Security Now! #593 - 01-03-17

I’m NOT a Robot! (really)

This week on Security Now!

Law enforcement and the Internet of Tattling things, a very worrisome new and widespread PHP eMail vulnerability, Paul and Maryjo score a big concession from Microsoft, a six year old "hacker" makes the news, Apple discovers how difficult it is to make developers change, hyperventilation over Russian malware found on a power utility's laptop, the required length of high entropy passwords, more pain for Netgear, an update on the just finalized v1.3 of TLS, the EFF's growing "Secure" messaging scorecard, a bunch of fun miscellany... and how does that "I'm not a Robot" checkbox work?

Bernard is quite certain he’s not a robot!

Security News

Warrant for Amazon Echo records in murder case gets privacy advocates' attention.

- A man was found dead in a suspect's backyard patio hot tub with bruises and cuts consistent with a fight, and blood in the hot tub water.
- The suspect will be tried on charges of 1st-degree murder.
- Detectives in an Arkansas murder investigation want to obtain data from the suspect's various IoT systems.
- They've asked Amazon for anything that the suspect's Amazon Echo may have "overheard."
- They've also noted from the suspect's smart water meter that 140 gallons of water was used between 1am and 3am the night the victim was found dead in the suspect's hot tub.
- Investigators assume and allege that the waterwas used to wash away evidence of what happened on the patio.
- The examination of the water meter and the request for stored Echo information raises a bigger question about privacy. At a time when we have any number of devices tracking and automating our habits at home, should that information be available for use against us in criminal cases?
- The defense attorney argues that I should not be, stating: "You have an expectation of privacy in your home, and I have a big problem that law enforcement can use the technology that advances our quality of life against us."
- There's also the question of the reliability of information from smart home devices since accuracy can be an issue for any number of readily hackable IoT gadgets. So someone could plausibly be framed by their IoT devices. However, an audio recording would seemingly be a solid piece of evidence, if released.
- An Amazon spokesperson said: "Amazon will not release customer information without a valid and binding legal demand properly served on us. Amazon objects to overbroad or otherwise inappropriate demands as a matter of course."
- Some facts:
    - The Amazon Echo only captures audio and streams it to the cloud when the device hears the wake word "Alexa."
    - A ring on the top of the device turns blue to give a visual indication that audio is being recorded.
    - Those clips, or "utterances" as the company calls them, are stored in the cloud until a customer deletes them either individually or all at once. When that's done, the "utterances" are permanently deleted.
    - And, the microphones on an Echo device can be manually turned off at any time.

- Links:
  - http://katv.com/news/local/warrant-for-amazon-echo-records-in-murder-case-gets-privacy-advocates-attention
  - http://www.foxnews.com/tech/2016/12/28/amazon-alexa-data-wanted-in-murder-investigation.html
  - https://www.engadget.com/2016/12/27/amazon-echo-audio-data-murder-case/
  - http://www.nydailynews.com/news/national/police-receive-warrant-search-murder-suspect-amazon-echo-article-1.2925898
  - https://techcrunch.com/2016/12/27/an-amazon-echo-may-be-the-key-to-solving-a-murder-case/

An extremely worrisome PHPMailer 0-Day

- SecurityFocus: http://www.securityfocus.com/archive/1/539967

- Critical PHPMailer Flaw leaves Millions of Websites Vulnerable to Remote Exploit
  - PHPMailer is the world's most popular PHP eMail transport software.

  - It is one of the most popular open source PHP libraries used by at least 9 million PHP websites and popular open source web applications worldwide including WordPress, Drupal, 1CRM, SugarCRM, Yii, and Joomla include the PHPMailer library and use it to send email.

  - Dawid Golunski of Legal Hackers, a Polish security researcher, discovered a critical vulnerability (CVE-2016-10033) which allows an attacker to remotely execute arbitrary code in the context of the web server and compromise the target web application.

  - Golunski wrote: "To exploit the vulnerability, an attacker could target common website components such as contact/feedback forms, registration forms, password email resets and others that send out emails with the help of a vulnerable version of the PHPMailer class. A successful exploitation could let remote attackers gain access to the target server in the context of the web server account which could lead to a full compromise of the web application."

