Security Now! #449 - 04-01-14

Q&A #185

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!

- The NSA / Dual_EC_DRBG flaw is worse than we knew.
- Is Google's Always HTTPS for Gmail a bad thing?
- A quick WiFi password install for iPhones.
- The Collapse in Cloud Storage pricing.
- Advertising in Firefox?
- Miscellany, SQRL, SpinRite and
- 11 Listener and Follower questions.

Security News:

Reuters: "Exclusive: NSA infiltrated RSA security more deeply than thought"

- http://www.reuters.com/article/2014/03/31/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331
- More about the Dual_EC_DRBG: http://dualec.org/
- ***Summary of the results:*** The researchers analyzed the use of Dual EC in four recent TLS/SSL library implementations: RSA BSAFE Share for C/C++, RSA BSAFE Share for Java, Microsoft SChannel, and OpenSSL. The major findings are as follows:
    - The RSA BSAFE implementations of TLS make the Dual EC back door particularly easy to exploit compared to the other libraries analyzed. The C version of BSAFE makes a drastic speedup in the attack possible by broadcasting long contiguous strings of random bytes and by caching the output from each generator call. The Java version of BSAFE includes fingerprints in connections, making it relatively easy to identify them in a stream of network traffic.
    - SChannel does not implement the current Dual EC standard: it omits one step of the Dual EC algorithm. This omission does not prevent attacks; in fact, it makes them slightly faster.
    - A previously unknown bug was discovered in OpenSSL that prevented the library from running when Dual EC is enabled. It is still conceivable that someone is using Dual EC in OpenSSL, since the bug has an obvious and very easy fix which was applied in order to evaluate the resulting version of OpenSSL, which the paper calls "OpenSSL-fixed." OpenSSL-fixed turns out to provide additional entropy ("additional input") with each call to the library. In practice, this additional input can make attacks significantly more expensive than for the other libraries.

- **ALSO...** Evidence of an implementation of a non-standard TLS extension called "Extended Random" was discovered in the RSA BSAFE products. This extension, co-written at the request of the National Security Agency, allows a client to request longer TLS random nonces from the server, a feature that, if it enabled, would speed up the Dual EC attack by a factor of up to 65,000.
- Extended Random?
    - http://tools.ietf.org/html/draft-rescorla-tls-extended-random-00
    - The United States Department of Defense has requested a TLS mode which allows the use of longer public randomness values for use with high security level cipher suites like those specified in Suite B [I-D.rescorla-tls-suiteb]. The rationale for this as stated by DoD is that the public randomness for each side should be at least twice as long as the security level for cryptographic parity, which makes the 224 bits of randomness provided by the current TLS random values insufficient.

      This document specifies an extension which allows for additional randomness to be exchanged in the Hello messages.

Google forcing TLS a bad thing?

- Robert L. Mitchell / ComputerWorld / "Reality Check" column...
- "Google to Gmail customers: You WILL use HTTPS"
- http://blogs.computerworld.com/privacy/23698/google-customers-you-will-use-https
- Claims that "user choice" is being removed.
- Claims that response time is hindered.
- (And he got a good deal of flack from that odd column.)

Auto-WiFi-Config

- Karl Kornel (@californiaKARL)
- Karl's Config: https://www.dropbox.com/s/atpas6tvgoetjt4/example.mobileconfig.txt
- Apple's Utilities: http://support.apple.com/downloads/#iphone%20configuration%20utility
- https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html

Other's follow Google's cloud pricing reductions

- Amazon, and now Microsoft
- http://techcrunch.com/2014/03/31/microsoft-azure-matches-amazons-price-cuts-and-introduces-new-basic-tier/
- Microsoft matched Amazon's cuts and in some cases undercuts.

Firefox to add advertising?

- http://www.zdnet.com/mozilla-clarifies-defends-firefox-ad-position-7000026335/
- "Mitchell Baker, chair of the Mozilla Foundation, defends Firefox's new ad program. Firefox users remain wary."
- Nine large tiles on a New Tab's page.
- Two of the nine, for example, might be sponsored.
- But NO TRACKING.
- <Previous ZDNet quote> True, Mozilla needs funds. At the moment, Mozilla is largely dependent on Google for its income. Mozilla's $300 million/year deal with Google is up for renewal in December 2014. Last time the extension didn't happen until the last minute. Perhaps Mozilla is preparing for a future without Google's partnership.

"Why Windows XP's Demise is Bad for Linux and Open Source"

- http://thevarguy.com/open-source-application-software-companies/033114/why-windows-xps-demise-bad-linux-and-open-source
- He says that he runs XP in a VirtualBox VM on Linux for:
  - Editing large book manuscripts that cause LibreOffice to collapse.
  - Playing "Age of Kings"
- WinXP is SO MUCH LEANER than Vista/7/8 that moving up will be impossible.

Miscellany

Neil Young's ultra-high-resolution music player passes $5 Million

http://techcrunch.com/2014/03/29/neil-youngs-ponoplayer-passes-5m-in-kickstarter-pledges/
https://www.kickstarter.com/projects/1003614822/ponomusic-where-your-soul-rediscovers-music?ref=most_funded
$800,000… but now have $5,218,872 pledged with 14 days to go
192 kHz at 24 bits. -- what does Andy say about the idea??
Is it worth it?
http://people.xiph.org/~xiphmont/demo/neil-young.html

Typo keyboard injunction granted.

- (Hardly surprising since the design IS a direct ripoff of BlackBerry.)
- In the United States, a design patent is a form of legal protection granted to the ornamental design of a functional item. Design patents are a type of industrial design right.
- A US design patent covers the ornamental design for an object having practical utility. An object with a design that is substantially similar to the design claimed in a design patent cannot be made, used, copied or imported into the United States. The copy does not have to be exact for the patent to be infringed. It only has to be substantially similar.

SQRL Update

- 51 languages registered for translation
- Indonesian just requested... that'll give us 52.
- UI is coming to life...

SpinRite Success Story

Andreas in Sweden
Subject: SpinRite testimonial
Date: 18 Mar 2014 05:55:42
:
Hi Steve (and Leo)

I like to thank you for Spinrite. A while back my MacBook Pro would not boot up. The funny thing is that I rarely shut down my computer at the end of the day, I usually just put it to sleep. But on this occasion I did shut it down. As I did, it hit me that my last backup was a couple of days ago and I had some files which had not been backed up. But I brushed it off, thinking I could back up these files once I start my computer the next day... and what can go wrong? it will not be any problem. Boy was I wrong. When I came back and tried to start my computer it would not boot up into OS X. How hard I tried with recovery disks and other tools but nothing would help. I was able to boot into my Windows partition, so I knew that something was wrong with my OS X partition. In windows, I was able to purchase and download SpinRite immediately from you, though sitting on the edge of my seat, hoping my windows partition would not crash as well. With some tinkering, I got SpinRite going. Once it had finished, my Mac would boot up like nothing had happened, working faster and smoother than before. I was able to back up all my files and just to be safe I bought and installed a new SSD. So big thanks for saving my files!

Best Regards
Andreas