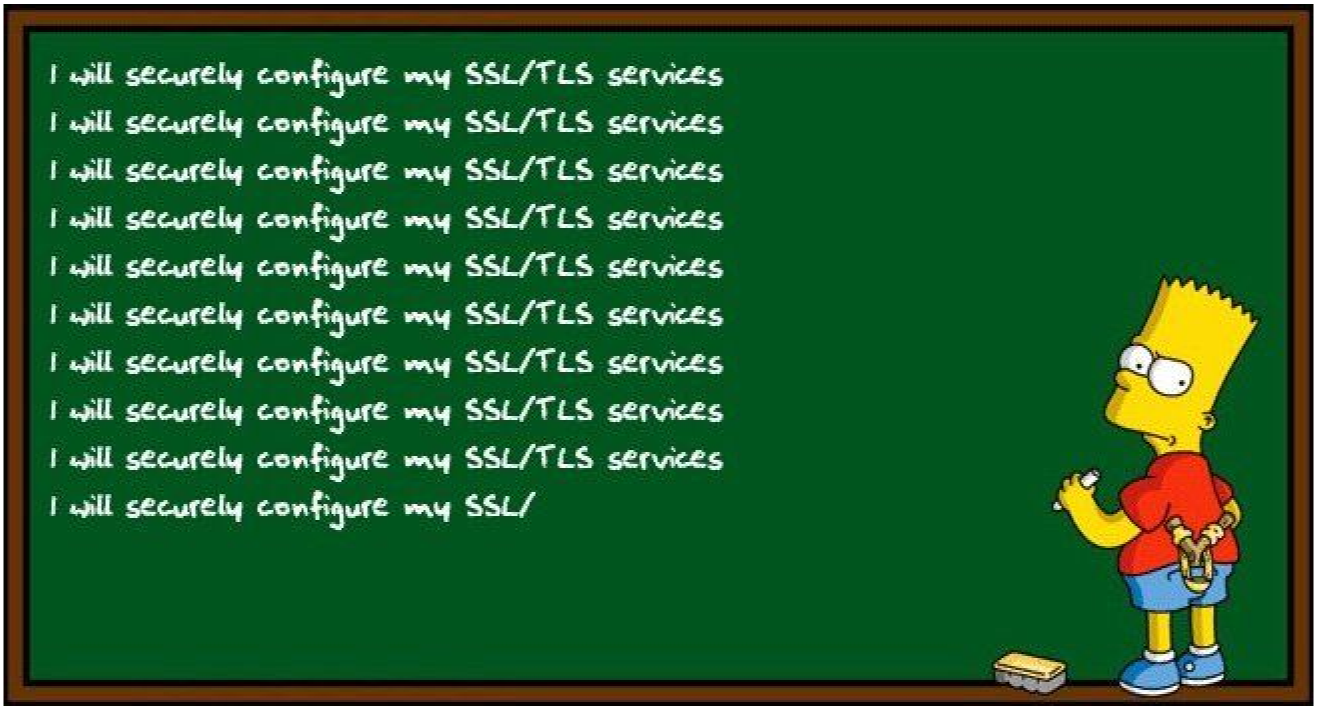
Security Now! #579 - 09-27-16

A Very Busy Week!

This week on Security Now!

- Brian Krebs forced to change move from Akamai to Google's Project Shield
- Yahoo's record-breaking, massive 500-million-user data breach
- Apple's acknowledged iOS 10 backup PBKDF flaw
- Well known teen hacker Jailbreaks his new iPhone 7 in 24 hours
- Microsoft formally allows removal of GWX
- A new OpenSSL server DoS flaw
- More WoSign/StartCom woes (Mozilla prepares to pull the plug)
- Bittorrent Sync renamed and more deeply documented
- A bit of errata, some miscellany, and ten questions and comments from our terrific listeners.


I will securely configure my SSL/TLS services
I will securely configure my SSL/TLS services
I will securely configure my SSL/TLS services
I will securely configure my SSL/TLS services
I will securely configure my SSL/TLS services
I will securely configure my SSL/TLS services
I will securely configure my SSL/TLS services
I will securely configure my SSL/TLS services
I will securely configure my SSL/TLS services
I will securely configure my SSL/

Security News

Akamai terminates Brian Krebs' free DDoS service after a massive sustained attack

- Why the silencing of KrebsOnSecurity opens a troubling chapter for the 'Net
  - http://arstechnica.com/security/2016/09/why-the-silencing-of-krebsonsecurity-opens-a-troubling-chapter-for-the-net/
- Brian Krebs forced to change move from Akamai to Google's project shield
  - https://projectshield.withgoogle.com/public/
- Project Shield is a free service that uses Google technology to protect news sites and free expression from DDoS attacks on the web.
  - Advanced DDos protection
  - Project Shield is built on Google's infrastructure, creating a multi-layer defense system to protect your site against DDoS attacks, including layer 3/4 and layer 7 attacks.
  - Free, unlimited protection
  - No matter the size of your website or the size of the attack, Project Shield provides free protection for news, journalist, human rights, and elections monitoring sites.
  - Customizable caching
  - Project Shield caches content to strengthen DDoS defenses and improve site performance. You can customize the cache settings to meet your site's needs.