  - Golunski responsibly reported the vulnerability to the developers, who have patched the vulnerability in their new release, PHPMailer 5.2.18... and all versions of PHPMailer before the critical release of PHPMailer 5.2.18 are affected, so web administrators and developers are strongly recommended to update to the patched release.

  - But!... The first patch of the vulnerability CVE-2016-10033 was incomplete and the whole mess was publicly disclosed on a security mailing list, so Golunski has published a demonstrates bypass to carry out Remote Code Execution on all current versions (including 5.2.19).

  - Millions of websites currently remain unpatched and are vulnerable.

- Some Technical Details:
  - The patch for CVE-2016-10033 vulnerability added in PHPMailer 5.2.17 sanitizes the $Sender variable by applying escapeshellarg() escaping before the value is passed to mail() function.

  - It does not however take into account the clashing of the escapeshellarg() function with internal escaping with escapeshellcmd() performed by mail() function on the 5th parameter.

  - As a result it is possible to inject an extra quote that does not get properly escaped and break out of the escapeshellarg() protection applied by the patch in PHPMailer 5.2.17.

  - An attacker could pass the -X parameter of sendmail to write out a log file with arbitrary PHP code.

  - This makes the current latest 5.2.19 and 5.2.18 versions of PHPMailer vulnerable to Remote Code Execution despite the patch.

- Dawid Golunski
  - PHPMailer < 5.2.20 Remote Code Execution PoC 0day Exploit (CVE-2016-10045) (Bypass of the CVE-2016-1033 patch)

    Discovered by Dawid Golunski (@dawid_golunski)
    https://legalhackers.com

    Desc:
    I discovered that the current PHPMailer versions (< 5.2.20) were still vulnerable to RCE as it is possible to bypass the currently available patch.

    This was reported responsibly to the vendor & assigned a CVEID on the 26th of December. The vendor has been working on a new patch which would fix the problem but not break the RFC too badly. The patch should be published very soon.

    I'm releasing this as a 0day without the new patch available publicly as a potential bypass was publicly discussed on oss-sec list with Solar Designer in the PHPMailer < 5.2.18 thread, so holding the advisory further would serve no purpose.

  - Current advisory URL:
    - https://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10045-Vuln-Patch-Bypass.html

  - PoC exploit URL:
    - https://legalhackers.com/exploits/CVE-2016-10045/PHPMailer_RCE_exploit.pl

Microsoft Admits Its Malware-Style Windows 10 Upgrade Sales Pitch Went Too Far

- Microsoft CMO Chris Capossela on aggressive Windows 10 upgrades

- In an interview with Paul and MaryJo on Windows Weekly, Chris Capossela, Microsoft's Chief Marketing Officer, called the weeks between Microsoft's initial patch update and the eventual decision to reverse course "very painful," saying:

  "We know we want people to be running Windows 10 from a security perspective, but finding the right balance where you're not stepping over the line of being too aggressive is something we tried and for a lot of the year I think we got it right, but there was one particular moment in particular where, you know, the red X in the dialog box which typically means you cancel didn't mean cancel.

  And within a couple of hours of that hitting the world, with the listening systems we have we knew that we had gone too far and then, of course, it takes some time to roll out the update that changes that behavior. And those two weeks were pretty painful and clearly a lowlight for us. We learned a lot from it obviously."

- (Somehow their "listening systems" missed the previous six months of industry-wide howling over earlier "Get Windows 10" arm twisting behavior.)

- Never10: Downloads/day: 2,236 & Total downloads: 2,262,108

- Links:
  - https://www.extremetech.com/computing/241587-microsoft-finally-admits-malware-style-get-windows-10-upgrade-campaign-went-far
  - https://www.techdirt.com/articles/20161227/10130536350/microsoft-finally-admits-malware-style-windows-10-upgrade-sales-pitch-went-too-far.shtml
  - http://www.businessinsider.com/microsoft-cmo-chris-capossela-windows-10-upgrades-2016-12
  - http://news.softpedia.com/news/microsoft-admits-it-went-too-far-with-aggressive-windows-10-updates-511245.shtml

(In the holiday season's classic demonstration of the security/convenience tradeoff)...

