

Security Now! #457 - 05-27-14

Q&A #188

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!

- Industry veteran and ISP, Brett Glass, joins us to discuss Net Neutrality,
- A nifty WinXP hack to continue receiving security updates,
- eBay joins the ranks of those who have had their user database stolen,
- A couple of Apple security Woes,
- SQRL progress report...
- and Questions from our listeners

Security News:

Get WinXP updates through 2019 with Simple registry hack

- First heard from Matt Graham
- <http://www.grahamlabs.com/2014/05/embedded-saves-day.html>
- <http://www.zdnet.com/registry-hack-enables-continued-updates-for-windows-xp-7000029851/>
- <http://betanews.com/2014/05/26/how-to-continue-getting-free-security-updates-for-windows-xp-until-2019/>
- Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\WPA\PosReady]
"Installed"=dword:00000001

eBay loses control of its user password database (Last Wednesday)

<https://blog.ebay.com/ebay-inc-ask-ebay-users-change-passwords/>

<http://www.cnet.com/news/ebay-hacked-requests-all-users-change-passwords/>

eBay said:

- The database was compromised in late February and early March,
- Held eBay customer's names, encrypted passwords, email addresses, physical addresses, phone numbers, and dates of birth.
- However, users' financial information was not accessed.
- The company narrowed down the attack to "a small number of employee login credentials" stolen by cyberattackers, which it said provided access to eBay's corporate network.
- NO EVIDENCE that any of the stolen data has been used.

Apple iCloud hack?

- Hacker "Oleg Pliss" is demanding \$100 to unlock locked iPhones, iPads and Macs.
- Primarily in Australia, but some reports from Briton.
- Ransoms between \$50 and \$100 sent to a Paypal account: lock404(at)hotmail.com.
- Passcode is added to the device, preventing them from getting back in.
- Users who already have a passcode can restore from an iTunes backup.
- No solution, though, if no passcode on phone prior to the attack.

Apple's OS X - Whoops! Expired security cert.

- http://www.macworld.com/article/2158788/apple-neglects-to-renew-ssl-certificate-breakeks-software-update-in-the-process.html#tk.rss_all
- "swscan.apple.com"
- <http://www.digicert.com/help/>
- Valid from 25/May/2014 to 24/May/2016

SQLR:

- The need for secure storage.
- Philip Rogaway's OCB (AEAD - Authenticated Encryption with Associated Data) mode implemented.
- SQLR's Secure Storage System redesigned, implementation is next.

SpinRite:

From: "Matt"

Date: Sun, 25 May 2014 23:23:54 -0000

To: Security Now Feedback

Subject: SpinRite Saves the Day

X-Location: Waterloo, Ontario

Hi Steve,

I'm a fourth year Computer Engineering student at the University of Waterloo and SpinRite recently saved my team and me 100's of hours of work. During fourth year, we have to come up with a design project that showcases what we have learned throughout our degree. My team had worked for over a year on our project, and had most of it stored on one member's Lenovo laptop. Three days before the project was due, his computer would no longer boot. We hadn't backed the project up in over a week, so it was critical that we got our data back. Since the system wouldn't boot, we tried putting the hard drive in an external enclosure to recover just the data. But the drive wouldn't mount on any of our systems. Desperate, I remembered that I had purchased a copy of SpinRite a few years back and had it burned on a CD at my apartment. I raced home to get the CD, and popped it into the laptop. 16 hours later, SpinRite had fixed and recovered the data in more than 50 bad sectors and we were able to pull the data we needed from the drive. Thanks for your hard work and for the excellent podcast.

-Matt

More Harry's Feedback:

- Brandon (@BScottX)
Reposting my @harrys recommendation. Best shave ever and better prices. Glad to see they're now sponsoring Security Now w/@SGgrc on @TWiT!
- Others have reported similar amazement and still others have reported ordering.