Security Now! #461 - 06-24-14

Q&A #190

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 return of Open Wireless??
- "YAFOOSL" stands for "Yet ANOTHER Fork of Open SSL"
- Apple cautiously inching TouchID forward
- Guess who's going to start selling domain names?
- Positive legislative noises about patent and NSA surveillance
- Miscellaneous hi-jinx and updates,
- And 10 questions and answers

Security News:

OpenWireless.org (registered in 2011 by the EFF)

- TheRegister.Co.Uk
  - http://www.theregister.co.uk/2014/06/24/open_your_wifi_to_improve_privacy/
  - Headline: "EFF wants you to open your Wi-Fi to IMPROVE privacy"
  - The Electronic Frontier Foundation (EFF) wants internet users to go back to the turn of the century and open their wireless networks for anyone to connect, in order to enhance privacy. The EFF wants us all to use the OpenWireless initiative's free router firmware, which allows users to create open guest networks that anyone in range can use.

- EFF: "Open Wireless"
  https://www.eff.org/issues/open-wireless
  <"> Imagine being able to walk around any street in any city and never worrying about checking an email, downloading a map, making a video call, or streaming a song. EFF believes that open wireless networks greatly contribute to the public good.

  Computer users, worried about privacy or security risks, have largely taken the default route of closing down their networks. Though the willingness to operate in a secure environment is understandable, the issue is that modern encryption systems make open sharing with friends, family, and passersby very difficult.

  In order to promote beneficial uses of the Internet in all walks of life, EFF and a coalition of organizations are launching the Open Wireless Movement. We are working on new

technologies and best practices that will allow individuals, businesses, and community organizations to open up their wireless networks—while not sacrificing privacy, security, and quality.

Opening one's wireless is a neighborly act that should be supported by router manufacturers, Internet Service Providers, and legal systems. There have been cases where individuals running open networks were wrongfully raided for one of their guests' wrong actions, but these cases are highly exceptional. We believe that individuals hosting networks should gain the same protections as service providers, especially since Open Wireless services are becoming ubiquitous. More and more cafes, airports, libraries, schools, and individuals happily share their networks with customers and passersby. We encourage Internet Service Providers to not have blanket prohibitions of Open Wireless in their terms of service, and we think business models could be built off of letting customers run open nodes.

Open Wireless also helps conserve radio spectrum. It turns out that wireless networks (e.g. 802.11) operate much more efficiently than cell phone towers. Because wireless systems are connected to a much more distributed system of routers, many more devices can operate on the same frequency.

If you wish to find out more about Open Wireless, go to https://openwireless.org. If you are a technologist or company that would like to get involved with the movement, email openwireless@eff.org.

- Details:
    - Pros & Cons:
        - Many (but not all) ISP end-user agreements specifically forbid offering open WiFi.
        - Until this becomes the norm, IP-targeting will still be used.
        - Comcast's user-hotspots make IP-targeting increasingly less useful
    - "openwireless.org" <--- SSID
    - https://www.eff.org/deeplinks/2014/05/open-wifi-not-copycrime-effs-primer-open-wifi-and-copyright
    - Open Wi-Fi and Copyright: (May 23, 2014)
        - https://www.eff.org/files/2014/05/28/open-wifi-copyright_0.pdf
    - Uses EAP-TLS for encryption, which requires a client certificate.
        - EFF bundles a server cert into their firmware.
        - EAP-TLS enjoys VERY wide support

TouchID Inches forward

- http://bgr.com/2014/06/23/iphone-6-ipad-air-2-ipad-mini-3/
- Based upon leaks of TouchID sensor orders from China...
- Devices expected to be announced later in 2014 - new iPhone 6's, iPad AIR and iPad Mini are ALL expected to be incorporating TouchID.
- One SQRL developer indicated that the TouchID API is a Binary go/no-go indication:
- Application requests a real time prompt to confirm the user's TouchID identity.
- System replies with an indication of success or failure.

Adam Langley Forks OpenSSL:

- https://www.imperialviolet.org/2014/06/20/boringssl.html (Friday)
- Tentatively named: "BoringSSL" ??
- <"> Earlier this year, before Apple had too many goto fails and GnuTLS had too few, before everyone learnt that TLS heart-beat messages were a thing and that some bugs are really old, I started a tidy up of the OpenSSL code that we use at Google.

  We have used a number of patches on top of OpenSSL for many years. Some of them have been accepted into the main OpenSSL repository, but many of them don't mesh with OpenSSL's guarantee of API and ABI stability and many of them are a little too experimental.

