Security Now! #581 - 10-11-16

Yahoo & Primal Worries

This week on Security Now!

Today Windows update changes for 7 and 8.1, an exploit purchaser offers a $1.5 million bounty for iOS hacks, WhisperSystems encounter first bug, an IEEE study reveals pervasive "Security Fatigue" among users, Firefox and Chrome news, following the WoSign Woes, Samsung Note 7 news, some errata, a bunch of miscellany... and a look into new Yahoo troubles and concerns over the possibility of hidden trapdoors in widely deployed prime numbers.

The impact of Let's Encrypt on the SSL certificate market

By some measures, Let's Encrypt may have become the Internet's largest Certificate Authority.

Security News

The first Second Tuesday of the new updating paradigm for Windows 7 and 8.1

- Brian Krebs reported:
    - Adobe and Microsoft today each issued updates to fix critical security flaws in their products. Adobe's got fixes for Acrobat and Flash Player ready.

      Microsoft's patch bundle for October includes fixes for at least five separate "zero-day" vulnerabilities — dangerous flaws that attackers were already exploiting prior to today's patch release.

      Also notable this month is that Microsoft is changing how it deploys security updates, removing the ability for Windows users to pick and choose which individual patches to install.

- 0-Day flaws are in:
    - IE & Edge
    - Microsoft Office
    - GDI+ (exploitable through the browser)
    - Internet Messaging component of Windows.

- Three new monoliths:
    - A security-only quality update
        - A single update containing all NEW security fixes for that month
    - A security monthly quality rollup
        - A single update containing all new security fixes for that month (the same ones included in the security-only update released at the same time), as well as fixes from all previous monthly rollups. This can also be called the "monthly rollup."
    - A preview of the monthly quality rollup
        - An additional monthly rollup containing a preview of new non-security fixes that will be included in the next monthly rollup, as well as fixes from all previous monthly rollup. This can also be called the "preview rollup." This preview rollup will be released on the third Tuesday of the month (also referred to as the "C week").

iPhone exploit bounty surges to an eye-popping $1.5 million

- Zerodium triples price for iOS exploits, doubles Android bounties to $200,000.

- http://arstechnica.com/security/2016/09/1-5-million-bounty-for-iphone-exploits-is-sure-to-bolster-supply-of-0days/

- Dan Goodin writes:
  A controversial broker of security exploits is offering $1.5 million (£1.2 million) for attacks that work against fully patched iPhones and iPads, a bounty that's triple the size of its previous one.

Zerodium also doubled, to $200,000, the amount it will pay for attacks that exploit previously unknown vulnerabilities in Google's competing Android operating system, and the group raised the amount for so-called zeroday exploits in Adobe's Flash media player to $80,000 from $50,000. After buying the working exploits, the company then sells them to government entities, which use them to spy on suspected criminals, terrorists, enemies, and other targets.

Last year, Zerodium offered $1 million for iOS exploits, up to a total of $3 million. It dropped the price to $500,000 after receiving and paying for three qualifying submissions. On Thursday, Zerodium founder Chaouki Bekrar said the higher prices are a response to improvements the software makers—Apple and Google in particular—have devised that make their wares considerably harder to compromise.

"Prices are directly linked to the difficulty of making a full chain of exploits, and we know that iOS 10 and Android 7 are both much harder to exploit than their previous versions," he told Ars. Asked why a string of iOS exploits commanded 7.5 times the price of a comparable one for Android he said: "That means that iOS 10 chain exploits are either 7.5 x harder than Android or the demand for iOS exploits is 7.5 x higher. The reality is a mix of both."

Signal for Android Attachment Bug

- https://whispersystems.org/blog/signal-android-attachment-bug/
- https://pwnaccelerator.github.io/2016/signal-part1.html
- https://pwnaccelerator.github.io/2016/signal-part2.html
- https://cybermashup.com/2016/09/21/hunting-for-vulnerabilities-in-signal-part-3/

- Wonderful Bug:
  <quote> When the Android code retrieves an audio, video, or image attachment, it verifies a cryptographic "message authentication code" to ensure that the attachment hasn't been modified in any way while in transit. Jean-Philippe Aumasson and Markus Vervier pointed out that a 32-bit integer was used to represent the attachment length in that calculation.