Yahoo breaks the record for the largest security breach in history
Half a Billion Accounts!

- If you've ever created a Yahoo account, take these steps immediately to protect your data
  - http://www.recode.net/2016/9/22/13024884/yahoo-data-breach-privacy-security-hacking-online-safety
- Here's what you should know, and do, about the Yahoo breach
  - http://www.pcworld.com/article/3123398/security/heres-what-you-should-know-and-do-about-the-yahoo-breach.html
- Yahoo confirms huge data breach, affecting at least 500 million accounts
  - http://www.cnbc.com/2016/09/22/yahoo-confirms-huge-data-breach-affecting-at-least-500-million-accounts.html

- The good news: Yahoo! was using the very strong BCRYPT PBKDF.

- The bad news: The wording in Yahoo's announcement suggests that most, but not all, passwords were hashed with bcrypt. We don't know how many passwords were hashed with another algorithm, nor which one it was. The fact that this was not specified in Yahoo's announcement or FAQ suggests that it's an algorithm that's weaker than bcrypt and that the company didn't want to give away that information to attackers.

- Since there's no way to tell if your account was among those whose passwords were hashed with bcrypt or not, the safest option at this point is to consider your email compromised and to do as much as damage control as possible.

- (We've cover situations where old algorithms were never retired, older vulnerable hashes remained present for backward compatibility, and the newer stronger algorithms were used only for new accounts.)

- (((Note: How does a provider migrate from old to new?)))

Elcomsoft discovers a Severe' Security Flaw in iOS 10

- https://motherboard.vice.com/read/the-new-ios-has-a-critical-security-flaw-says-iphone-cracking-company-1
- Oleg Afonin, a security researcher at Elcomsoft, discovered that a flaw in the password hashing used to protect iOS 10's backups was suddenly 2500 times easier to brute-force.

- He "irresponsibly disclosed" his discovery publicly without first notifying Apple.
    - (Though Elcomsoft's business is selling their iPhone penetrating capabilities.)

- Apple has acknowledged the problem.

- <Oleg quote> When working on an iOS 10 update for Elcomsoft Phone Breaker, we discovered an alternative password verification mechanism added to iOS 10 backups. We looked into it, and found out that the new mechanism skips certain security checks, allowing us to try passwords approximately 2500 times faster compared to the old mechanism used in iOS 9 and older.

  This new vector of attack is specific to password-protected local backups produced by iOS 10 devices. The attack itself is only available for iOS 10 backups. Interestingly, the 'new' password verification method exists in parallel with the 'old' method, which continues to work with the same slow speeds as before.

  By exploiting the new password verification mechanism, we were able to support it in our latest update, Elcomsoft Phone Breaker 6.10. Since this is all too new, there is no GPU acceleration support for the new attack. However, even without GPU acceleration the new method works 40 times faster compared to the old method *with* GPU acceleration.

  This is extra-troublesome because decrypting a backup is currently the only way of cracking modern non-jailbroken phones. And even a jailbreak will not expose the Keychain's protections... but decrypting a back WILL. So within the iPhone cracking/break-in community, backup decryption is the golden goose.

    - iOS 9 (CPU): 2,400 passwords per second (Intel i5)
    - iOS 9 (GPU): 150,000 passwords per second (NVIDIA GTX 1080)
    - iOS 10 (CPU): 6,000,000 passwords per second (Intel i5)

Teen Hacker Jailbroke The iPhone 7 in Just 24 Hours (after he finished his homework)

- https://motherboard.vice.com/read/iphone-7-jailbreak

- Household priorities:
  - Parents: “Now Luca… you can crack your new iPhone 7 AFTER you’ve finished your homework.”
  - Luca: “But Mom!... a new crack is worth up to $200,000!”
  - Parents: “That’s nice, dear, but geography is important too! You need to know where Aleppo is, if you’re going to be President someday.”

- Within 24 hours of obtaining his iPhone 7, Luca Todesco, took advantage of a series of bugs he found and exploited to accomplish the first reported Jailbreak of an iPhone 7.

- While Luca has not disclosed any details, no one doubts his claim given his reputation and track record of previous successful hacks.

- Luca did say that the iPhone 7 is tighter and more secure and made his job harder, but still not yet impossible.

Remove software related to the Windows 10 free upgrade offer

- https://support.microsoft.com/en-us/kb/3184143
- KB3184143
- About this update:
  This update removes the Get Windows 10 app and other software related to the Windows 10 free upgrade offer that expired on July 29, 2016. For a complete list of the software removed by this Windows Update, see the update replacement information.
- Four versions, for Win7 and 8.1 in both 32- and 64-bit flavors.

