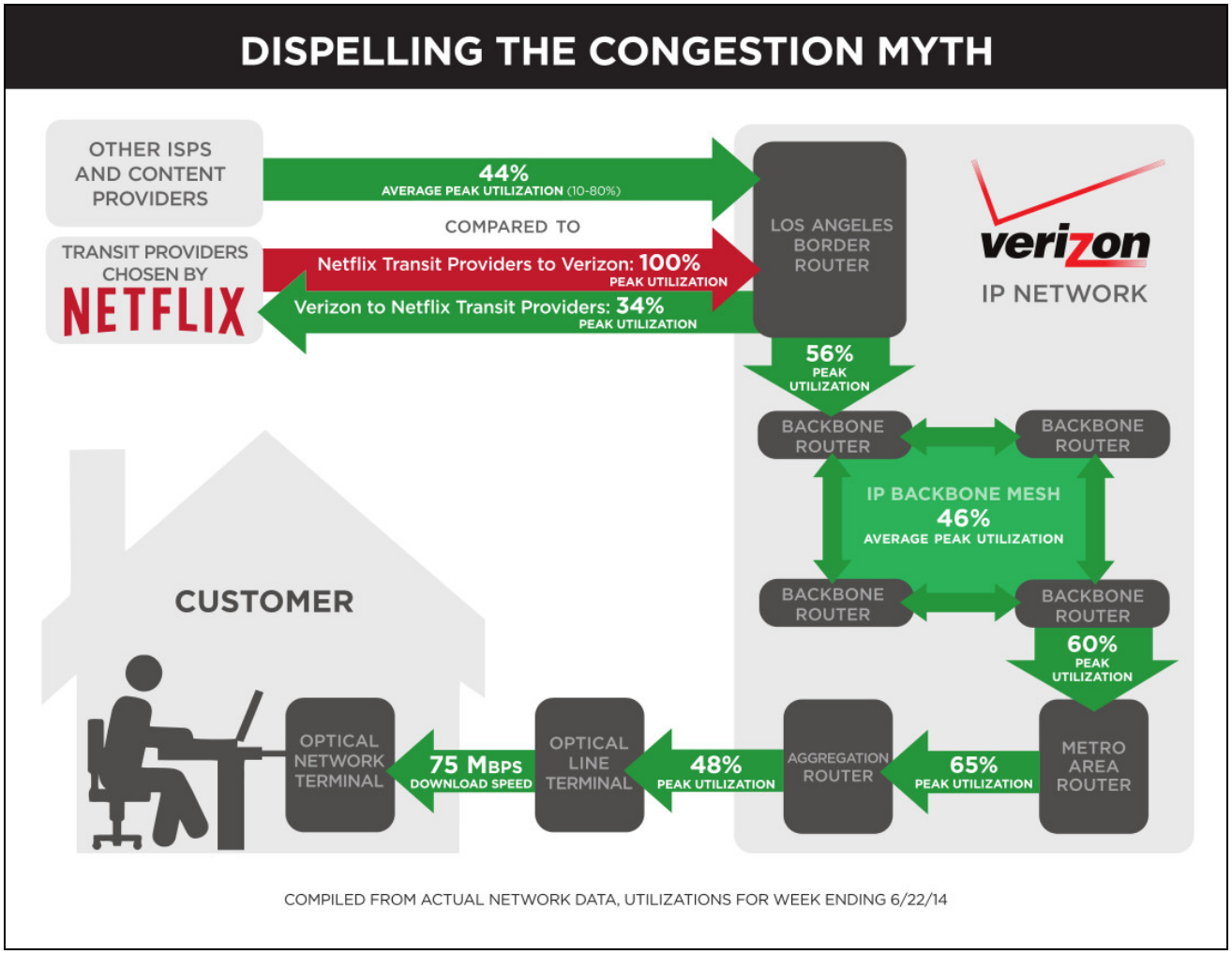
Security Now! #464 - 07-15-14

Q&A #192

Link Tracking Warning!
This document was first authored in Google Docs, then Downloaded as a PDF. So, Google has thoughtfully (ha!) added "tracking" redirections to all of the links here. (I have no idea why, but that's Google.) If that bothers you, simply copy the text of the link into your browser's URL field.

This week on Security Now!

- Are web-based password managers suddenly insecure?
- Three IOT ("Internet of Things") standardization groups
  - New term: "Sleepy Nodes"
- A few hours ago Google announced "Project Zero"
- LibreSSL stumbles upon leaving the gate
- Netflix and Verizon are still squabbling… but there's hope.
- Has CryptoLocker been neutralized?