  This means that if the attachment is greater than 4GB, the integer representing the attachment's length wraps back around starting from a value of 0. If an attacker were to hack the Signal server and append 4GB of data to a legitimate 1MB attachment while in transit from Bob to Alice, the code that verified the integrity of the attachment on Alice's end would only "see" 1MB of data to verify after downloading the full (1MB + 4GB) attachment from the server. This is because the 32-bit integer representing the 4.001GB attachment's length wraps around to zero at 4GB and ends up at 1MB again. If the attacker hasn't modified that original 1MB of data, then everything checks out fine, even though they've appended 4GB. This is obviously not the outcome we want.

- Various practical considerations make exploitation difficult. For example, the extra attached payload must be exactly 4GB.

- Despite that, Moxie & Co. immediately pushed a patch for Signal for Android. Neither iOS nor Desktop were affected... nor were any other consumers of the Signal protocol.

- <quote> This is the first time that anyone has ever found a bug like this in Signal, though, so huge thanks to Jean-Philippe Aumasson and Markus Vervier for helping to further improve the security and stability of the app.

'Security fatigue' leading computer users to more or less just give up

- https://www.computer.org/csdl/mags/it/2016/05/mit2016050026-abs.html
- https://nakedsecurity.sophos.com/2016/10/07/security-fatigue-leading-computer-users-to-more-or-less-just-give-up/

- Study, submitted to the IEEE, IT Professional, group: NIST (National Institute of Standards & Technology) conducted a survey, not looking for this... but "Security Fatigue" came oozing out of the questionaires.

- People are tired and fed up with the burden of being made so responsible for their online security.

- Abstract:
  Security fatigue has been used to describe experiences with online security. This study identifies the affective manifestations resulting from decision fatigue and the role it plays in users' security decisions. A semistructured interview protocol was used to collect data (N = 40). Interview questions addressed online activities; computer security perceptions; and the knowledge and use of security icons, tools, and terminology. Qualitative data techniques were used to code and analyze the data identifying security fatigue and contributing factors, symptoms, and outcomes of fatigue. Although fatigue was not directly part of the interview protocol, more than half of the participants alluded to fatigue in their interviews. Participants expressed a sense of resignation, loss of control, fatalism, risk minimization, and decision avoidance, all characteristics of security fatigue. The authors found that the security fatigue users experience contributes to their cost-benefit analyses in how to incorporate security practices and reinforces their ideas of lack of benefit for following security advice.

Firefox Test Pilot

- https://testpilot.firefox.com/experiments/tab-center
- Tab Center - native side tabs (Tree Style Tab)
- Page Shot - screen shots built right into the browser. (I use screengrab.)
- Min Vid - sticky video window remains while user browses the web
- Tracking Protection
- Activity Stream
- No more 404s - auto linked to the Wayback Machine
- Universal Search - dynamic search as search terms are entered.

Google Chrome soon won't be such a burden on your computer

- https://www.cnet.com/news/google-chrome-soon-wont-be-such-a-burden-your-computer/
- In Chrome 55, due in December, the V8 JavaScript engine (on both desktop and mobile) will have a significantly reduced memory footprint... by as much as 40% on sites such as Reddit, Twitter, the NYT, etc.

The ongoing Woes of WoSign

- Representatives of WoSign, StartCom & parent Qihoo 360 met with Mozilla today in London.
- WoSign has released a full disclosure document. https://www.wosign.com/report/WoSign_Incident_Report_Update_07102016.pdf Mostly appears to be software bugs of various sorts.
    - Validate site ownership using with any server port.
        - (They claimed that some users had servers running on other ports, so feature added.)
    - Validating ownership of a subdomain and obtain a certificate for the parent domain.
    - Here's one we didn't cover yet: <quote> "This is another system bug that when the subscriber finished the domain control validation, he/she can use a special professional method to add other un-validated domain to the order, then our system issued the certificate including all domains in the order.
- In another problem, they had placed ADVERTISEMENTS in some of the certificates, adding a description with a "buy.wosign.com" link.
- WoSign's CEO is out. WoSign and StartCom are going to de-merge and have separate management and operations teams. (Having a single company issuing certificates under different names is not permitted by the CAB baseline requirements.)

