, we believe that nobody does well at first, and thanks to the community scrutinity and critical studies of the code, this kind of tool becomes more robust the longer it lives.

- How It Feels
  The video is obviously a setbacks for us, especially after the euphoric past week where we went from ~100 to 1600+ stars, but we are glad that people review our code in depth and this came up early on.

- Actions
  We will use the full alphabet in the next version by default. We will probably increase the default length of generated passwords.

  So in the future, we will describe (with drawings) the future algorithm and its implementation. We will simplify the code to helps everyone understand how it works. And we hope you will keep your eyes peeled for mistakes and stay critical to the code.

**Samy Kamkar: PoisonTap - exploiting locked computers over USB.  (Last Wed, 11/16)**

- https://samy.pl/poisontap/

- The Genesis:
  - Sept 6th: Rob Fuller... "Snagging creds from locked machines"
  - <quote> First off, this is dead simple and shouldn't work, but it does. Also, there is no possible way that I'm the first one that has identified this, but here it is (trust me, I tested it so many ways to confirm it because I couldn't believe it was true)

  - TL;DR USB Ethernet + DHCP + Responder == Creds
  - https://room362.com/post/2016/snagging-creds-from-locked-machines/

- "Applied Hacking" -- PoisonTap - siphons cookies, exposes internal router & installs web backdoor on locked computers

- How PoisonTap Works:
  - PoisonTap produces a cascading effect by exploiting the existing trust in various mechanisms of a machine and network, including USB/Thunderbolt, DHCP, DNS, and HTTP, to produce a snowball effect of information exfiltration, network access and installation of semi-permanent backdoors.
  - $5 Weaponized Raspberry Pi Zero.

- Features:
  - Emulates an Ethernet device over USB (or Thunderbolt)
  - Hijacks all Internet traffic from the machine (despite being a low priority/unknown network interface)
  - Siphons and stores HTTP cookies and sessions from the web browser for the Alexa top 1,000,000 websites
  - Exposes the internal router to the attacker, making it accessible remotely via outbound WebSocket and DNS rebinding (thanks Matt Austin for rebinding idea!)
  - Installs a persistent web-based backdoor in HTTP cache for hundreds of thousands of domains and common Javascript CDN URLs, all with access to the user's cookies via cache poisoning.
  - Allows attacker to remotely force the user to make HTTP requests and proxy back responses (GET & POSTs) with the user's cookies on any backdoored domain.
  - Does not require the machine to be unlocked
  - Backdoors and remote access persist even after device is removed and attacker sashays away

- PoisonTap evades the following security mechanisms:
  - Password Protected Lock Screens
  - Routing Table priority and network interface Service Order
  - Same-Origin Policy
  - X-Frame-Options
  - HttpOnly Cookies
  - SameSite cookie attribute
  - Two-Factor/Multi-Factor Authentication (2FA/MFA)

  - DNS Pinning
  - Cross-Origin Resource Sharing (CORS)
  - HTTPS cookie protection when Secure cookie flag & HSTS not enabled

- Video Demo: https://youtu.be/Aatp5gCskvk

- Securing Against PoisonTap
  - If you are running a web server, securing against PoisonTap is simple:
  - Use HTTPS exclusively, at the very least for authentication and authenticated content
  - Honestly, you should use HTTPS exclusively and always redirect HTTP content to HTTPS, preventing a user being tricked into providing credentials or other PII over HTTP
  - Ensure Secure flag is enabled on cookies, preventing HTTPS cookies from leaking over HTTP.
  - When loading remote Javascript resources, use the Subresource Integrity script tag attribute
  - Use HSTS to prevent HTTPS downgrade attacks

- Desktop Security
  - Adding cement to your USB and Thunderbolt ports can be effective.
  - Closing your browser every time you walk away from your machine can work, but is entirely impractical.
  - Disabling USB/Thunderbolt ports is also effective, though also impractical.
  - Locking your computer has no effect as the network and USB stacks operate while the machine is locked, however, going into an encrypted sleep mode where a key is required to decrypt memory (e.g., FileVault2 + deep sleep) solves most of the issues as your browser will no longer make requests, even if woken up.

- Source code published on Github: https://github.com/samyk/poisontap

**KryptoWire discovers mobile phone firmware that transmitted personally identifiable information without user consent or disclosure.**

- (Last Tuesday, 11/15)  http://www.kryptowire.com/adups_security_analysis.html
- Kryptowire has identified several models of Android mobile devices that contained firmware that collected sensitive personal data about their users and transmitted this sensitive data to third-party servers without disclosure or the users' consent. These devices were available through major US-based online retailers (Amazon, BestBuy, for example) and included popular smartphones such as the BLU R1 HD.

