Security Now! #516 - 07-14-15

SQRL Revisited

This week on Security Now!

- More Hacking Team Revelations:
  - Another Abode FLASH 0-day
  - A hacking team UEFI rootkit
- OpenSSL's latest problem
- Another plea to the government from encryption experts
- Still worse news from the OPM breach
- Some notes about Windows WiFi (non)Sense and AdBlock Plus
- Miscellaneous tidbits
- And... a look at SQRL… after 92 weeks!

SQRL's Official Logo & Icon

https://www.grc.com/sqrl/logo.htm

Security News

Another 0-Day Flash vulnerability found amid the Hacking Team's data!
https://helpx.adobe.com/security/products/flash-player/apsa15-04.html
https://www.fireeye.com/blog/threat-research/2015/07/cve-2015-5122_-_seco.html

- Regarding the first exploit, FireEy wrote:
  The HackingTeam leak already resulted in the public disclosure of another 0-Day Adobe Flash vulnerability which was quickly adopted by multiple groups and used in widespread attacks. FireEye Labs identified a PoC for another Adobe Flash zero-day vulnerability buried within the leaked data, and alerted Adobe to the issue.
- FireEye notes, this second one is just as well and clearly written as the previous one.
- As one hack monitoring site put it: "Code was fast disclosed, integrated to MetaSploit and as we were all expecting again, integration in Exploit Kits was a matter of hours."
- Both the past one and this one are being used to install file encrypting ransomware.
- Mozilla quickly moved to block all versions of FLASH.
- Adobe releases 18,0,0,209
- Chrome auto-updated too.

"OccupyFlash.org"

- http://occupyflash.org/
- "The movement to rid the world of the Flash Player plugin"

Hacking Team data dump reveals their UEFI Rootkit technology.
http://www.pcworld.com/article/2948092/security/hacking-teams-malware-uses-uefi-rootkit-to-survive-os-reinstalls.html
http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems/

- Allows their RCS 9 (Remote Control System) to survive HD changes, reformats, etc.
- Modules for the "Insyde UEFI BIOS", a Taiwanese BIOS used by HP, Dell, Lenovo, Acer, Asus & Toshiba.
- Believed to also be compatible with AMI's BIOS.
- May require physical access, but remote install not ruled out.
- Notes:
  - To install the RCS UEFI rootkit, an attacker must reboot the system into the UEFI shell, extract the firmware, write the rootkit to the dumped image and then flash it back to the system.
- The rootkit has three modules:
  - one for reading and writing to NTFS file systems;
  - one for hooking the OS boot process;
  - one that checks if RCS is present on the system.
- The rootkit checks for the existence of two software agents called scout.exe and soldier.exe every time the system is rebooted. If they don’t exist, it installs scout.exe at a predefined location inside the OS, the Trend Micro researchers said.
- How to prevent?
  - Enable UEFI Secure Boot.
  - Update the firmware to its latest version.
  - Activate a strong BIOS/UEFI access password.

The OpenSSL "CVE-2015-1793" certificate verification bug

https://www.openssl.org/news/secadv_20150709.txt
http://arstechnica.com/security/2015/07/critical-openssl-bug-allows-attackers-to-impersonate-any-trusted-website/
http://thehackernews.com/2015/07/openssl-vulnerability-ssl-certificate.html
https://threatpost.com/openssl-patches-critical-certificate-validation-vulnerability/113703

- Last Monday the OpenSSL team announced a "high severity" update coming in three days.
- The often-quoted official statement:
  - "During certificate verification, OpenSSL will attempt to find an alternative certificate chain if the first attempt to build such a chain fails. An error in the implementation of this logic can mean that an attacker could use certain checks on untrusted certificates to be bypassed, such as the CA flag, enabling them to use a valid leaf certificate to act as a CA and 'issue' an invalid certificate."
- What it means:
  - There was a way for bad guys to create a certificate for an arbitrary website, and to induce those two, one-month-old versions of OpenSSL, to trust the certificate even through it was never signed by a valid certificate authority.
- So, it was a certificate chain verification bug.
- Mitigating Factors:
  - Discovered by Google's Adam Langley and BoringSSL's David Benjamin.
  - Was only just introduced with the very recent June 11th, 2015 update.
  - Only affects the 1.0.1 and 1.0.2 series, not the venerable 0.9.8 and 1.0.0 versions.
  - No reports of it being used in the wild. No reports of public exploit.
  - This would impact client trust, but none of the major browsers use OpenSSL: IE, Chrome, Firefox, or Safari.
  - Linux Distros were largely safe since they haven't updated OpenSSL since.
    - Red Hat, CentOS and Ubuntu are all fine.

Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications

- 34-pages & written by a who's who of security and cryptography.
- http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf
- **Abstract:**
  Twenty years ago, law enforcement organizations lobbied to require data and communication services to engineer their products to guarantee law enforcement access to all data. After lengthy debate and vigorous predictions of enforcement channels going dark, these attempts to regulate the emerging Internet were abandoned. In the intervening years, innovation on the Internet flourished, and law enforcement agencies found new and more effective means of accessing vastly larger quantities of data. Today we are again hearing calls for regulation to mandate the provision of exceptional access mechanisms. In this report, a group of computer scientists and security experts, many of whom participated in a 1997 study of these same topics, has convened to explore the likely effects of imposing extraordinary access mandates. We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago. In the wake of the growing economic and social cost of the fundamental insecurity of today's Internet environment, any proposals that alter the security dynamics online should be approached with caution.

Exceptional access would force Internet system developers to reverse forward secrecy design practices that seek to minimize the impact on user privacy when systems are breached. The complexity of today's Internet environment, with millions of apps and globally connected services, means that new law enforcement requirements are likely to introduce unanticipated, hard to detect security flaws. Beyond these and other technical vulnerabilities, the prospect of globally deployed exceptional access systems raises difficult problems about how such an environment would be governed and how to ensure that such systems would respect human rights and the rule of law.

- **The biggest problem for those who wrote this paper:** No clear statement of requirements from the government. Merely vague "political" cautions.
    - <quote> The current public policy debate is hampered by the fact that law enforcement has not provided a sufficiently complete statement of their requirements for technical experts or lawmakers to analyze.

Consequences of compliance with "Exceptional Access" requirements:

- Loss of Forward Secrecy!
  <quote> The first technical obstacle is that although the mode of encrypting a symmetric key with a public key is in common use, companies are aggressively moving away from it because of a significant practical vulnerability: if an entity’s private key is ever breached, all data ever secured with this public key is immediately compromised. Because it is unwise to assume a network will never be breached, a single failure should never compromise all data that was ever encrypted.

  Thus, companies are moving towards forward secrecy, an approach that greatly reduces the exposure of an entity that has been compromised. With forward secrecy, a new key is negotiated with each transaction, and long-term keys are used only for authentication. These transaction (or session) keys are discarded after each transaction — leaving much less for an attacker to work with. When a system with forward secrecy is used, an attacker who breaches a network and gains access to keys can only decrypt data from the time of the breach until the breach is discovered and rectified; historic data remains safe. In addition, since session keys are destroyed immediately after the completion of each transaction, an attacker must interject itself into the process of each transaction in real time to obtain the keys and compromise the data.

  The security benefits make clear why companies are rapidly switching to systems that provide forward secrecy. However, the requirement of key escrow creates a long-term vulnerability: if any of the private escrowing keys are ever compromised, then all data that ever made use of the compromised key is permanently compromised. That is, in order to accommodate the need for surreptitious, third-party access by law enforcement agencies, messages will have to be left open to attack by anyone who can obtain a copy of one of the many copies of the law enforcement keys. Thus all known methods of achieving third-party escrow are incompatible with forward secrecy.

- Escrow Key Management:
    - Who would control the escrowed keys? Within the US, one could postulate that the FBI or some other designated federal entity would hold the private key necessary to obtain access to data and that judicial mechanisms would be constructed to enable its use by the plethora of federal, state, and local law enforcement entities. However, this leaves unanswered the question of what happens outside a nation's borders. Would German and French public- and private-sector organizations be willing to use systems that gave the US government access to their data — especially when they could instead use locally built systems that do not? What about Russia? Would encrypted data transmitted between the US and China need to have keys escrowed by both governments? Could a single escrow agent be found that would be acceptable to both governments? If so, would access be granted to just one of the two governments or would both need to agree to a request?

- Concentration of ultra-high-value targets for bad actors.
    - If law enforcement's keys guaranteed access to everything, an attacker who gained access to these keys would enjoy the same privilege.

- Managing Jurisdiction:
    - <quote> The greatest impediment to exceptional access may be jurisdiction. Building in exceptional access would be risky enough even if only one law enforcement agency in the world had it. But this is not only a US issue. The UK government promises legislation this fall to compel communications service providers, including US-based corporations, to grant access to UK law enforcement agencies, and other countries would certainly follow suit. China has already intimated that it may require exceptional access. If a British-based developer deploys a messaging application used by citizens of China, must it provide exceptional access to Chinese law enforcement? Which countries have sufficient respect for the rule of law to participate in an international exceptional access framework? How would such determinations be made? How would timely approvals be given for the millions of new products with communications capabilities? And how would this new surveillance ecosystem be funded and supervised? The US and UK governments have fought long and hard to keep the governance of the Internet open, in the face of demands from authoritarian countries that it be brought under state control. Does not the push for exceptional access represent a breathtaking policy reversal?

OPM - Loss =includes= More than 1.1 Million Fingerprint Images!

- http://www.defenseone.com/management/2015/07/second-opm-hack-stole-data-215m-people-including-biometric/117457/
- Second OPM 21.5 million records breach.