Even the newly replaced Samsung Note 7 phones are exploding.

- http://www.wsj.com/articles/samsung-to-halt-galaxy-note-7-production-temporarily-1476064520
- It may never have been the battery, or not ONLY the battery.
- The Note 7's battery charge management may also be defective.
- Samsung has halted production of the Note 7.

Errata

Peter Brumby (@PeterBrumby)
Hi Steve. Love the podcast and SpinRite. It is the first and probably only time I will be able to contribute to the podcast. In SN 580 you said you submitted grc.com and grc.com to the HSTS pre load list. However you can only submit the base domain grc.com. The HSTS preload list is then applied to the base domain and all its subdomains including www. It's a very minor point but could mess up a non https subdomain if you weren't aware. Keep up the good work.

Miscellany

Westworld

Timeless

The Lost Fleet

A Night Without Stars

HSF Success:

- Janice Morse (via twitter from @sassyjan1209)
  Hi Steve, my son listens to your podcast. I have not had a good night's sleep since 1978, I have been diagnosed with all three forms of sleep apnea. I have had 8 sleep studies, the conclusion is that I never hit REM sleep, I live being exhausted at all times. I wake up exhausted and shook up from nightmares. My son brought over the niacinamide and melatonin. The first night I only got up once, instead of the usual every 25 minutes, with a headache, but I gave it another night, and WOW, not only did I get up only once, but I woke up rested, ready to go for the day, and had a pleasant dream. WOW! Now I've had my 5th successful night in a row, and I am not only looking forward to going to bed, my entire demeanor has changed, I am so excited. If I continue to respond to these natural remedies this is a life changer. Thank you. I will pray that this information gets out to more sufferer's, I certainly will do my best. Janice Morse

- [I asked Janice if I could share her feedback publicly, she replied:]

- Absolutely, use it. I have never imagined I would ever have energy, and happiness. I had no idea what lack of sleep was actually costing me. I am giddy with hope.

The SQRL song! <g>

SpinRite

3n0m41y (@3n0m41y) / 8:14am / October 10th

So yet again SpinRite saves the day for me...
Had an old drive with baby pictures on it.. would not read at all... knew that if I am not able to recover pictures wife will put me out with trash.. (kidding)
Pulled out my trusty copy of SpinRite and, on level 2, it fixed drive!
Now I have all pictures back! Thanks for an awesome product!
Just sent you a Yabba Dabba Do for another copy because you saved day!

Yahoo! in the Doghouse

Massive Half a Billion user account breach kept secret since 2014.

Through the first half of last year, January through June of 2015, software was installed by Yahoo into its systems to help the US government search through the eMails of all its users.

Reuters / October 4th, 2016
http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT
Exclusive: Yahoo secretly scanned customer emails for U.S. intelligence - sources
Reuters has recently reported that in 2015, Yahoo complied with an order it received from the U.S. government to search ALL of its users' incoming emails, in real time.
The EFF notes: "There's still much that we don't know at this point, but if the report is accurate, it represents a new—and dangerous—expansion of the government's mass surveillance techniques."

EFF <quote>:
This is the first public indication that the government has compelled a U.S.-based email provider—as opposed to an Internet-backbone provider—to conduct surveillance against all its customers in real time.

[Steve's note: This is the logical outcome of the "going dark" problem, where the majority of the traffic that's now flowing across the Internet is strongly encrypted. In this new environment, the endpoints where traffic is both concentrated and decrypted, is the place to which surveillance must now move.]