- Who is KryptoWire?
  Kryptowire was jumpstarted by the Defense Advanced Research Projects Agency (DARPA) and the Department of Homeland Security (DHS S&T). Kryptowire provides mobile application security analysis tools, anti-piracy technologies, mobile app marketplace security analytics, and Enterprise Mobility Management (EMM) solutions. Kryptowire was founded in 2011, is based in Fairfax, Virginia, and has a customer base ranging from government agencies to national cable TV companies.

- These are not some obscure off-brand Android:
    - Aug 3rd: ArsTechnica: Review: A $60 Amazon phone that's way better than Amazon's actual phone.
        - http://arstechnica.com/gadgets/2016/08/review-blus-r1-hd-redefines-what-you-can-get-in-a-60-smartphone/
        - Selling your lock screen to Amazon cuts this cheap phone's price in half.

- BLU: "Bold Like Us" / R1 HD "The Rebel In You" - Starting at $49.95, exclusively on Amazon.
    - http://www.bluproducts.com/r1-hd/
    - https://www.amazon.com/BLU-R1-HD-Exclusive-Lockscreen/dp/B01F9N5QXI
    - "Currently Unavailable"

- PCMag:
    - http://www.pcmag.com/review/345824/blu-r1-hd
    - Pros:
        - Inexpensive.
        - Sturdy build.
        - Solid battery life.
        - Latest Android software.
        - Dual SIM card slots and expandable storage.

    - Cons:
        - Prime-subsidized phone includes Amazon bloatware and advertising.
        - Lackluster camera.

    - Bottom Line
        - The Blu R1 HD is an unlocked Android phone with a good balance of performance for the price, making it a fantastic value for Amazon Prime users and regular customers alike.

- Wired, in July:
    - Blu itself is easy enough to explain. It’s a smartphone company, based in Florida, that specializes in surprisingly affordable hardware that runs minimally tweaked Android firmware. As for the caveats, its R1 HD is one of two phones that are Prime Exclusives, a new program that gives Amazon Prime members steep discounts on devices in exchange for allowing ads on their lock screens, in their notifications, as well as on a suite of preinstalled Amazon apps.

- 3,202 Reviews on Amazon.

- (Continuing...) These devices actively transmitted user and device information including the full-body of text messages, contact lists, call history with full telephone numbers, unique device identifiers including the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI).

  The firmware could target specific users and text messages matching remotely defined keywords.

The firmware also collected and transmitted information about the use of applications installed on the monitored device, bypassed the Android permission model, executed remote commands with escalated (system) privileges, and was able to remotely reprogram the devices.

The firmware that shipped with the mobile devices and subsequent updates allowed for the remote installation of applications without the users' consent and, in some versions of the software, the transmission of fine-grained device location information.

The core of the monitoring activities took place using a commercial Firmware Over The Air (FOTA) update software system that was shipped with the Android devices we tested and were managed by a company named Shanghai Adups Technology Co. Ltd.

Our findings are based on both code and network analysis of the firmware. The user and device information was collected automatically and transmitted periodically without the users' consent or knowledge.

The collected information was encrypted with multiple layers of encryption and then transmitted over secure web protocols to a server located in Shanghai. This software and behavior bypasses the detection of mobile anti-virus tools because they assume that software that ships with the device is not malware and thus, it is white-listed.

In September 2016, Adups claimed on its web site to have a world-wide presence with over 700 million active users, and a market share exceeding 70% across over 150 countries and regions with offices in Shanghai, Shenzhen, Beijing, Tokyo, New Delhi, and Miami. The Adups web site also stated that it produces firmware that is integrated in more than 400 leading mobile operators, semiconductor vendors, and device manufacturers spanning from wearable and mobile devices to cars and televisions.

- KryptoWire provides a comparison to 2011's "CarrierIQ" spyware which we covered at the time.

- <quote> We analyzed the Personally Identifiable Information (PII) collected and transmitted in an encrypted format to servers in Shanghai by the bestselling unlocked smartphones sold by major online retailers.