Six year old daughter uses her sleeping mom's thumb to purchase $250 worth of Pokemon toys

- Ashlynd Howell of Little Rock, Arkansas is a precocious 6-year old.

- While her mom, Bethany, was sleeping on the couch, Ashlynd gently used her mom's thumb to unlock the Amazon app on her phone. Ashlynd then proceeded to order $250 worth of Pokemon presents for herself. When her parents got 13 confirmation notices about the purchases, they thought that either they'd been hacked (technically they were... but not be someone remote) or that their daughter had ordered them by mistake. But she proudly explained, "No, Mommy, I was shopping." The Howells were able to return only four of the items.

- Links:
  - http://www.usatoday.com/story/news/nation/2016/12/28/girl-uses-sleeping-moms-thumbprint-pokemon/95907370/
  - http://m.sfgate.com/news/article/Six-year-old-breaks-into-mom-s-phone-to-buy-10822968.php
  - http://gizmodo.com/kid-hero-buys-250-in-pokemon-swag-with-sleeping-moms-t-1790498699

(From the "Forcing people to change is difficult, department.)

Apple has punted on their planned Jan 1st HTTPS (ATS) requirement for iOS apps.

- During the 2016 WWDC, Apple announced that it would require HTTPS connections for iOS apps by the end of 2016.

- Apple's head of security engineering and architecture, Ivan Krstic, said during a WWDC presentation: "Today, I'm proud to say that at the end of 2016, App Transport Security (ATS) is becoming a requirement for App Store apps. This is going to provide a great deal of real security for our users and the communications that your apps have over the network."

- ATS is a feature Apple debuted in iOS 9. When ATS is enabled, it forces an app to connect to web services over an HTTPS connection rather than HTTP, which keeps user data secure while in transit by encrypting it.

- Just as the "S" in IoT stands for "Security", as we know, the "S" in HTTPS stands for secure. But since we have little idea what mobile apps are doing behind the scenes, it can be impossible to determine whether an app's own cloud connections are authenticated and encrypted.

- So ATS is enabled by default for iOS 9, but developers can still switch ATS off and allow their apps to send data over an HTTP connection... an allowance which was supposed to end at the end of this year. And ATS requires the use of TLS v 1.2, with a few exceptions for already encrypted bulk data, like media streaming.

- But as the deadline approached, Apple changed their tune. On December 21st, Apple posted:
  - https://developer.apple.com/news/?id=12212016b&1482372961
  - "App Transport Security (ATS), introduced in iOS 9 and OS X v10.11, improves user security and privacy by requiring apps to use secure network connections over HTTPS. At WWDC 2016 we announced that apps submitted to the App Store will be required to support ATS at the end of the year. To give you additional time to prepare, this deadline has been extended and we will provide another update when a new deadline is confirmed..."

- More about ATS: https://developer.apple.com/videos/play/wwdc2016/706/

Headlines: "Russian malware detected in US electricity utility."

- Lots of smoke and noise.

- Some malware associated with a known Russian hacking campaign known as "Grizzly Steppe" was found on a single, isolated, laptop owned by a Burlington, Vermont electric utility.

- However... that laptop was not and had nothing to do with the electric power grid operation and management.

- Everybody take a deep breath.

- And speaking of hyperventilation:
    - Vermont's state governor, Peter Shumlin, said in a statement: “Vermonters and all Americans should be both alarmed and outraged that one of the world’s leading thugs, Vladimir Putin, has been attempting to hack our electric grid, which we rely upon to support our quality of life, economy, health, and safety.”

    - Peter Welch, a Democratic US representative for Vermont, said Russian hacking was “rampant… systemic, relentless, predatory” and added: “They will hack everywhere, even Vermont, in pursuit of opportunities to disrupt our country.”

- Great... so we've been talking about the inherent vulnerabilities of our power grid for quite some time, yet no one appears will to find or raise and commit the money that is going to be required to fix it.

