Security Now! #529 - 10-13-15

Q&A #220

This week on Security Now!

- Joe Siegrist and the LastPass acquisition
- Patch Tuesday
- Another dent in SHA-1
- CAB forum wants to extend SHA-1 for another year.
- US Government plans not to force "cryptotapping"... for now.
- A comment Edward Snowden posted on Reddit 4 months ago.

Security News:

LastPass is purchased by LogMeIn

Considerations for our interview with Joe Siegrist, founder and CEO of LogMeIn:

- Our password repository is THE most precious and sensitive information we have.
- There's probably nothing more crucial in today's online world.
- Trusting all of our logon passwords to a 3rd-party, ANY 3rd-party, is a HUGE DEAL.
- So here's the problem:
- LogMeIn has a highly blemished reputation… and reputation is everything.
    - LogMeIn's Facebook Post: June 23, 2011 @ 1:44pm
      We receive a lot of messages thanking us for making LogMeIn Free, well, free. Let's make this official: there's no need to thank us. LogMeIn Free is and will always be free. For today, you can just pay us in "Likes."
    - January 21st, 2014: "Changes to LogMeIn Free"
      http://blog.logmein.com/it-management/logmein-changes
      After ten years, LogMeIn's free remote access product, LogMeIn Free, is going away. We will be unifying our portfolio of free and premium remote access products into a single offering. This product will be a paid-only offering, [...]
- Our experience with Hamachi after LogMeIn acquired them.
    - (Not good)
    - Now… a "free trial" with no documentation about what "trial" means.
- LogMeIn aside... we like LastPass ***just the way it is.***
    - This acquisition may benefit LastPass (and bravo for them, really)... but in what possible way does this truly benefit LastPass users?
    - If history is any lesson (and it's all we have to go on) LogMeIn will, in time, ruin LastPass and work to leverage/monetize/corporatize their $110M purchase.
    - So this changes things... and in password management ANY CHANGE is frightening.
- … And what the hell is "Meldium"

Patch Tuesday...

- Six patch bundles
  - Three Critical & three important

- Toolbar use-after-free vulnerability
  - All supported versions of Windows

- Security Update for JScript and VBScript to Address Remote Code Execution (3089659)
  - ONLY Vista & Windows Server 2008

  - This security update resolves vulnerabilities in the VBScript and JScript scripting engines in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if an attacker hosts a specially crafted website that is designed to exploit the vulnerabilities through Internet Explorer (or leverages a compromised website or a website that accepts or hosts user-provided content or advertisements) and then convinces a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that uses the IE rendering engine to direct the user to the specially crafted website.

    An attacker who successfully exploited the vulnerabilities could gain the same user rights as the current user and, if the current user is logged on with administrative user rights, the attacker could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

    This security update is rated Critical for affected versions of the JScript and VBScript scripting engines on supported editions of Windows Vista, Windows Server 2008, and Server Core installations of Windows Server 2008 R2. For more information, see the Affected Software section.

    The update addresses the vulnerabilities by modifying how the VBScript and JScript scripting engines handle objects in memory, and helping to ensure that affected versions of VBScript properly implement the ASLR security feature. For more information about the vulnerabilities, see the Vulnerability Information section.

1Blocker v1.1

- Site Whitelisting
  - The BEST whitelisting of any app, since we have full visibility and auditing
- Blocks annoying EU cookie-using notices.
- Improved reduced-confusion user-interface.

(Rene: Tweetbot v4 -- Oh Thank GOD! Totally agree!!)

SHA-1 "Freestart" Collisions

- http://arstechnica.co.uk/security/2015/10/sha1-crypto-algorithm-securing-internet-could-break-by-years-end/
- The SHAppening: freestart collisions for SHA-1
- A full, successful, 80-round collision created in the SHA-1 Compression function.
- Processing power increased at a faster rate than we expected.
- A 64 GPU cluster was able to calculate a compression function collision in 10 days.
- A FULL SHA-1 collision would allow signature spoofing of SHA-1 certs.

Should we keep issuing new SHA-1 certificates?