  [They] transmitted the body of the user's text messages and call logs to a server in located in Shanghai. All of the data collection and transmission capabilities we identified were supported by two system applications that cannot be disabled by the end user. These system applications have the following package names:

  - com.adups.fota.sysoper
  - com.adups.fota

- The data collection and transmission capability is spread across different applications and files. The data transmission occurred every 72 hours for text messages and call log information, and every 24 hours for other PII data. The information was transmitted to the following back-end server domains:

  - bigdata.adups.com (primary)
  - bigdata.adsunflower.com
  - bigdata.adfuture.cn
  - bigdata.advmob.cn

- All of the above domains resolved to a common IP address: 221.228.214.101 that belongs to the Adups company. During our analysis, bigdata.adups.com was the domain that received the majority of the information whereas rebootv5.adsunflower.com with IP address: 61.160.47.15 was the domain that can issue remote commands with elevated privileges to the mobile devices.

  Before the data transmission occurs the device checks in with a remote server using a REST API and is instructed on what to collect. It is worth noting that the REST endpoint differs for various phone manufacturers and even phone models. Below is an example of a check-in response:

- They found the key in the code.  It uses DES encryption.  (Fast, simple and good enough to obscure casual analysis.)

- CONCLUSION:
  As smartphones are ubiquitous and, in many cases, a business necessity, our findings underscore the need for more transparency at every stage of the supply chain and increased consumer awareness. Kryptowire has developed tools aimed at detecting non-compliant software that can violate privacy and security policies that are not necessarily classified as malware. In many cases, these applications are benign, but exhibit behavior non-compliant with organizational, industry, and government policies.

  Kryptowire has communicated its findings with respect to the affected devices with Google, Amazon, Adups, and BLU Products, Inc.

  Consumers that believe their devices may be affected can refer to the manufacturer warranty or retailer terms of purchase for more information.

**Anubis Networks finds an Android OTA update mechanism that's very vulnerable to attack**

- http://blog.anubisnetworks.com/blog/ragentek-android-ota-update-mechanism-vulnerable-to-mitm-attack
- In this article, we will be detailing an issue we discovered affecting a number of low-cost devices. It allowed for adversaries to remotely execute commands on the devices as a privileged user if they were in a position to conduct a Man-in-the-Middle attack. The binary responsible appears to be an insecure implementation of an OTA (Over-the-air) mechanism for device updates associated to the software company, Ragentek Group, in China. All transactions from the binary to the third-party endpoint occur over an unencrypted channel, which not only exposes user-specific information during these

communications, but would allow an adversary to issue commands supported by the protocol. One of these commands allows for the execution of system commands. This issue affected devices out of the box.

On Tuesday, November 15th, the New York Times reported on an issue affecting a similar set of device manufacturers that caused the devices to report sensitive material, such as text messages and the user's previous physical locations, back to the Chinese software company Shanghai ADUPS Technology Co., Ltd. This was an issue discovered and announced by Kryptowire, and covered in more detail in a posted article on their website. The issue described in this article is unrelated to the one discovered by Kryptowire.

- Analysis
  We acquired one of the affected devices, a BLU Studio G, from Best Buy. After building a passive network traffic capturing system, an unencrypted transaction to the Ragentek head-end (oyag[.]lhzbdvm[.]com) was observed not long after proceeding through the Android first-use setup process on the device:

  The device then attempted to contact two other pre-configured domains, which were previously unregistered until AnubisNetworks acquired them. This gave us immediate visibility into the larger population of affected devices, which are detailed later in this article. We were able to associate the network transactions back to specific binaries on the device, and were the ones investigated as part of this analysis:

- Endpoints and Hosts
  This binary has been observed to cycle through three specific hosts:
    - oyag.lhzbdm.com - Domain owned by Ragentek
    - oyag.prugskh.net - AnubisNetworks sinkhole
    - oyag.prugskh.com - AnubisNetworks sinkhole

- We have observed over 2.8 million distinct devices, across roughly 55 reported device models, which have checked into our sinkholes since we registered the extraneous domains. In some cases, we have not been [able] to translate the provided device model into a reference to the real world device. These are the devices captured in the "Others" category above. Thus, there could be additional device models affected by this problem not outlined in this article or by CERT.

  Please refer to the CERT Knowledgebase reference at the end of this article for additional information about how to check whether your device is affected. To manually verify, you can monitor for outbound connections from your phone to the hostnames described earlier in the article. If the transactions occur over HTTP instead of HTTPS, then the device would be affected by this issue.