  But as Android, Chrome and other products have started to need some subset of these patches, things have grown very complex. The effort involved in keeping all these patches (and there are more than 70 at the moment) straight across multiple code bases is getting to be too much.

  So we're switching models to one where we import changes from OpenSSL rather than rebasing on top of them. The result of that will start to appear in the Chromium repository soon and, over time, we hope to use it in Android and internally too.

  There are no guarantees of API or ABI stability with this code: we are not aiming to replace OpenSSL as an open-source project. We will still be sending them bug fixes when we find them and we will be importing changes from upstream. Also, we will still be funding the Core Infrastructure Initiative and the OpenBSD Foundation.

  But we'll also be more able to import changes from LibreSSL and they are welcome to take changes from us.

  (Note: the name is aspirational and not yet a promise.)

- https://boringssl.googlesource.com/boringssl/
  - Looking at the changelog... Adam is doing serious work on "BoringSSL"

Google to start offering Domains

- https://domains.google.com/about/
- <">A domain name, your address on the Internet, says a lot about who you are and what you do. New domain endings like .guru and .photography can help you find a meaningful address that stands out on the web. Every domain includes easy forwarding, branded email (you@your_company.com), simple management tools and other helpful features.</">
- Features:
  - https://domains.google.com/about/features.html
  - No additional cost for private registration
  - "Branded eMails" -- up to 100 eMail aliases on your domain
  - Domain forwarding
  - Up to 100 subdomains

- Use of Google's infrastructure
- Simple domain management tools (sample screenshot shows 1-year for $12)
- Integration with top website building tools
- Availability of new domain endings:
- .guru / .photography / etc.

Legislation Watch -- the NSA and Patents... (First, the NSA...)

- https://www.eff.org/deeplinks/2014/06/eff-statement-massie-lofgren-amendment-passing-house
- [Last Thursday] the US House of Representatives passed an amendment to the Defense Appropriations bill which cuts funding for NSA backdoors and "backdoor searches."

  The amendment passed overwhelmingly with votes from both sides of the aisle: 293 ayes, 123 nays, and 1 present.

  As it is now, the NSA collects emails, browsing and chat history under Section 702 of FISA, searching through these communications of Americans without a warrant. This practice has become known as "backdoor searches." The amendment which passed would block the NSA from using any of its funding from this Defense Appropriations Bill to conduct such warrantless searches.

  Secondly, the amendment prohibits the NSA from using its budget to mandate or request that private companies and organizations add backdoors to the encryption standards that are meant to protect users' privacy on the web.

Patent Watch:

- One of the most closely watched cases this year in front of the Supreme Court was UNANIMOUSLY decided.
- Australia-based Alice Corp. vs CLS Bank
- Alice Corp. had previously obtained a patent on how to display funds held in escrow by an intermediary...
- Alice Corp. had charged CLS Bank with patent infringement.
- CLS Bank wanted the patent overturned.
- It went all the way to the Supreme Court.
- Thursday, the Supreme Court ruled that (as the Washington Post nicely summed it up), "running a concept through a computer doesn't merit a patent."
- If it DID merit a patent, as Justice Clarence Thomas wrote, "an applicant could stake a claim to any principle of the physical or social sciences by reciting a computer system configured to implement the relevant concept.
- The overarching point was: Alice didn't "invent" anything. They obtained a patent by showing how to use a computer to implement an "escrow" in the real world. THEY ADDED NOTHING other than "do it with a computer."
- The disappointing news... we got ZERO useful new tests or thinking about software patents, as has been long hoped for. Writing for the court, Clarence Thomas explicitly said that he didn't need to deal with the abstract-idea problem, because the facts of the case were so obviously against the company with the bad patents.

Hack of the Week:

- "rothgar" @rothgar
    - @SGgrc a cool story about Google's use of the 95/5 rule j.mp/1yjedJo
      If the link doesn't work find p187 from In the Plex
- Steven Levy's book: "In The Plex: How Google Thinks, Works, and Shapes Our Lives"
  <quote> Back in 2000, Google wanted to get speedier by setting up data centers in locations closer to its users. Its first priority was getting servers on the East Coast of the United States. By the spring of that year, Gogle was occupying space in a colo in North Virginia. The tricky part of setting up in a new facility was loading all those thousands of servers with the indexes. That involved terabytes of data, which was potentially going to force Google to pay a huge amount of money to the bandwidth provider that owned the fiber. "Networking was very expensive," Holzle, "And our data push would take twenty hours at a gigabyte per second--that would cost us something like $250,000 a month." To save money, Google deviced a trick that exploited a loophole in the billing system known as the 95th Percentile Rule. Over the period of a month, the provider would measure how much information was moving, automatically taking a measurement every five minutes. In order to discard unusual spikes in activity, when the billing rate was calculated the provider would lop off the measurements in the top five perceniles and bill the customer at the rate of the 95th percentile.