Jeremi M Gosney (@jmgosney)

- Sagitta: https://sagitta.pw/company/

- Company
  Sagitta HPC is the leader in high-performance password cracking. We deliver enterprise-grade turnkey solutions that are designed by world-renowned password cracking experts and are tailored for information security, forensics, law enforcement, and litigation support professionals. Our modular distributed solution can accommodate clusters of any size, and integrates seamlessly with the popular free software you already know and love. Whether you need a standalone system with three GPUs or a cluster of three hundred, you can count on Sagitta HPC to deliver the perfect solution.

  Sagitta HPC is a wholly-owned subsidiary of Stricture Group LLC, founded in January 2013 by Stricture Group founders Jeremi Gosney and Russell Graves after a large number of inquiries were received asking them to replicate and improve upon their 25-GPU VirtualCL cluster. Since then, Sagitta has delivered solutions to dozens of government and law enforcement agencies, Fortune 500 companies, security consulting firms, and litigation support firms around the world.

At Sagitta's R&D lab, we perform heavy research into the best possible hardware and software combinations for our own internal use at Stricture Group. The best of the best solutions then become products that we make available to our customers. We push the bar higher and higher with each generation, frequently requiring us to write custom code such as od6config to enable the use of next-generation hardware. We also develop our own in-house code in order to maximize the performance and enhance the potential of our products.

Sagitta also gives back to the community by frequently contributing and volunteering time to free/open source password cracking projects, such as Hashcat and John the Ripper.

- **Brutalis...**

- Brutalis is an eight-GPU monster, clawing its way through hashes at unprecedented speeds. Providing up to eight Nvidia GPUs, two Intel Xeon E5-2600V3 CPUs, and up to 768 GB of registered ECC memory, the Brutalis is the fastest, meanest, most hardcore system money can buy. Ships with a 3-year warranty.

- Jeremi's Tweet:
  I've encountered several people lately who use password managers & are generating random passwords 20+ chars long (some as long as 200!)

A security expert found a 0-Day flaw in NETGEAR WNR2000 Routers

- A security researcher, Pedro Ribeiro, discovered vulnerabilities in NETGEAR WNR2000 Routers, including a zero-day flaw, that could be exploited remotely to take full control of the device if remote administration is enabled.

- A scan by Ribeiro has revealed at least 10,000 vulnerable devices with the remote admin enabled that are affected by an RCE flaw, though the total number of affected devices could be much greater.

- Ribeiro attempted to responsibly contact and notify Netgear of his findings, then decided to publish the advisory and to release the exploit code when Netgear never responded to his emails.

- The vulnerabilities were found in NETGEAR WNR2000v5, which does not have remote administration enabled by default on the latest firmware. Remote attacks against WNR2000v5 routers would be possible if a user had manually enabled remote administration.

- Ribeiro stated that the NETGEAR WNR2000 router allows an administrator to perform sensitive actions by invoking the CGI apply.cgi URL on the web server on the device. The URL is exposed by the embedded web server uhttpd .

- While reverse engineering uhttpd, Ribeiro discovered that another function, the apply_noauth.cgi, allows an unauthenticated user to perform sensitive actions on the device including changing Internet WLAN settings, retrieving the admin password, and more... including the exploitation of a stack buffer overflow that would allow arbitrary remote code injection.

TLS v1.3 finalized

- https://www.eff.org/deeplinks/2016/12/what-happened-crypto-2016
- TLS 1.3 design finalized

  The biggest practical development in crypto for 2016 is Transport Layer Security version 1.3. TLS is the most important and widely used cryptographic protocol and is the backbone of secure Internet communication. After years of work by hundreds of researchers and engineers, the new TLS design is considered final from a cryptography standpoint. The protocol is now supported and available in Firefox, Chrome, and Opera.

  While it might seem like a minor version upgrade, TLS 1.3 is a major redesign from TLS 1.2 (which was finished over 8 years ago). In fact, one of the most contentious issues was whether the name should be changed, much as SSL was changed to TLS, to indicate how much of an improvement TLS 1.3 really is.

  A noticeable improvement in speed will be a big factor. TLS 1.3 has been tuned for speed by reducing the number of network round-trips required before data can be sent, either to one round-trip (1-RTT) or even zero round-trips (0-RTT) for repeat connections. These ideas have appeared before in experimental form through the QUIC protocol and False Start for earlier TLS versions, but as part of the default behavior of TLS 1.3 they will soon become much more widespread. This means latency will decrease and webpages will load faster.