- Conclusion
  This analysis revealed two critical discoveries:
    - Firstly, the vulnerability described above allows for users to be subjected to significant attacks in positions where an adversary can perform a Man-in-the-Middle attack.
    - Secondly, this OTA binary was distributed with a set of domains preconfigured in

the software. Only one of these domains was registered at the time of the discovery of this issue. If an adversary had noticed this, and registered these two domains, they would've instantly had access to perform arbitrary attacks on almost 3,000,000 devices without the need to perform a Man-in-the-Middle attack. AnubisNetworks now controls these two extraneous domains to prevent such an attack from occurring in the future for this particular case.

**A(nother) iPhone Lockscreen Bypass**

- http://www.iclarified.com/57887/newly-discovered-trick-lets-you-bypass-iphone-lockscreen-and-access-contacts-photos-more-video
- Newly Discovered Trick Lets You Bypass iPhone Lockscreen and Access Contacts, Photos, More
- A new trick has been discovered that lets you bypass the iPhone's lockscreen and access contacts, photos, and other information for any device with Siri enabled.

- Christina Warren / Gizmodo / Friday
  This Weird Trick Apparently Lets You Bypass Any iPhone's Lock Screen
- http://gizmodo.com/this-weird-trick-apparently-lets-you-bypass-any-iphones-1789134941

- First, you need to call the phone you want to gain access to. If you don't know the number, you can ask Siri "Who am I?" to get it. (A FaceTime call will work as well.) Then, from the incoming call screen, choose the "Message" option and choose "Custom." That opens up a screen to reply to the call with a message.

  From here, you need to enable Voice Over mode, by invoking Siri and saying, "Turn on Voice Over." This will enable an accessibility feature that will read out items on the screen.

  This is where it gets really tricky. Then, you need to double tap on the recipient filed on the message (the name), while also tapping on a random key on the keyboard. This should open up a "to" field on the SMS that will then let you search through contacts already on the phone. (You'll know you've gotten the bug to work when you see the tools pop up next to the compose message box.)

  At this point, you've already broken into the phone to a certain degree, because you can see all of the contacts. Pressing on an "i" icon next to a contact should show details about the contact, which will then allow the user to create a new contact. This is where the exploit becomes really useful. Tapping on the new contact button, a user can opt to add in a photo and doing that will allow access to all the photos on a camera roll. This basically means a skilled person could browse all of your photos without you knowing.

  Tricks that let hackers bypass any iPhone's lockscreen are hardly new, and they typically take a little bit of skill and luck. And although the iDeviceHelp video and others like it are cropping up all over YouTube, it's always safe to remain skeptical about how dangerous these tricks might be. As far as bugs go, this one feels fairly innocuous since it requires prolonged physical access to a device. And although you can access photos, actually doing anything with that data is a different story.

- If you disable Siri on the lock screen (and Hey Siri) this stops this security hole. If you do that then at least you will have some safety that way until Apple issues a proper fix.

**And another iPhone locking link is going around**

- Charlie Miller at 9to5Mac reports.
- https://9to5mac.com/2016/11/21/iphone-froze-after-playing-video-fix/
- There's another malicious link floating around that will cause any iOS device to freeze & require a hard reset

- [CHARLIE] Every so often, a weird bug related to iOS will emerge that causes some sort of temporary misbehaving for users affected by it. For instance, nearly two years ago the infamous "effective power" bug took the internet by storm, and we've seen various other similar issues since then.

  Now, it has been discovered that playing a certain .mp4 video in Safari on any iOS device will cause the device to slow to a crawl and eventually freeze altogether…

  In the video from EverythingApplePro, viewing a certain video in Safari will cause iOS to essentially overload and gradually become unusable. We won't link the infectious video here for obvious reasons, but you can take our word for it when we say that it really does render your device unusable.

  It's not clear why this happens. The likely reason is that it's simply a corrupted video that's some sort of memory leak and when played, iOS isn't sure how to properly handle it, but there's like more to it than that.

  Because of the nature of the flaw, it isn't specific to a certain iOS build. Playing the video on an iPhone running as far back as iOS 5 will cause the device to freeze and become unusable.

  Interestingly, with iOS 10.2 beta 3, if you let an iPhone affected by the bug sit there for long enough, it will power off and indefinitely display the spinning wheel that you normally see during the shutdown process.

  If someone sends you the malicious link and you fall for it, this is luckily a pretty easy problem to fix. All you have to do is hard reboot your device. For any iPhone but the iPhone 7, this can be down by long-pressing the power and Home buttons at the same time. The iPhone 7, of course, uses a new non-mechanical Home button. In order to reboot an iPhone 7, you must long-press the power button and volume down button at the same time.