Windows 10 - WiFi Sense:

- Simon Zerafa (@SimonZerafa) 7/10/15, 2:47 AM
  @SGgrc @padresj Windows 10 WiFi sense is enabled by default in the latest build (10166). I've turn it off.

TechWeek Europe: University Rolls Out Adblock Plus, Saves 40 Percent Network Bandwidth

http://www.techweekeurope.co.uk/e-marketing/adblock-plus-adblocking-network-traffic-172245

- A Canadian university claims to have saved between 25 and 40 percent of its network bandwidth by deploying Adblock Plus across its internal network.
- The study tested the ability of the Adblock Plus browser extension in reducing IP traffic when installed in a large enterprise network environment, and found that huge amounts of bandwidth was saved by blocking web-based advertisements and video trailers.
- The study was carried out over a period of six week, and involved 100 volunteers in an active enterprise computing environment at the university. The study's main conclusions were that Adblock Plus was not only effective in blocking online advertisements, but that it "significantly" reduced network data usage.
- Researchers said that the reduced network data demand would lead to lower infrastructure costs than a comparable network without Adblock Plus. The reduced network data demand could also lead to lower energy costs overall, said the paper, as a by-product of lower commodity network costs.

Miscellany:

A Big Number Calculator for iOS & Android:

- From the "Go language" team: Ivy
- https://itunes.apple.com/us/app/ivy-big-number-calculator/id1012116478?mt=8
- https://play.google.com/store/apps/details?id=org.golang.ivy

LHC finds another theoretical particle!

- Thanks to Virgilio Corrado (@virgiliocorrado)
- (Movie: Particle Fever - about the early days of the LHC.)
- http://www.theverge.com/2015/7/14/8957981/pentaquark-cern-lhc-discovery
- Scientists at the Large Hadron Collider have announced the discovery of the pentaquark, a class of subatomic particle consisting of four quarks and one antiquark bound together. Like the Higgs boson before it, the pentaquark's existence has been theorized for years, but experiments in the early-2000s claiming to have detected the exotic form of matter were later invalidated. Many scientists had since given up on the pentaquark for good, but this time, say CERN physicists, there's no doubt it's been found.

Media:

- "Humans" on AMC is turning out to be terrifically interesting.

SpinRite:

June 7th (one week ago)
From: Kevin Wilhelm

After listening to Steve's podcasts for years and hearing stories about SpinRite, I finally got to use it in a real critical situation.

I work for an IT company that for the most part does Managed Services, but sometimes get called for "break fix" work. On this occasion, we were contacted by a large national boat manufacturing company whose headquarters are local. I was assigned with going onsite to "revive" an old XP machine that had crashed a while back but they wanted to get data off it. Once I got there and learned of the whole picture, they were actually getting audited for accounting purposes and they realized that the only instance of a very old program resided on this one computer, and there was no support to be found anymore for this program. So, it was not just a matter of getting data off the drive, but really getting the operating system running, so we could attempt to run the program and get the data from it.

Well, I broke out my trusty SpinRite CD (which I honestly hadn't used in over 4 years), and within 2 hours…..WOILA! The OS booted, the user could log in, and open the program like nothing ever happened. Needless to say, I lectured them on the all the things they did wrong that lead to this situations and which could so easily have cost them dearly. I was happy to be able to offer assistance with your product, and will certainly recommend it to many more for years to come!!!

Thanks Steve!

Kevin Wilhelm,
Senior Systems Engineer

SQRL Revisited

Ned Griffin (@Ned_Griffin) 4:57pm · 13 Jul 2015 · Twitter Web Client
@SGgrc Nice. I hope to one day have the slightest idea what you are talking about when you bring up the SQRL project on the podcast.

Episode #424, October 2nd with Tom - SQRL: Secure QR Login

- 92 weeks ago.
- Slow and careful evolution into a complete an mature Internet Identity Authentication System.
- 2-party design..
- CAN also support 3rd-party "federated" identity.

The core SQRL concept -- A refresher

- An HMAC keyed by a large random number:
  - Hash-based Message Authentication Code.
  - Just like Crypto uses a key to encrypt and decrypt.
  - A way of creating a "keyed hash"
- Everyone gets their own personal hash function.
- Every website's domain name is hashed to produce a personal private key!

SQRL's keying hierarchy

- Rescue Code - 24 digits (1.5x credit card number)
  - SQRL's "get out of jail, free" card
- 2-party system means no recourse
- You may never need it... but just in case...
- User's password

What if I want another identity for the same site?

- Alternate IDs

What if my SQRL identity is stolen? Or if I'm worried it might have been?

- Identity Lock.
- Low-bar to disable, High-bar to enable.
- Rekeying an identity.

What if I want to stop using SQRL?

- Removal
- (and also replacement)
- SQRL incorporates complete identity lifecycle management.

What if a fraudulent site shows a SQRL ID from another site?

- The spoofing problem.

Where we are today:

- GRC
- Jeff Arthur (iOS)
- Ralf W. (Android)
- PHP, Python, etc.....