Security Now! #498 - 03-10-15

Freak & RowHammer

This week on Security Now!

- Patch Tuesday
- The CIA really wants to crack Apple's iPhone security,
- A bunch of recent odds & ends about routers, redirection & the Apple Watch ... then:
- In-Depth technical examination of this week's two big security items:
- What's up with FREAK
- An exploit against DRAM

Security News

Patch Tuesday's Details:

- 14 Patch Bundles, 5 Critical and all RCE / the remaining 9 "Important"
    - #1: Standard monthly Cumulative Security Update for Internet Explorer.
        - "The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer."
    - #2: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution
        - ... resolves a vulnerability in the VBScript scripting engine in Microsoft Windows. The vulnerability could allow remote code execution if a user visits a specially crafted website which uses VBScript.
    - #3: RCE Vulnerability in Windows
    - #4: RCE in Adobe Font Driver
    - #5: RCE in Office -- don't open a specially crafted Microsoft Office file.

The CIA's been after Apple for years!

- https://firstlook.org/theintercept/2015/03/10/ispy-cia-campaign-steal-apples-secrets
- First the news... then what this fully means: The impossibility of protecting local decryption).
- Long rambling story with facts scattered anf a lot of repetition.
- Researchers claimed to have successfully modified the OS X updater to install a keylogger.
- CIA's researchers claim to have modified Apple's Xcode development platform so that any applications built with it will automatically include backdoors, and infected apps can somehow "invite" other apps to join in.
- The TPM -- Trusted Platform Module -- has been a long-term target of this group.
- And they make also been focusing intently upon the iPhone:
- <quote> The Snowden documents do not address how successful the targeting of

Apple’s encryption mechanisms have been, nor do they provide any detail about the specific use of such exploits by U.S. intelligence. But they do shed light on an ongoing campaign aimed at defeating Apple's efforts to secure its products, and in turn, its customers’ private data.

- <quote> In the top-secret documents, ranging from 2010 through 2012, the researchers appear particularly intent on extracting encryption keys that prevent unauthorized access to data stored — and firmware run — on Apple products.
- In an abstract of a 2011 presentation at "The Jamboree" (the annual meeting) the researchers noted that the Intelligence Community is highly dependent on a very small number of security flaws, many of which are public, and which Apple eventually patches. They then promised that their presentation could provide the intelligence Community with a "method to non-invasively extract" encryption keys used on Apple devices.
- Another presentation focused on physically extracting the key from Apple’s hardware.
- In other words: a side-channel attack using EMF emissions or power consumption, and a brute-force pop-the-top of the chip attack.
- The first "Jamboree" took place in 2006, shortly before the introduction of the first iPhone.
- So... what's the dilemma??

Miscellany

James Bennett Saxon (@iShming):

- @SGgrc I have FIOS with Verizon supplied router. Can I wipe their scary firmware??

Keith V (@shadowcomputer)

- @SGgrc SSL error visiting steve.grc.com in chrome? pic.twitter.com/QfTmilLqob

blog.grc.com & steve.grc.com

- CNAME (alias) versus 301 Redirect
- Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

www.podcastawards.com... closing March 24th.

The Apple Watch

- Pricing:
  - $349 / $399
  - $549-$1,049 / $599-$1099
  - $10,000 to $17,000
- "Okay... we're going to do a watch. It'll do all of the expected iPhone-extension things. But what more can be give it?"
  - But ONLY if the other person has one too! (Network externalities: Lisa *is* getting one so that she can receive Leo's "intimate doogles".)
- Oh... and the new MacBook AIR is stunning!

SpinRite

Michael Parker (@twangatang) 3/11/15, 7:22 AM

- @SGgrc Hey. A decade of wanting to use SpinRite but couldn't find a need, my day finally came: It saved my SSD which would not boot! Thanks!

Freak & RowHammer

The “FREAK” -- Flaw in Android and Apple devices cripples HTTPS crypto protection
http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html
https://www.smacktls.com/

Testing Sites: Browser - https://freakattack.com/ Server - https://SSLLabs.com

Bug forces millions of sites to use easily breakable key once thought to be dead.
http://arstechnica.com/security/2015/03/freak-flaw-in-android-and-apple-devices-cripples-https-crypto-protection/

Old-school, export-grade crypto standard used until the 1990s can be triggered to downgrade security of client, servers, researchers find.
http://www.darkreading.com/attacks-breaches/freak-out-yet-another-new-ssl-tls-bug-found/d/d-id/1319320?_mc=RSS_DR_EDT

Who had vulnerable servers?
36.7% (!!!!) of the 14 million sites serving browser-trusted certs.

- Many are Akamai CDN endpoints.