  In addition, TLS 1.3 promises big improvements in security. It incorporates two important lessons from decades of experience with TLS: First, the protocol has been simplified by removing support for a number of old protocol features and obsolete cryptographic algorithms. Additionally, TLS 1.3 was designed with the benefit of model checking (which has been used to find flaws in many older versions of TLS and SSL). TLS 1.3 was analyzed

extensively by the cryptographic community during the standardization process, instead of waiting until the protocol is widely deployed and difficult to patch.

- Since this is a core protocol -- perhaps THE core protocol -- upon which we all rely, a forthcoming Security Now podcast will walk through the changes in TLS v1.3 from those we have previously discussed at length.

The EFF's excellent "Surveillance Self Defense" page:

- https://ssd.eff.org/

- Overviews:
  - An Introduction to Threat Modeling
  - Animated Overview: How Strong Encryption Can Help Avoid Online Surveillance
  - Animated Overview: How to Make a Super-Secure Password Using Dice
  - Animated Overview: Protecting Your Device From Hackers
  - Animated Overview: Using Password Managers to Stay Safe Online
  - Choosing Your Tools
  - Creating Strong Passwords
  - Keeping Your Data Safe
  - Seven Steps To Digital Security
  - What Is Encryption?
  - Why Metadata Matters

- Tutorials
  - How to: Avoid Phishing Attacks
  - How to: Circumvent Online Censorship
  - How to: Delete your Data Securely on Linux
  - How to: Delete Your Data Securely on Mac OS X
  - How to: Delete Your Data Securely on Windows
  - How to: Enable Two-factor Authentication
  - How to: Encrypt Your iPhone
  - How to: Install and Use ChatSecure
  - How to: Use KeePassX
  - How to: Use OTR for Mac
  - How to: Use OTR for Windows
  - How to: Use OTR on Linux
  - How to: Use PGP for Linux
  - How to: Use PGP for Mac OS X
  - How to: Use PGP for Windows
  - How to: Use Signal for Android
  - How to: Use Signal on iOS
  - How to: Use Tor for Windows
  - How to: Use Tor on Mac OS X
  - How to: Use WhatsApp on Android
  - How to: Use WhatsApp on iOS

- Briefings
    - An Introduction to Public Key Cryptography and PGP
    - Attending Protests (International)
    - Attending Protests (United States)
    - Choosing the VPN That's Right for You
    - Communicating with Others
    - How Do I Protect Myself Against Malware?
    - Key Verification
    - Protecting Yourself on Social Networks
    - The Problem with Mobile Phones
    - Things to Consider When Crossing the US Border

NEXT WEEK on Security Now!...

- **A close look at the Russian PHP-based malware**

Miscellany

Holiday PDK Episode.

- Several people asked: You don't have a picture of the "portable dog killer"?

The Puzzle of 2016 was: "The Sequence"

The top slogan of 2016 was: "The S in IoT stands for security"

"Travelers" on Netflix

- Produced by Brad Wright
  Brad Wright is a Canadian television producer, screenwriter and actor. He is best known as the creator or co-creator of the television series Stargate SG-1, Stargate Atlantis and Stargate Universe.
- Eric McCormack

Homeland Season 6

- Preview of First Episode now available.
- Season 6 Jan 15 at 9PM ET/PT

The Expanse | Syfy

- http://www.syfy.com/theexpanse
- Season 2 Trailer is online
- We have one month to re-watch the first season... Season 2 starts February 1st.

Bitcoin price moves back above $1000 for the first time in three years.