Security News:

As expected, Microsoft removes its trust of the Indian Certificates.

- https://technet.microsoft.com/library/security/2982792
- <quote> Microsoft is aware of improperly issued SSL certificates that could be used in attempts to spoof content, perform phishing attacks, or perform man-in-the-middle attacks. The SSL certificates were improperly issued by the National Informatics Centre (NIC), which operates subordinate CAs under root CAs operated by the Government of India Controller of Certifying Authorities (CCA), which are CAs present in the Trusted Root Certification Authorities Store. This issue affects all supported releases of Microsoft Windows. Microsoft is not currently aware of attacks related to this issue.

  The subordinate CA has been misused to issue SSL certificates for multiple sites, including Google web properties. These SSL certificates could be used to spoof content, perform phishing attacks, or perform man-in-the-middle attacks against web properties. The subordinate CAs may also have been used to issue certificates for other, currently unknown sites, which could be subject to similar attacks.

  To help protect customers from potentially fraudulent use of this digital certificate, Microsoft is updating the Certificate Trust list (CTL) for all supported releases of Microsoft Windows to remove the trust of certificates that are causing this issue.
- Examine the "Untrusted Certificates" folder for:
  - NIC Certifying Authority
  - CCA India 2007 / 48 22 82 4e ce 7e d1 45 0c 03 9a a0 77 dc 1f 8a e3 48 9b bf
  - NIC CA 2011
  - CCA India 2011 / c6 79 64 90 cd ee aa b3 1a ed 79 87 52 ec d0 03 e6 86 6c b2
  - NIC CA 2014
  - CCA India 2014 / d2 db f7 18 23 b2 b8 e7 8f 59 58 09 61 50 bf cb 97 cc 38 8a

Google Goes Further:

- http://googleonlinesecurity.blogspot.com/2014/07/maintaining-digital-certificate-security.html
- Update Jul 9: India CCA informed us of the results of their investigation on July 8. They reported that NIC's issuance process was compromised and that only four certificates were misissued; the first on June 25. The four certificates provided included three for Google domains (one of which we were previously aware of) and one for Yahoo domains. However, we are also aware of misissued certificates not included in that set of four and can only conclude that the scope of the breach is unknown.

  The intermediate CA certificates held by NIC were revoked on July 3, as noted above. But a root CA is responsible for all certificates issued under its authority. In light of this, in a future Chrome release, we will limit the India CCA root certificate to the following domains and subdomains in order to protect users:
  - gov.in
  - nic.in
  - ac.in
  - rbi.org.in
  - bankofindia.co.in
  - ncode.in & tcs.co.in

“Critical Vulnerabilities Found in Web-Based Password Managers”

- http://devd.me/papers/pwdmgr-usenix14.pdf
- Yes... found, reported and fixed 10 months ago, last September.
- Out of respect for the researchers, Lastpass remained quiet about it until their paper was (just) published.
- LastPass:
    - In August 2013, a security researcher at UC Berkeley, Zhiwei Li, contacted us to responsibly disclose novel vulnerabilities with the LastPass bookmarklets (actively used by less than 1% of the user base) and One Time Passwords (OTPs). Zhiwei discovered one issue that could be exploited if a LastPass user utilized the bookmarklet on an attacking site, and another issue if the LastPass user went to an attacking site while logged into LastPass, and used their username to potentially create a bogus OTP.

      Zhiwei only tested these exploits on dummy accounts at LastPass and we don't have any evidence they were exploited by anyone beyond himself and his research team. The reported issues were addressed immediately, as confirmed by their team, and we let them publish their research before discussing it.

- All but one vendor responded immediately and fixed the known issues.
- Full IN-DEPTH COVERAGE next week.
- http://techcrunch.com/2014/07/11/lastpass-finds-security-holes-in-its-online-password-manager-doesnt-think-anyone-exploited-them/
- http://blog.lastpass.com/2014/07/a-note-from-lastpass.html
- http://www.net-security.org/secworld.php?id=17111

IoT Standardization:

- Insecure LED lights used a fixed AES key.
- Three efforts:
    - AllSeen Alliance
    - OIC
    - Thread
- In chronological order:
- A few months ago the Linux Foundation announced the AllSeen Alliance
    - "AllJoyn" software developed by Qualcomm.
    - https://www.alljoyn.org/
    - https://allseenalliance.org/
    - Press Release announcing 50 members.
    - Microsoft joined on July 2nd.
    - “A Common Language for the Internet of Everything”
    - Our homes, our cars, and the things around us are getting smarter every day. AllJoyn™ is the open source project that lets the compatible smart things around us recognize each other and share resources and information across brands, networks, and operating systems. AllJoyn was initially developed by Qualcomm Innovation Center, Inc. and is now a collaborative open source project of the AllSeen Alliance, AllJoyn gives manufacturers and developers the tools they need to invent new ways for smart things to work together.

