Security Now! #452 - 04-22-14
Q&A #186

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!

- Ladar Levinson's Appeal Ruling.
- The Netgear/Cisco/Linksys/Diamond router backdoor not as tightly closed as we hoped and assumed.
- How Google could finally bring true PGP-style end-to-end encryption to the masses.
- The OpenBSD project forks the OpenSSL project.
- In the Q&A: What about Jailbreaking iOS??

Security News:

Ladar Levinson loses at appeal:

- Edward Snowden referenced "Lavabit Email"
- Ladar, forced to turn over the keys, finally printed them out on paper, complying but making them essentially useless.
- Was held in "Contempt of court."
- The US 4th Circuit Court of Appeals upheld contempt of court citations against Ladar Levison for his refusal to hand over the master encryption keys to Lavabit's email service last summer.
- CNET: Seth Rosenblatt:
    - <quote> The appellate court didn't comment on the substantive issue in the case, whether the government had the right to demand the encryption keys that would allow them to observe all traffic of a targeted email account. Instead, the appeals court ruled that the Internet privacy issues raised in Levison's appeal were not clearly articulated while he was defending himself in district court.

      The appeals court said Levison should have brought forward his claim that the government was exceeding its authority under US "pen register" and "trap and trace" statutes before being charged with contempt of court by the district judge last summer.
    - Terms:
        - "Pen Registers" record the phone numbers that call an individual.
        - "Trap & Trace" records the phone numbers that are called.

- Judge G. Steven Agee wrote for the three-judge appellate panel that the statement was legally inadequate:
    - <quote> Levison's statement to the district court simply reflected his personal angst over complying with the Pen/Trap Order, not his present appellate argument that questions whether the district court possessed the authority to act at all.

- ACLU attorney Brian Hauss said in a statement:
    - The court focused its decision on procedural aspects of the case unrelated to the merits of Lavabit's claims. On the merits, we believe it's clear that there are limits on the government's power to coerce innocent service providers into its surveillance activities. The government exceeded those limits when it asked Lavabit to blow up its business -- and undermine the encryption technology that ensures our collective cybersecurity -- to get information that Lavabit itself offered to provide.

- Ladar: "Freedom is the ability to do something that somebody else disagrees with. To make a choice that somebody else wouldn't make. The problem with disrupting our right to privacy is that at the same time we do that, we disrupt our right to free speech. And without the ability to speak freely, a democracy is no longer a democracy."

Port 32764 is back

- Eloi Vanderbeken of Synacktiv on 4/18/2014 (4 days ago)
- http://www.synacktiv.com/ressources/TCP32764_backdoor_again.pdf
- Sean Gallagher, writing for ArsTechnica:
    - The same security researcher who originally discovered a backdoor in 24 models of wireless DSL routers has found that a patch intended to fix that problem doesn’t actually get rid of the backdoor—it just conceals it. And the nature of the “fix” suggests that the backdoor, which is part of the firmware for wireless DSL routers based on technology from the Taiwanese manufacturer Sercomm, was an intentional feature to begin with.
- 24 models confirmed vulnerable: Netgear, Cisco and Linksys, and Diamond.
- 6000 vulnerable exposed routers known on the Internet.
- Patched in January
- Now:
    - Opens a raw socket and wait for Ethernet packets of Ethertype 0x8888.
        - Specifies what type of packet is encapsulated in the Ethernet packet. What it's carrying.
        - Ethertype 0x0800 is IPv4. ARP is 0x0806
    - If PAYLOAD == md5("DGN1000") and PacketType == 0x201
        - Then: system("scfgmgr -f &")
    - Also, PacketType 0x200 will ping the router, returning its MAC address.
    - And PacketType 0x202 will change its LAN IP address.
- The packet’s payload, in the version of the backdoor discovered by Vanderbecken in the firmware posted by Netgear, is an MD5 hash of the router’s model number (DGN1000).
- New commands too... to make the router's lights flash.

Google is researching ways to make encryption easier to use in Gmail

- http://venturebeat.com/2014/04/21/google-is-researching-ways-to-make-encryption-easier-to-use-in-gmail/
- <<<< Steve: Elaborate on why this is totally doable >>>>
- But... one creepy thing at the end of the article:
  - VentureBeat: "Don't expect Google to set up site-wide end-to-end encryption, however. For Google to monetize Gmail, it must be able to scan messages in order to serve targeting ads to users. It's an advertising business, after all."

The OpenBSD project has forked OpenSSL to create LibreSSL

- http://www.libressl.org/
- "At the moment we are too busy deleting and rewriting code to make a decent web page. No we don't want help making web pages, thank you."
- It's being called "The Purge"
- The "OpenSSL Valhalla Rampage"
- http://opensslrampage.org/
- <Quote from the site> "Tearing apart OpenSSL, one arcane VMS hack at a time."
- From the OpenBSD lead:
  - 90,000 lines of C code have been removed, reducing the overall line count by 150,000 lines.
  - (Some of that is just formatting consistency to make the code more understandable.)
  - 99.99% of the community does not care about OpenSSL's support for VMS (DEC/HP OS).
  - 98% do not care about Windows support.
  - They care about POSIX support... so that it can be used with Unix and Unix derivatives.
  - They don't care about FIPS compliance.
  - Even after all those changes, the codebase is still API compatible.
  - The entire OpenBSD ports tree (8700 applications) continue to compile and work, after all those changes.
  - "Pretty much no one needs to write their own 'printf' implementation."

Apple releases v7.1.1 to fix a few issues from v7.1

- Further improvements to Touch ID fingerprint recognition
- Fixes a bug that could impact keyboard responsiveness
- Fixes an issue when using Bluetooth keyboards with VoiceOver enabled

Security Funnies:

- Simon Zerafa @SimonZerafa
- @SGgrc Due to a security leak, your biometric data may have been compromised. We recommend you change your fingerprints as soon as possible.

SpinRite:

mar (@mtropyancheno) / 5:31am · 19 Apr 14 · web
@GibsonResearch Just recovered a 500Gb drive. After 28 hours working that out SPINRITE brought it back to life! Another happy customer!