Including: U.S. government sites like www.nsa.gov, www.whitehouse.gov and www.irs.gov.
And the FBI tip reporting site (tips.fbi.gov) was also vulnerable.
And the connect.facebook.net site which serves all of the "Like" buttons everywhere.

Vulnerable TLS client libraries include

- OpenSSL (CVE-2015-0204): versions before 1.0.1k are vulnerable. Upgrade.
- BoringSSL: versions before Nov 10, 2014 are vulnerable. Upgrade.
- SecureTransport (CVE-2015-1067, CVE-2015-2235): versions before iOS 8.2, AppleTV 7.1, and OS X Security Update 2015-002 are vulnerable.
- SChannel (CVE-2015-1637): before KB3046049 is vulnerable. See the security bulletin.
- LibReSSL: versions before 2.1.2 are vulnerable.
- Mono: versions before 3.12.1 are vulnerable.
- IBM JSSE: is vulnerable. A fix is being tested.

Web browsers that use the above TLS libraries are vulnerable, including:

- Chrome: versions before 41 on various platforms are vulnerable.
- Internet Explorer: on OS versions before March 9 are vulnerable.
- Safari: on OS versions before March 9 are vulnerable.
- Opera: versions before 28 are vulnerable.
- Android Browser: is vulnerable. Switch to Chrome 41.
- Blackberry Browser: is vulnerable. Wait for a patch.

RowHammer: Exploiting DRAM

Whats?

- A team at CMU (Carnegie Mellon University)
- http://users.ece.cmu.edu/~yoonguk/papers/kim-isca14.pdf
- The CMU guys laid out all of the framework... then some guys inGoogle's Project Zero team weaponized if by creating proof of concept code that works!
- http://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html

About DRAM.

- RowHammer is about exploiting the possibility of deliberately thrashing a tightly controlled region of DRAM that the attcker DOES control, with the aim of "flipping a bit" in memory the attacker does not contain. In other words: Breaking out of OS process containment.
- << Explain about DRAM and refresh, destructive reads, Row caching and L1, L2, L3.>>
- Talk about Parity and ECC.
- Typical refresh is every 64 milliseconds.
- The CMU experimenters were able to introduce DRAM errors into 110 out of 129 DRAM modules from three major DRAM manufacturers.
- They found that (i) it takes as few as 139K accesses to induce an error and (ii) up to one in every 1.7K cells is susceptible to errors.
- As a result, high-density DRAM is more likely to suffer from disturbance, a phenomenon in which adjacent cells interfere with each other's operation.
- If a cell is disturbed beyond its noise margin, it malfunctions and experiences a disturbance error.
- All DRAM modules manufactured in the past two years (2012 and 2013) were vulnerable, which implies that the appearance of disturbance errors in the field is a relatively recent phenomenon affecting more advanced generations of process technology.

In Google's Project Zero testing they were able to induce bit flips in HALF of the laptops they tested. Exploit requirements:

- Running 64-bit Linux.
- The absolute physical addresses of memory we have access to:

- Linux allows this via /proc/PID/pagemap.
- The relative physical addresses of memory we have access to. Linux can allow this via its support for “huge pages”, which cover 2MB of contiguous physical address space per page. Whereas a normal 4k page is smaller than a typical DRAM row, a 2MB page will typically cover multiple rows, some of which will be in the same bank.

```
code1a:
        mov (X), %eax  // Read from address X
        mov (Y), %ebx  // Read from address Y
        clflush (X)       // Flush cache for address X
        clflush (Y)       // Flush cache for address Y
        jmp  code1a
```

Exploits:

- NaCl -- Chrome's Native Client sandbox
  - By flipping a sensitive bit in the runtime code blocks, a sandbox escape can be created.

- Linux Kernel Privilege escalation
  - Use /proc/self/pagemap to flip a bit in its own pagetable... and thus gain access to all of the machine's physical memory.

Mitigations:

- Vendors ARE apparently aware of this and are taking steps.
- BIOS: Increasing the BIOS refresh rate:
  - Google writes: As an experiment, we measured the time required to cause a bit flip via double-sided hammering on one Model #4 laptop. This ran in the “less than 5 minutes” range. Then we updated the laptop’s BIOS to the latest version and re-ran the hammering test.
  -
  - We initially thought this BIOS update had fixed the issue. However, after almost 40 minutes of sequentially hammering memory, some locations exhibited bit flips.
  -
  - We conjecture that the BIOS update increased the DRAM refresh rate, making it harder — but not impossible — to cause enough disturbance between DRAM refresh cycles. This fits with data from Yoongu Kim et al’s paper (see Figure 4) which shows that, for some DRAM modules, a refresh period of 32ms is not short enough to reduce the error rate to zero.

- A self-test Linux users can run:
  - https://github.com/google/rowhammer-test