  It doesn't appear that there are any longstanding effects of viewing the malicious video. Presumably this is something Apple will fix with an upcoming software update, but in the meantime, be on the look out for suspicious links floating around out there.

## SpinRite

Ben Aylett
Location: Perth, Western Australia
Subject: Finally!
Date: 14 Nov 2016 19:22:40
:
I am a regular technology guest on a local radio talkback station in Perth Western Australia and I had a caller tell me about problems he was having with his hard drive. Of course I went right to my favorite hard drive tool which, of course, was SpinRite.

Thanks for making a great tool that I use at least once a month to help out others. It usually brings drives back from the dead, and occasionally confirms my suspicions that the hard drive is beyond salvation.

Either way, I am proud to share GRC and all your good work with my listeners and clients when I can.

## Security News, continuing...

**Robert Graham (Errata Rob) who created "BlackICE"**

- "This security camera was infected by malware 98 seconds after it was plugged in"
- https://techcrunch.com/2016/11/18/this-security-camera-was-infected-by-malware-in-98-seconds-after-it-was-plugged-in/

- Here's an object lesson on the poor state of the so-called Internet of Things: Robert Stephens plugged a Wi-Fi-connected security camera into his network and it was compromised in… 98 seconds.

  Stephens, a tech industry veteran, wasn't so naive as to do this without protecting himself. It was walled off from the rest of the network and rate-limited so it couldn't participate in any DDoS attacks.

  He monitored its traffic carefully, expecting to see — as others have — attempts to take over the device. But even the most jaded among us probably wouldn't have guessed it would take less than two minutes.

  - 8/x: Actually, it took 98 seconds for first infection pic.twitter.com/EDdOZaEs0V
    — Rob Graham ?? (@ErrataRob) November 18, 2016

- Ninety-eight seconds after it jumped on the Wi-Fi, the camera was attacked by a Mirai-like worm that knew the default login and password. The worm (its advance agent, really) checked the specs of its new home and then downloaded the rest of itself onto the device and, had Stephens not locked it down beforehand, would then be ready to participate in all manner of online shenanigans.

  The camera, a cheap off-brand one from a company that sells smartwatches for $12, isn't exactly best-in-class. This type of thing could be fixed with a firmware update or, in some cases, by simply changing the default password, but not everyone knows to do that, and even the most tech-savvy people might not get that done in two minutes.

Better-quality devices will almost certainly be better protected against this kind of thing, and may for example block all incoming traffic until they're paired with another device and set up manually. Still, this is a good reminder that it really is a jungle out there.

**Bruce Schneier gives Congress some sobering truth...**

- http://www.dailydot.com/layer8/bruce-schneier-internet-of-things/
- The Daily Dot: <quote> Speaking before members of Congress, the internet pioneer made clear the dangers of the internet of things: 'The internet era of fun and games is over'

- Internet pioneer Bruce Schneier issued a dire proclamation in front of the House of Representatives' Energy & Commerce Committee Wednesday: "It might be that the internet era of fun and games is over, because the internet is now dangerous."

- The meeting, which focused on the security vulnerabilities created by smart devices, came in the wake of the Oct. 21 cyberattack on Dyn that knocked Amazon, Netflix, Spotify, and other major web services offline.

- Schneier's opening statement provided a clear distillation of the dangers posed by connected devices. He starts around the 1:10:30 mark in the livestream...

- Here's how he framed the Internet of Things, or what he later called the "world of dangerous things":

  [Bruce]: As the chairman pointed out, there are now computers in everything. But I want to suggest another way of thinking about it in that everything is now a computer: This is not a phone. It's a computer that makes phone calls. A refrigerator is a computer that keeps things cold. ATM machine is a computer with money inside. Your car is not a mechanical device with a computer. It's a computer with four wheels and an engine… And this is the Internet of Things, and this is what caused the DDoS attack we're talking about.

- He then outlined four truths he's learned from the world of computer security, which he said is "now everything security."

- 1) 'Attack is easier than defense'

- [Bruce] Complexity is the worst enemy of security. Complex systems are hard to secure for an hours' worth of reasons, and this is especially true for computers and the internet. The internet is the most complex machine man has ever built by a lot, and it's hard to secure. Attackers have the advantage.