- Last week the Open Interconnect Consortium (OIC)
  - http://www.openinterconnect.org/
  - THE OPEN INTERCONNECT CONSORTIUM IS BEING FOUNDED BY LEADING TECHNOLOGY COMPANIES WITH THE GOAL OF DEFINING THE CONNECTIVITY REQUIREMENTS AND ENSURING INTEROPERABILITY OF THE BILLIONS OF DEVICES THAT WILL MAKE UP THE EMERGING INTERNET OF THINGS (IOT).
  - Intel, Broadcom, Samsung, Atmel, Dell, Wind River Systems and more expected soon.
  - International Data Corporation expects the installed base of the Internet of Things will be approximately 212 billion "things" globally by the end of 2020. This is expected to include 30.1 billion installed "connected (autonomous)" things. Today, these devices are connecting to each other using multiple, and often incompatible approaches. Atmel, Broadcom, Dell, Intel, Samsung and Wind River believe that in order to achieve this scale, the industry will need both the collaboration of the open source community and industry standards to drive interoperability of these devices.
  - The Open Interconnect Consortium (OIC) will seek to define a common communication framework based on industry standard technologies to wirelessly connect and intelligently manage the flow of information among devices, regardless of form factor, operating system or service provider. OIC also intends to deliver open source implementations for a variety of IoT market opportunities and vertical segments from smart home solutions to automotive and more.
  - Open source platform to be released shortly.
  - Expected to focus upon security and authentication.
  - Initially targeting home & office... then automotive.

- The Thread Group, launched TODAY...
  - http://threadgroup.org/
  - Site claims: "THREAD SOLVES RELIABILITY, SECURITY, POWER, AND COMPATIBILITY ISSUES FOR CONNECTING PRODUCTS AROUND THE HOME.
  - ONCE AND FOR ALL."
  - Google's NEST Labs, Samsung, ARM, Freescale, Big Ass Fans, Silicon Labs, Yale Security.
  - Nest's products are already using the Thread Protocol.
  - Thread's aim is not an IOT platform but a new wireless protocol which AllSeen and OIC could work on top of.
  - Targeting:
  - Low-Power connections appropriate for battery-operated devices.
  - Security functions within a mesh-style network.
  - Thread supports "Sleepy Nodes" able to operate for years on a single AA battery.
  - Based upon IEEE 802.15.4
  - Short messaging, streamlined routing protocol, SoC.
  - Scalable to interconnect 250+ devices.
  - IPv6 and 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks)
  - Sub-Ghz and also 2.4 Ghz.
  - http://en.wikipedia.org/wiki/6LoWPAN
  - http://datatracker.ietf.org/wg/6lowpan/charter/

Google's Project Zero:

- Let's take the case of the young American hacker George Hotz...
  - At age 17 in 2007, George hacked and cracked AT&T's lock on the iPhone.
  - Later he reverse-engineered and cracked the PlayStation 3. After Sony sued him they settled with his agreement to never hack another Sony product.
  - Then he cracked Chrome OS's security, winning a $150,000 reward from Google for doing so.
  - And two months later, Google's (Hacker Herder) "Chris Evans" hired George full-time to join Google's new team of elite hackers in Project Zero.
- Several members from inside Google have been recruited… e.g. Tavis Ormandy.
- Soon to have more than 10 members on the team.
- Overall goal is to make the Internet safer:
  - The team members are free to look everywhere.
  - Responsible Disclosure
  - Bugs posted to a public external database once patched.
- Links:
  - Andy Greenberg writing for WIRED: http://www.wired.com/2014/07/google-project-zero/
  - http://googleonlinesecurity.blogspot.com/2014/07/announcing-project-zero.html

LibreSSL's PRNG is Unsafe on Linux (thanks Simon Zerafa)