OpenSSL Security Advisory [22 Sep 2016]

- OCSP Status Request extension unbounded memory growth (CVE-2016-6304)
- In brief: This is a server-side vulnerability where a malicious client can successfully leverage an edge-case in OpenSSL to bring down a remote server by causing OpenSSL to consume all of the server's memory. In TLS connection setup, clients can request "stapled" OCSP status from the server.

- https://www.openssl.org/news/secadv/20160922.txt
  - <quote> A malicious client can send an excessively large OCSP Status Request extension. If that client continually requests renegotiation, sending a large OCSP Status Request extension each time, then there will be unbounded memory growth on the server. This will eventually lead to a Denial Of Service attack through memory exhaustion. Servers with a default configuration are vulnerable even if they do not support OCSP. Builds using the "no-ocsp" build time option are not affected.

- Servers using OpenSSL versions prior to 1.0.1g are not vulnerable in their default configuration, but only if an application explicitly enables OCSP stapling support.
  - OpenSSL 1.1.0 users should upgrade to 1.1.0a
  - OpenSSL 1.0.2 users should upgrade to 1.0.2i
  - OpenSSL 1.0.1 users should upgrade to 1.0.1u

WoSign and StartCom

- https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/NAH6NVf3JPI

- via Vincent Lynch (@vtlynch) // Involved in and follows the CA industry closely:
  Vincent: "Mozilla now believes that StartCom purposefully backdated an SHA-1 certificate for a payment processing company -- a flagrant violation."

- Mozilla: Today, Mozilla is publishing an additional document containing further research into the back-dating of SHA-1 certificates, in violation of the CAB Forum Baseline Requirements, to avoid browser blocks. It also contains some conclusions we have drawn from the recent investigations, and a proposal for discussion regarding the action that Mozilla's root program should take in response.

  Mozilla: Taking into account all of the issues listed above, Mozilla's CA team has lost confidence in the ability of WoSign/StartCom to faithfully and competently discharge the functions of a CA. Therefore, we propose that, starting on a date to be determined in the near future, Mozilla products will no longer trust newly-issued certificates issued by either of these two CA brands.

  We plan to distrust only newly-issued certificates to try and reduce the impact on web users, as both of these CA brands have substantial outstanding certificate corpuses.

Bittorrent Sync, renamed to: Resilio

- https://www.resilio.com/docs/Resilio_Sync_Security_and_Privacy_Brief.pdf
- Title: "Sync / Security & Privacy Brief"
- "Inofficial Protocol Specification" (July 2013)
  - https://forum.resilio.com/topic/21338-inofficial-protocol-specification/

Errata

- Ben Yanke (@musicasacra62) / 9/21/16, 7:11 AM
  @SGgrc fyi: the ubiquity router is actually Debian based.
- (((Note))): I misspoke and said that pfSense and the Ubiquity router were both FreeBSD.

Miscellany

- "Timeless" / NBC / October 3rd
  When a mysterious criminal steals a secret state-of-the-art time machine, planning to use it to change past events to destroy America in the present, the only hope is a team of unexpected heroes composed of a scientist, a soldier and a history professor. The trio must use the stolen machine's prototype to journey back in time to critical events, being careful not to affect history themselves, while working to stay one step ahead of the villain who would unravel the timeline and understand the mystery driving his mission before it's too late.

- "The Strain" -- now in season #3. (Previous seasons on Hulu and… elsewhere.)

SpinRite

Anthony Cunningham (@kaylore92)
Hi Steve. As I listened to last weeks Security Now, Father Robert made a comment that I thought I might be able to help with, plus it would work as a SpinRite story.

Close to the end of the podcast, he mentioned he wished you could get SpinRite to work on cell phones, and I would like to note that that request might be possible already. A previous SpinRite testimonial talked about using it on a virtual machine to do multiple runs at the same time. At the time that got me to try it... and what do you know it worked! I also used it on a live Linux USB distro that was at the time not working right and it fixed that as well. Recently the cell phone I use at work as my podcast/streaming player was getting rather slow and laggy, so I thought "what the heck I'll try SpinRite on it!" and see what happens.

Using Virtual Box on Linux, I plugged in the phone to the USB, had Virtual Box set it as a raw disk, spun up a VM with SpinRite and pointed it at the cell phone. SpinRite did it's thing, and about an hour later it was done, I unplugged the phone, rebooted it, and after that it was running faster and more stable than it had for over a year! I thought to myself this was great, I'll try it on my Nexus 5 next, but that unfortunately was a no go. The phone must be able to be seen as a mass storage device in order to be used as a raw disk in VirtualBox, and for some reason the Nexus 5 will only read as a non-mass storage USB device.

I hope Father Robert can try this out and see if it helps.

~ EOF ~