- 2) 'There are new vulnerabilities in the interconnections'

- [Bruce] The more we connect things to each other, the more vulnerabilities in one thing affect other things. We're talking about vulnerabilities in digital video recorders and webcams that allowed hackers to take websites. … There was one story of a vulnerability in an Amazon account [that] allowed hackers to get to an Apple account, which allowed them to get to a Gmail account, which allowed them to get to a Twitter account. Target corporation, remember that attack? That was a vulnerability in their HVAC contractor that allowed the attackers to get into Target. And vulnerabilities like this are hard to fix. No one system might be at fault. There might be two secure systems that come together to create insecurity.

- 3) 'The internet empowers attackers'

- [Bruce] Attacks scale. The internet is a massive tool for making things more efficient. That's also true for attacking. The internet allows attacks to scale to a degree that's impossible otherwise. We're talking about millions of devices harnessed to attack Dyn, and that code, which somebody smart wrote, has been made public. Now anybody can use it. It's in a couple dozen botnets right now. Any of you can rent time on one dark web to attack somebody else. (I don't recommend it, but it can be done.)

  And this is more dangerous as our systems get more critical. The Dyn attack was benign. A couple of websites went down. The Internet of Things affects the world in a direct and physical manner: cars, appliances, thermostats, airplanes. There's real risk to life and property. There's real catastrophic risk.

- 4) 'The economics don't trickle down'

- [Bruce] Our computers are secure for a bunch of reasons. The engineers at Google, Apple, Microsoft spent a lot of time on this. But that doesn't happen for these cheaper devices. … These devices are a lower price margin, they're offshore, there's no teams. And a lot of them cannot be patched. Those DVRs are going to be vulnerable until someone throws them away. And that takes a while. We get security [for phones] because I get a new one every 18 months. Your DVR lasts for five years, your car for 10, your refrigerator for 25. I'm going to replace my thermostat approximately never. So the market really can't fix this.

  Bruce then laid out his argument for why the government should be a part of the solution, and the danger of prioritizing surveillance over security.

  (Remember, Bruce has become a bit of an anti-government-spying activist. He is NO FAN of government intervention. It's a little like Linus Torvalds or Richard Stallman saying they want more government involvement...)

- [Bruce] It was OK when it was fun and games. But already there's stuff on this device that monitors my medical condition, controls my thermostat, talks to my car: I just crossed four regulatory agencies, and it's not even 11 o'clock. This is something that we're going to need to do something new about. And like many new agencies in the 20th century, many new agencies were created: trains, cars, airplanes, radio, nuclear power. My guess is that [the internet] is going to be one of them. And that’s because this is different. This is all coming. Whether we like that the technology is coming, it’s coming faster than we think. I think government involvement is coming, and I’d like to get ahead of it. I’d like to start thinking about what this would look like.

We’re now at the point where we need to start making more ethical and political decisions about how these things work. When it didn’t matter—when it was Facebook, when it was Twitter, when it was email—it was OK to let programmers, to give them the special right to code the world as they saw fit. We were able to do that. But now that it’s the world of dangerous things—and it’s cars and planes and medical devices and everything else—maybe we can’t do that anymore.

That’s not necessarily what Schneier wants, but he recognizes its necessity.

[Bruce] I don’t like this. I like the world where the internet can do whatever it wants, whenever it wants, at all times. It’s fun. This is a fun device. But I’m not sure we can do that anymore.”

**Britain passes the most extreme law ever passed in a democracy**

- http://www.zdnet.com/article/snoopers-charter-expansive-new-spying-powers-becomes-law/
- "The law requires UK internet providers to store browsing histories -- including domains visited -- for one year, in case of police investigations."
- [Zack Wittaker]
  The UK has just passed a massive expansion in surveillance powers, which critics have called "terrifying" and "dangerous".

  The new law, dubbed the "snoopers' charter", was introduced by then-home secretary Theresa May in 2012, and took two attempts to get passed into law following breakdowns in the previous coalition government.

  Four years and a general election later -- May is now prime minister -- the bill was finalized and passed [last] Wednesday by both parliamentary houses.

  Civil liberties groups have long criticized the bill, with some arguing that the law will let the UK government "document everything we do online".

  The law will force internet providers to record every internet customer's top-level web history in real-time for up to a year, which can be accessed by numerous government departments; force companies to decrypt data on demand -- though the government has never been that clear on exactly how it forces foreign firms to do that that; and even disclose any new security features in products before they launch.

  Not only that, the law gives intelligence agencies the power to legally hack into computers and devices of citizens (known as equipment interference), although some protected professions -- such as journalists and medical staff -- are layered with marginally better protections.

The bill was opposed by representatives of the United Nations, all major UK and many leading global privacy and rights groups, and a host of Silicon Valley tech companies.