  Google's exploitation of the rule was like the correct answer to a trick question in one of its hiring interviews. It decided to squeeze the movement of all of its information into those discounted spikes. "We figuredd our that if we used zero bandwidth all month, except for 30 hours once a month, we would be under that 5 percent", says Reese. For two nights a month, from 6pm to 6am Pacific time, Google moved all the data in its indexes from West to East. "We would push as fast as we could, and that would cause massive traffic to go across, but it was during the lull hours for them... And, of course, the bill came out to be nothing.", say Reese, "because then they lopped off the top 5 percent, our remaining bandwidth was in fact zero... because we didn't use any otherwise. I literally turned off the router ports for twenty-eight or twenty-nine days per month." </quote>

Errata:

- **Adam Ross @ross549**
  @SGgrc a small point which makes a big difference. Ghash.io is a commercial entity that rents hashing time on their equipment, not a pool.
- **Federico Bett @fede_cba**
  @SGgrc just writing to let you know that you have some listeners from Argentina. Keep up the good work! Regards from Córdoba, Argentina.
- **Chelsea Handler, moves from 'E!' to Netflix.**
  TechCrunch writes: "Netflix has just announced an exclusive deal with the beautiful and brilliant Chelsea Handler for an upcoming series of talk show programming featuring the comedienne herself. Both the network and Handler are keeping mum about how the show will be formatted, but they did explicitly state that it will "still encompass Chelsea's unfiltered opinions on topical entertainment and cultural issues, as well as her signature guest interviews."

Media Update:

- "The Last Ship" was *amazing*
- TNT, Sundays -- Pilot is re-airing this week
- The Last Ship is a 1988 post-apocalyptic fiction novel written by William Brinkley. A television series based on the novel premiered on June 22, 2014, on TNT.

SQRL:

- http://translate.grc.com/ --> Crowdin.Net/projects/sqrl
- 405 translators, 57 languages

SpinRite:

From: "Sean Zicari"
Subject: SpinRite success story - Recovery is a dish best served cold
Date: Mon, 23 Jun 2014 17:15:47 -0000

Hi Steve!

I wanted to share a success story through unexpected means. First off, I've been listening to the podcast for a couple of years now and am a big fan blah blah blah (in honor of how Leo normally reads those sentences). Seriously though, I love the podcast and really appreciate your expertise.

My friend called and asked advice about recovering data from the hard drive in his PowerMac G4. He's had the computer for years and has never performed maintenance on it to my knowledge. He said the computer wouldn't boot anymore, so he took it to a drive recovery specialist. After recovering from the quoted price, he called me for a second opinion. I thought this was the *perfect* chance to try SpinRite, so I said I would fix the drive for him for the cost of the SpinRite license (win-win!). He agreed and mailed the drive to me.

I ran SpinRite on level 2 first. That completed successfully. I rebooted and attempted to read some data from the drive. I was able to, but it took a long time to bring up files and folders. Specifically, the drive would make a repetitive scanning noise of some sort (not sure how to describe it but guessing you know what I'm talking about). I decided to run a level 4 scan next, but throughout the process the SpinRite UI was very slow to respond and froze frequently for long periods of time while the drive made the same repetitive scanning noises mentioned previously. At .12% the UI froze entirely and the drive went silent.

Reading through the SpinRite FAQ for ideas, and with a very pessimistic eye on the situation, I decided to try the last suggestion first. I put the drive in the fridge for an hour, popped it back in the computer and started a level 4 scan again. The scan process hit .12% and the UI started to move sluggishly, but overall not as bad as before. I shut the monitor off and left it go (I was on the way out the door, anyway). When I came back 4+ hours later, the scan process was almost 50% complete and moving along steadily!

It finished late last night. I'm happy to say the drive is totally quiet again, and the data seems to

be intact. There were a couple of i/o errors in my friend's Home folder which I'm guessing may be related to trying to read an hfs+ volume in Linux, but it looked like all the important data was accessible.

Thanks again for a fantastic product!