CAB Forum Ballot to extend issuance of SHA-1 Certs through 2016 (though expiring at end of 2016)
https://cabforum.org/pipermail/public/2015-October/006048.html
Ballot 152 - Issuance of SHA-1 certificates through 2016

The following motion has been proposed by Rick Andrews of Symantec and endorsed by Bruce Morton of Entrust, Jody Cloutier of Microsoft, and Kirk Hall of Trend Micro.

-- MOTION BEGINS -

1) Modify section 7.1.3 of Baseline Requirements as follows:

The purpose of the ballot is to allow the issuance of SHA-1 certificates through 2016, with maximum Expiry Date of 31 December 2016. Although the vast majority of customers have been able or will be able to transition to SHA-2 certificates by the issuance termination date of 31 December 2015, a very small number of very large enterprise customers have disclosed to us that they simply cannot complete this work before the issuance deadline. This is attributed to the sheer volume of certificates that they need to migrate (numbering in the thousands), and their end-of-year blackout period. These customers accept the risk of continuing to use new SHA-1 certificates, and assert that if they can continue to enroll for and receive SHA-1 certificates through 2016 (all with an expiration date of 31 December 2016 or earlier), they will be able to complete the transition by the end of 2016.

We realize that extending the issuance period will extend the collision attack period. Although we feel that the BRs [Baseline Requirements] already mandate enough entropy (typically in the certificate serial number) to guard against that attack, it can be further mitigated by limiting SHA-1 certificate issuance to Subordinate CAs that have a basicConstraints pathLength = 0.

The intent of the ballot is to allow limited issuance of SHA-1 certificates through 2016, as long as any SHA-1 certificate created in 2016 expires by the end of 2016. We also correct the number of the Section number in the body of the Section (which incorrectly references “Section 9.4.2” - that mistake was probably made in the conversion to RFC 3647 format).
Ballot was posted to the CAB mailing list on Friday, October 2nd.
Voting on this motion closes on Friday, October 16th.

Obama administration opts not to force firms to decrypt data — for now

- https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html?postshare=8201444416293020
- http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html?smid=tw-share&_r=0
- New York Times, NICOLE PERLROTH and DAVID E. SANGER:
  The Obama administration has backed down in its bitter dispute with Silicon Valley over the encryption of data on iPhones and other digital devices, concluding that it is not possible to give American law enforcement and intelligence agencies access to that information without also creating an opening that China, Russia, cybercriminals and terrorists could exploit.

  With its decision, which angered the F.B.I. and other law enforcement agencies, the administration essentially agreed with Apple, Google, Microsoft and a group of the nation's top cryptographers and computer scientists that millions of Americans would be vulnerable to hacking if technology firms and smartphone manufacturers were required to provide the government with "back doors," or access to their source code and encryption keys.

  Security Now's take: ... and even if they did, it wouldn't matter, since strong and unbreakable encryption is already and will always be freely available. It's just math. It's loose. It's too late. even if it were outlawed, bad guys will always be able to use it if they wish.

Another way to look at Privacy:

- https://www.privacytools.io/
- Of the whole "I'm not overly concerned about privacy because I have nothing to hide..."
- Snowden, about 4 months ago wrote on Reddit:
  "[...] I think the central issue is to point out that regardless of the results, the ends (preventing a crime) do not justify the means (violating the rights of the millions whose private records are unconstitutionally seized and analyzed).

  "Some might say "I don't care if they violate my privacy; I've got nothing to hide." Help them understand that they are misunderstanding the fundamental nature of human rights. Nobody needs to justify why they "need" a right: the burden of justification falls on the one seeking to infringe upon the right. But even if they did, you can't give away the rights of others because they're not useful to you. More simply, the majority cannot vote away the natural rights of the minority.

  "But even if they could, help them think for a moment about what they're saying. Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.

  "A free press benefits more than just those who read the paper."

- Again: “Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.”

SpinRite:

David in Montreal, Quebec wonders whether Steve uses SpinRite himself?

Hi Steve & Leo,

I know that your backup strategy is very good, but have you had a situation where you had to use your own product for maintenance or to recuperate data for any reason? How many times over the years?

Thank you and keep up the good work.
(You can use this question on Security Now)