The law will be ratified by royal assent in the coming weeks.

**Ransomware Developer Asks Security Researcher for Help in Fixing Broken Crypto**

- (A weird ethical dilemma)
- http://www.bleepingcomputer.com/news/security/ransomware-developer-asks-security-researcher-for-help-in-fixing-broken-crypto/
- Fabian Wosar, Emsisoft security researcher, is facing a moral dilemma like very few security researchers have faced before.

  Wosar, who is also a user of the Bleeping Computer forums where he's been active for the past few years helping ransomware victims, has received a private message from a user that has identified himself as one of the people who coded the Apocalypse ransomware.

  During their exchange, the ransomware coder has asked Wosar to help their crew fix a bug in the ransomware's encryption process that causes files to be overwritten with junk data.

  In order to secure Wosar's help, the ransomware coder has appealed to the researcher's dedication to helping ransomware victims. The crook says that if Wosar helps, they'll be able to provide a ransomware variant that doesn't destroy users' files.

  The ransomware author was very candid with Wosar in his request. He said that even if Wosar helps or not, money is more important to them, and they'll continue to spread their ransomware as they have been doing for the past six months.

  The only ones that will have something to gain are the ransomware victims, who, if they decide to pay, will regain access to their files. The request, in full, is below:

- [From the Ransomware Authors]: Once you have written that you feel sorry for the ransomware victims... You can help them. As you know, now we use CryptoApi, and if encryption function fails - we just fil file with garbage.

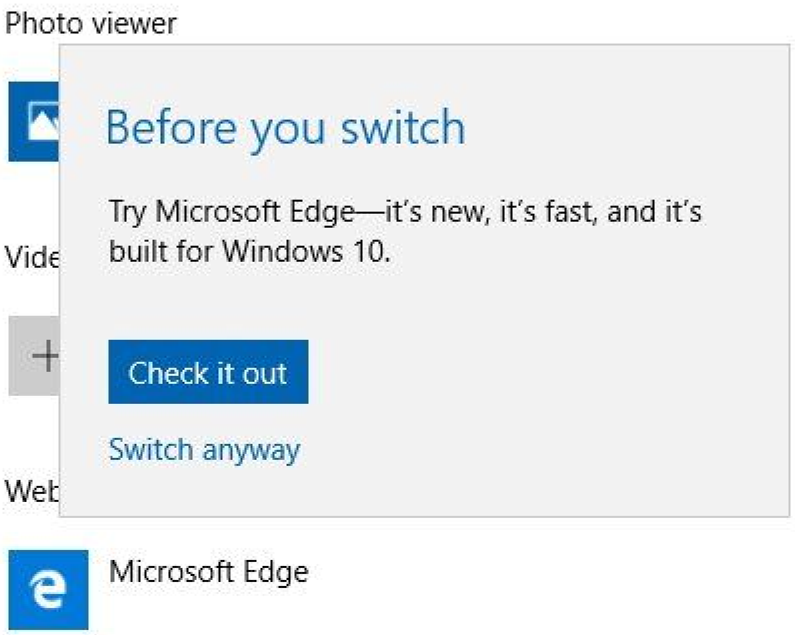
  As a result, after the decryption some victims crying to us... we try to keep an honest business, but money is more important to us, so some of the victims lose some of their files.

  How you can help them? I know you are the best in cryptography, so we can send you the encryption and decryption code, and you should point us where is a bug, we will fix it and no more fake encryptions with garbage instead of the file content.

- Fabian has successfully cracked some of their Cryptomalware in the past and posted decryptors for it.

### Windows 10 is now pushing Edge on Win10 Insider Preview users

- "Never Edge"?
- Matthias Bartosik (@b4rt0s1k)
- 11/21/16, 1:26 AM
- Latest #Win10 insider preview changes default browser to #Edge and tries to persuade me to stay when I want to switch back to @googlechrome? pic.twitter.com/movaQ98r5P



Before you switch

Try Microsoft Edge—it's new, it's fast, and it's built for Windows 10.

## Miscellany

### Why was "Black Nurse" named Black Nurse?

- [http://www.netresec.com/?page=Blog&month=2016-11&post=BlackNurse-Denial-of-Service-Attack](http://www.netresec.com/?page=Blog&month=2016-11&post=BlackNurse-Denial-of-Service-Attack)

- Update November 17, 2016

  There seems to be some confusion/amusement/discussion going on regarding why this attack is called the "BlackNurse". Also, googling "black nurse" might not be 100 percent safe-for-work, since you risk getting search results with inappropriate videos that have nothing to do with this attack.