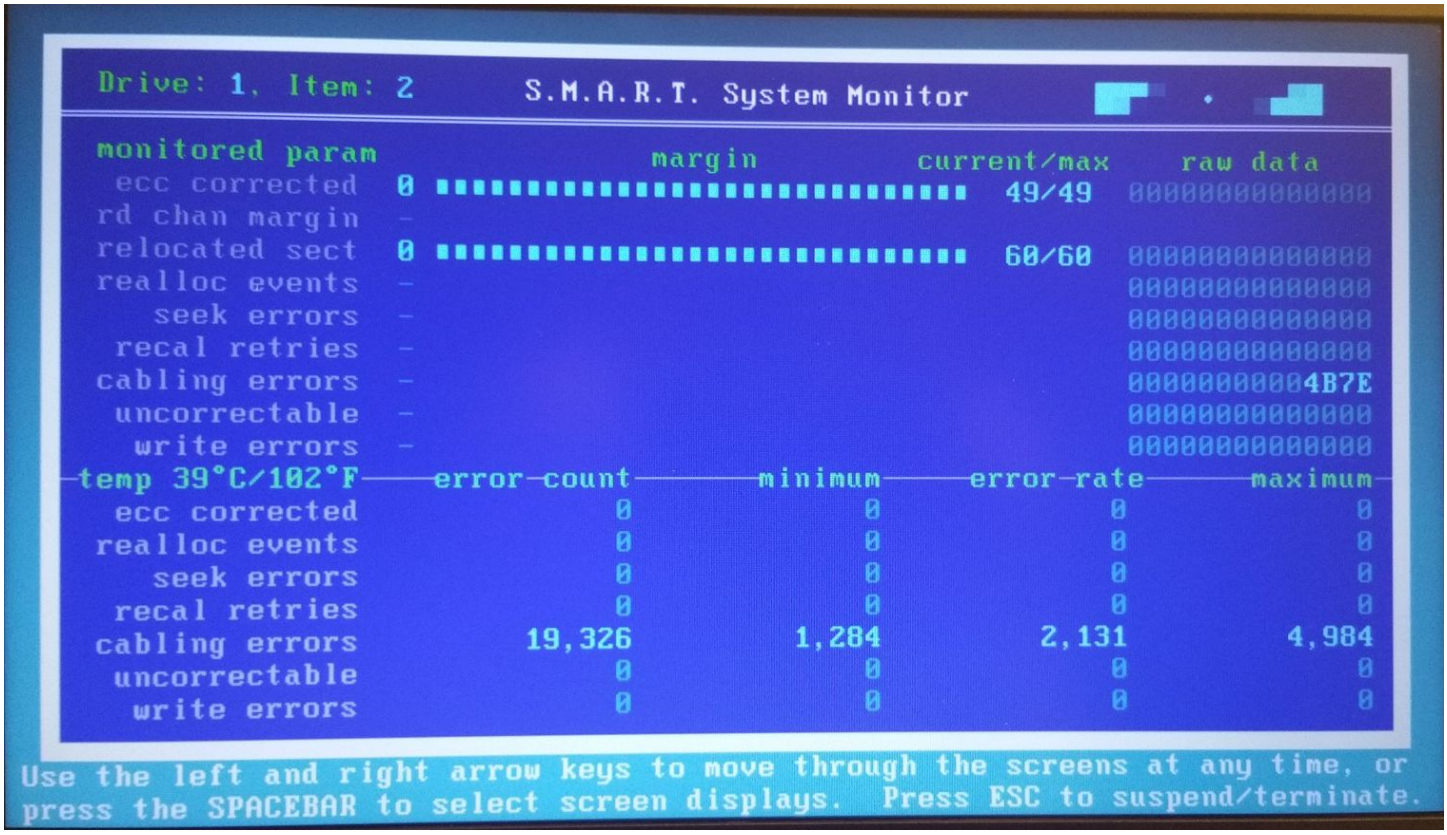
SpinRite

SpinRite cabling errors!

https://twitter.com/Keposet/status/810682216820797440/photo/1

Jason (@Keposet) / 12/18/16, 7:04 PM

@SGgrc friend of mine says he's never seen cabling errors before, what's going on here? #spinrite pic.twitter.com/jCdsWYINB5



I really really promise that I'm not a Robot!

Google Online Security Blog: Are you a robot? Introducing "No CAPTCHA reCAPTCHA"
https://security.googleblog.com/2014/12/are-you-robot-introducing-no-captcha.html

- Google isn’t telling us exactly how they are doing this.
- One investigator believes that incognito mode blocks the easy checkbox mode.
- Another investigator has partially spoofed by using a B-spline mouse path with randomized waypoints and destination.
- The user’s browser must be able to render the canvas.