- https://www.agwa.name/blog/post/libressls_prng_is_unsafe_on_linux
- Update:
  - First version of LibreSSL v2.0.0 released Friday.
  - Then it was quickly tweaked for some portability issues to v2.0.1 on Sunday.
- Andrew Ayer writes:
  - Despite the 2.0.x version numbers, these are only preview releases and shouldn't be used in production yet, but have been released to solicit testing and feedback. After testing and examining the codebase, my feedback is that the LibreSSL PRNG is not robust on Linux and is less safe than the OpenSSL PRNG that it replaced.
- Unix servers handle multiple connections by "forking" -- creating an identical copy of themselves to handle each new connection.
- In the case of a deterministic software-based PRNG, a "fork" creates an identical copy... which then generates identical PRNGs.
- LibreSSL and OpenSSL both attempt to detect forking by detecting ProcessID changes.
- But Linux PIDs are 16 bits so collisions are too likely among grandchild processes.
- Child forks are guaranteed not to have colliding PIDs… but not so THEIR children.
- OpenSSL has an explicit PRNG reseeding call... which LibreSSL turned into a NoOp.
- Thus, code what was aware of this danger and deliberately reseeded forked PRNGs are no longer safe.
- (SQRL's Entropy Harvester, for which the source has been published, is completely immune to these problems.)

NetFlix vs Verizon

- http://publicpolicy.verizon.com/blog/entry/why-is-netflix-buffering-dispelling-the-congestion-myth
- Verizon carefully analyzes one customer's 75 Mbit FIOS connection.
- Discovers saturation of the Peering-Point router (shock!).
- Claims that Netflix appears to have deliberately chosen
- Press notes that:
- Problems have continued after Netflix/Verizon agreement.
- Problems immediately disappeared after Netflix/Comcast agreement.
- <Verizon Quote:> Even though there is no congestion on our network, we're not satisfied if our customers are not. We fully understand that many of our customers want a great streaming experience with Netflix, and we want that too. Therefore, we are working aggressively with Netflix to establish new, direct connections from Netflix to Verizon's network. This doesn't "prioritize" Netflix traffic in any way, but it ensures that their traffic gets on our network through direct connections—not middleman networks—that are up to the task.

  The benefit of these direct connections will be two-fold. First, Verizon customers who use Netflix will have a significantly improved experience as Netflix traffic flows over non-congested links. Early tests indicate that this is the case. The other benefit will be that the congestion that we are seeing today on those links between these middleman networks and our L.A. border router will likely go away once the huge volume of Netflix traffic is routed more efficiently. This will improve performance for any other traffic that is currently being affected over those connections.

Has CryptoLocker been neutralized?

- http://www.scmagazine.com/cryptolocker-neutralized-says-justice-department/article/360782/
- http://www.justice.gov/opa/pr/2014/July/14-crm-727.html
  - Friday, July 11, 2014
  - The Justice Department also reported that Cryptolocker has been neutralized by the disruption and cannot communicate with the infrastructure used to control the malicious software. As a result, Cryptolocker is effectively non-functional and unable to encrypt newly infected computers.
- SC Magazine Reports: In its nine months of existence, the ransomware extorted more than $27 million from victims, the firm revealed. Last September, Bitdefender discovered the threat, which claimed more than 12,000 victims in less than a week by spreading through phishing emails.

Miscellany:

- Osmo for iPad
  - SO CLEVER!!!

"The Strain" on FX

- 8.6/10 on IMDB
- Yesterday / LATimes:
    - 'The Strain' recap: These vampires aren't sexy; they're just deadly.

      The vampires in FX's new thriller, "The Strain," are not -- repeat, not -- romantic. They're not brooding or conflicted or passionate or sparkly. They do not pout, pose or toss off come-hither glances. And not a single one of them looks anything like Alexander Skarsgard ("Eric Northman" on True Blood).

      As fans might expect from creature-creator extraordinaire Guillermo del Toro, the undead in this horror series are truly terrifying. They're also parasitic and viral, the product of a kind of contagion that single-mindedly seeks out hosts.

- "Night Zero" / reairing Thursday, Friday & Sun... before
- "The Box" next Sunday.

SQRL:

SpinRite:

Dan Hankins
Location: Scottsdale, AZ
Subject: Spinrite in a VM?
Date: 07 Jul 2014 07:09:52

Much thanks for Security Now! and Spinrite. Love the show and the product. I have a Spinrite question:

I recently started running Spinrite for Level 4 maintenance from within a VMWare virtual machine on my Linux host.

I discovered, much to my surprise, that running that way was more than an order of magnitude faster than native.

Why would this happen? I am concerned that because I have write caching turned on, the maintenance pattern writes are never reaching the hard drive. If that's true, it would defeat Level 4's attempt to refresh the surface. That would make Level 4 equivalent to Level 3 or Level 2.

Should I turn write caching off, or is something else going on?