Security Now! #453 - 04-29-14

Certificate Revocation

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 first not-going-to-be-patched 0-day flaw found affecting IE.
- Critical FLASH update pushed out by Adobe.
- Firefox v29... with the new UI that looks a lot like Chrome.
- Hope for funding the Internet's clearly important open source efforts.
- Routers with DD-WRT from the factory.

Security News:

IIS 0-Day Flaw Found

- http://www.fireeye.com/blog/uncategorized/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html
- Attacks are targeting IE9-11
    - None of which run on XP.
    - IE6 through 11 are vulnerable.

- http://steve.grc.com/ (Yes... Steve has a blog!)
    - Web browsers are growing insanely complex. It's pretty clear that they will be our next-generation operating platforms. And as the last annual "Pwn2Own" contest showed, none of them can currently withstand the focused attention of skilled and determined attackers, especially when some prize money is dangled on the other side of the finish line.

      With most recent exploits, the path to exploitation is convoluted and complex. In this case it depends upon somehow encountering malicious Web content with IE's ActiveScripting enabled, which loads an Adobe SWF (Shockwave FLASH) file which, in turn, uses JavaScript in this vulnerable version of IE (presently all versions of IE). But it does this via an obscure and readily disabled VML (Vector Markup Language) rendering extension.

- Vulnerability in Internet Explorer Could Allow Remote Code Execution
    - https://technet.microsoft.com/library/security/2963983

- Vulnerability requires:
    - http://thehackernews.com/2014/04/new-zero-day-vulnerability-cve-2014.html
    - Adobe Flash
    - ActiveScripting & ActiveX
    - VML parsing - disable Vector Markup Language (VML)

- regsvr32 -u "%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll

- Microsoft RACES to fix Internet Explorer bug that puts a QUARTER of web users at risk
    - Microsoft says Internet Explorer bug is present in versions 6 to 11 - which dominate 55 percent of PC browser market
    - Windows XP will not receive any updates - though between 15 and 25 percent of world's PCs use it
    - Attacks are currently against U.S.-based defense and financial sector firms
    - http://www.dailymail.co.uk/news/article-2614582/Microsoft-RACES-fix-Internet-Explorer-bug-says-WONT-step-fix-Windows-XP-browser.html
- Use-After-Free attack
    - Microsoft: The vulnerability exists in the way that Internet Explorer accesses an object in memory that has been deleted or has not been properly allocated. The vulnerability may corrupt memory in a way that could allow an attacker to execute arbitrary code in the context of the current user within Internet Explorer. An attacker could host a specially crafted website that is designed to exploit this vulnerability through Internet Explorer and then convince a user to view the website.

Firefox v29

- "New Streamlined Look"
- New flexible customization
- New version of Firefox Sync
- Continued forward movement on HTML and CSS standards.
- "Classic Theme Restorer" add-on available:
    - https://addons.mozilla.org/en-US/firefox/addon/classicthemerestorer/

Adobe Updates Flash to Fix another Critical Flaw

- Adobe has released a multi-platform patch for a flaw in Flash Player that is being actively exploited. Windows users running Flash Player versions 13.0.0 182 and earlier need to update as do Mac users running versions 13.0.0.201 and earlier, and Linux users running versions 11.2.202.350 and earlier. While the detected attacks target Flash on Windows machines, the flaw could soon be more widely exploited. The fix will be automatically pushed out to users running IE 10 and 11 on Windows 8 and to users of the Chrome browser.

Buffalo Tech routers are DD-WRT out of the box.

- n600 dual band.

Linux Foundation announced a 3-year initiative backed by at least $3.9 million to help underfunded open source projects -- with OpenSSL first but not last.

- Amazon, Cisco, Dell, Facebook, Fujitsu, Google, IBM, Intel, Microsoft, NetApp, Qualcomm, Rackspace, and VMware have all pledged to commit at least $100,000 a year for at least three years to the Linux Foundation's new "Core Infrastructure Initiative."
- $3.9 million pledged.
- The companies were VERY WILLING and wished they'd done it sooner.
- Previously, OpenSSL previously received about $2000 per year.
- http://www.theverge.com/2014/4/24/5646178/google-microsoft-and-facebook-launch-project-to-stop-the
- http://arstechnica.com/information-technology/2014/04/tech-giants-chastened-by-heartbleed-finally-agree-to-fund-openssl/

SpinRite:

Gary Foard in England
Subject: Spinrite testimonial
Date: Sat, 12 Apr 2014 07:50:22 -0000

Hi Steve

Long time listener etc. Just thought I'd drop you a note that you might like. I get pleasure from keeping old computers working and appreciate basic but good programs that have a purpose and do a good job.

So I was very happy when I saw how SpinRite worked and behaved. I use standard Ubuntu nearly everywhere now, since Windows M.E. ran out and was then relying on Firefox to keep me safe. I installed a full working Ubuntu OS on a USB thumb drive (not a live install ISO) so I have a fully patched computer rattling around in my pocket on my keyring. However once in a while it becomes very slow. So I get a very old 256 ram Compaq Presario 700 which was otherwise only used to practice Linux server commands on, boot SpinRite and run against the plugged-in USB drive. I have to run it on level 3 to do any good... but the difference is unbelievable!

So well done Steve for giving a very old computer a practical use, and keeping my portable Ubuntu disc running sweet.

Regards Gary Foard - TheBroadbandEngineer.co.uk

Revocation:

A review of the chain of trust model.

- Trusted Root.
- The move to intermediate certificates.

When good certificates go bad.

- The need to ***override***

The CRL

- Signed certificate contains "how to verify me" URL.
    - "CRL Distribution Points"
- Released daily, cached for a week.
- Monster CRLs
- Post-Heartbleed, Globalsign's CRL exploded to 5 megabytes.
- No one's happy. CA must supply the bandwidth!
- New CRL solution: many smaller sub-lists.
- But fundamental problem remains: Web browser is retrieving status it doesn't care about.

OCSP

- Online Certificate Status Protocol
- Once again, signed cert contains "how to verify me" URL.
    - "Authority Information Access" (AIA)
- Updated "instantly", cached for a day... thus much "fresher."
    - Perhaps cached even less under agreement.

Problems: (Flies in the ointment)

- Response Delays ... CRL or OCSP
- Response... never: The NO REPLY problem...
- The need to fail soft

OCSP Stapling to the rescue.

- Now the server obtains a single updated status from the CA.
- Enabled for many years in all Microsoft servers.
- Available in Apache, nginx and LiteSpeed... but disabled by default.

Attacking the system:

- Fail soft means that suitably positioned bad guys can leverage.
- A Fail Hard policy prevents
- (Only Firefox offers Fail Hard today.)

OCSP Must Staple

- In the cert would be best.
- In the response headers (a la HSTS) is interim.