  The term "BlackNurse", which has been used within the TDC Security Operations Center for some time to denote the "ICMP 3,3" attack, is actually referring to the two guys at the SOC who noticed how surprisingly effective this attack was. One of these guys is a former blacksmith and the other a nurse, which was why a college of theirs jokingly came up with the name "BlackNurse". However, although it was first intended as a joke, the team decided to call the attack "BlackNurse" even when going public about it.

**SQRL Presentation Slides**

- https://www.grc.com/sqrl/presentation.pdf

**The lack of Dark Matter and the Bullet Cluster**

- ... feedback from our listeners.

**This Week on the Fringe: "NASA research arm confirms reactionless space drive."**

- Science Alert:
  It's official: NASA's peer-reviewed EM Drive paper has finally been published

- http://www.sciencealert.com/it-s-official-nasa-s-peer-reviewed-em-drive-paper-has-finally-been-published

- After months of speculation and leaked documents, NASA's long-awaited EM Drive paper has finally been peer-reviewed and published. And it shows that the 'impossible' propulsion system really does appear to work.

  The NASA Eagleworks Laboratory team has put forward a hypothesis for how the EM Drive could produce thrust – something that seems impossible according to our current understanding of the laws of physics.

  In case you've missed the hype, the EM Drive, or Electromagnetic Drive, is a propulsion system first proposed by British inventor Roger Shawyer back in 1999. Instead of using heavy, inefficient rocket fuel, it bounces microwaves back and forth inside a cone-shaped metal cavity to generate thrust. According to Shawyer's calculations, the EM Drive could be so efficient that it could power us to Mars in just 70 days.

  But, there's a big problem with the system: It defies Newton's third law, which states that everything must have an equal and opposite reaction. According to the law, for a system to produce thrust, it has to push something out the other way. The EM Drive doesn't do this. Yet in test after test it continues to work. Last year, NASA's Eagleworks Laboratory team got their hands on an EM Drive to try to figure out once and for all what was going on.

  And now we finally have those results.

  The new peer-reviewed paper is titled "Measurement of Impulsive Thrust from a Closed Radio-Frequency Cavity in Vacuum", and has been published online as an open access 'article in advance' in the American Institute of Aeronautics and Astronautics (AIAA)’s Journal of Propulsion and Power. It'll appear in the December print edition.

- "Measurement of Impulsive Thrust from a Closed Radio-Frequency Cavity in Vacuum (AIAA)"
- http://arc.aiaa.org/doi/10.2514/1.B36120

- Conclusions:
  A vacuum test campaign that used an updated integrated test article and optimized torsion pendulum layout was completed. The test campaign consisted of a forward thrust element that included performing testing at ambient pressure to establish and confirm good tuning, as well as subsequent power scans at 40, 60, and 80 W, with three thrust runs performed at each power setting for a total of nine runs at vacuum. The test campaign consisted of a reverse thrust element that mirrored the forward thrust element. The test campaign included a null thrust test effort of three tests performed at vacuum at 80 W to try and identify any mundane sources of impulsive thrust; none were identified.

  Thrust data from forward, reverse, and null suggested that the system was consistently performing at 1.2±0.1 mN/kW, which was very close to the average impulsive performance measured in air. A number of error sources were considered and discussed. Although thermal shift was addressed to a degree with this test campaign, future testing efforts should seek to develop testing approaches that are immune to CG shifts from thermal expansion.

  As indicated in Sec. II.C.8, a modified Cavendish balance approach could be employed to definitively rule out thermal. Although this test campaign was not focused on optimizing performance and was more an exercise in existence proof, it is still useful to put the observed thrust-to-power figure of 1.2 mN/kW in context: The current state-of–the-art thrust to power for a Hall (Xenon ion plasma) thruster is on the order of 60 mN/kW. This is an order of magnitude higher than the test article evaluated during the course of this vacuum campaign; however, for missions with very large delta-v requirements, having a propellant consumption rate of zero could offset the higher power requirements. The 1.2 mN/kW performance parameter is over two orders of magnitude higher than other forms of “zero-propellant” propulsion, such as light sails, laser propulsion, and photon rockets having thrust-to-power levels in the 3.33–6.67 μN/kW.

- http://www.nasaspaceflight.com/2015/04/evaluating-nasas-futuristic-em-drive/

**~~ 30 ~~**