In attempting to justify its warrantless surveillance under Section 702 of the FISA Amendments Act—including Upstream and PRISM—the government has claimed that these programs only "target" foreigners outside the U.S. and thus do not implicate American citizens' constitutional rights. Here, however, the government seems to have dispensed with that dubious facade by intentionally engaging in mass surveillance of purely domestic communications involving millions of Yahoo users.

The [Reuters'] story explains that Yahoo had to build new capabilities to comply with the government's demands, and that new code may have, itself, opened up new security vulnerabilities for Yahoo and its users.

[The security personnel inside Yahoo who discovered this previously unknown software described it as buggy and poorly written, and rootkit-like.]

We read about new data breaches and attempts to compromise the security of Internet-connected systems on a seemingly daily basis. Yet this story is another example of how the government continues to take actions that have serious potential for collateral effects on everyday users.

Yahoo Timeline:
Software, unknown to Yahoo security, was discovered. It was believed to be rootkit malware. The discovery was escalated several levels until it reached the desk of Alex Stamos, who was, at the time, head of Yahoo security. He researched it, discovered that it had been deliberately planted into Yahoo's servers by others within Yahoo... and all further pursuit of "the case" was immediately suppressed.

- This was believed to have been done due to a secret order from the US government. Recently enacted legislation makes disclosure possible and open speech advocates are now pushing for clarity and visibility on this matter.

Yahoo makes it difficult to leave its service by disabling automatic email forwarding

- https://techcrunch.com/2016/10/10/yahoo-makes-it-difficult-to-leave-its-service-by-disabling-email-forwarding/
- http://hosted.ap.org/dynamic/stories/U/US_TEC_YAHOO_BREACH
- Yahoo's ability to newly enable eMail forwarding is suddenly "under development."
- Existing forward remains in effect... but users attempting to setup new account elsewhere are being actively thwarted by Yahoo's refusal to enable new forwarding.

Verizon wants a $1 Billion discount on its pending purchase of Yahoo.

Trapdoored Primes

https://eprint.iacr.org/2016/961.pdf

Cryptanalysis of 1024-bit trapdoored primes
http://caramba.inria.fr/hsnfs1024.html

Abstract:
We have completed a cryptanalysis computation which is at the same time a formidable achievement in terms of size (a 1024-bit discrete logarithm computation), and a small-scale undertaking in terms of computational resources (two months of calendar time on 2000 to 3000 cores).

In comparison, the "real" record for discrete logarithm is 768 bits (announced this spring) and required 10 times as much computational power.

To achieve this [dramatically faster cryptanalysis of a much harder 1024-bit prime] , we cheated. Deliberately. We chose the prime number which defines the problem to be solved in a special way, so that the computation can be made much more efficient. However, we did this in a subtle way, so that the trapdoor we inserted cannot be detected.

Unfortunately, for most of the prime numbers used in cryptography today, we have no guarantee that they have not been generated with such a trapdoor. We estimate that breaking a non-trapdoored 1024-bit prime is at least 10,000 times harder than breaking our trapdoored prime was for us once we knew the trapdoor.

Our computation raises questions about some Internet standards that contain opaque, fixed primes. Theoretically, we know how to guarantee that primes have not been generated with a trapdoor, but most widely used primes come with no such public guarantee. A malicious party who inserted a trapdoored prime into a standard or an implementation would be able to break any communication whose security relies on one of these primes in a short amount of time.

- "Current estimates for 1024-bit discrete log in general suggest that such computations are likely within range for an adversary who can afford hundreds of millions of dollars of special-purpose hardware," the researchers said in their paper. "In contrast, we were able to perform a discrete log computation on a specially trapdoored prime in two months on an academic cluster."

- "The near universal failure of implementers to use verifiable prime generation practices means that use of weak primes would be undetectable in practice and unlikely to raise eyebrows."

- The researchers estimate that performing similar computations for 2048-bit keys, even with backdoored primes, would be 16 million times harder than for 1024-bit keys and will remain infeasible for many years to come. The immediate solution is to switch to 2048-bit keys, but in the future all standardized primes should be published together with their seeds, the researchers said.

~30~