Security Leftovers

By *Rianne Schestowitz*
Created *07/08/2015 - 9:33pm*
Submitted by Rianne Schestowitz on Friday 7th of August 2015 09:33:24 PM Filed under Security [1]

- **Security updates for Friday [2]**

- **Security updates for Thursday [3]**

- **Black Hat Researchers Hack Rifle for Fun [4]**

  > "The reason we started doing this in the first place is Runa [Sandvik] is from Norway and has a very romanticized vision of the U.S., so loving all things America, we needed to go to a gun show," Augur said.
  >
  > At to the gun show, Sandvik became interested in the TrackingPoint weapon after learning that it is a Linux-powered device that could be connected to a phone via a mobile app.

- **And even Wintel is not safe [5]**

  > At the annual Black Hat conference delegates have been shown a new exploit for Intel and AMD x86 central processor units that has hitherto existed since 1977!
  >
  > [...]
  >
  > Christopher Domas, a security researcher with the Battelle Memorial Institute discovered the flaw. ?By leveraging the flaw, attackers could install a rootkit in the processors System

Management Mode (SMM), a protected region of code that underpins all the firmware security features in modern computers. Once installed, the rootkit could be used for destructive attacks like wiping the UEFI (Unified Extensible Firmware Interface) the modern BIOS or even to re-infect the OS after a clean install. Protection features like Secure Boot wouldn?t help, because they too rely on the SMM to be secure. The attack essentially breaks the hardware roots of trust,? Domas said.

- **HTML5 privacy hole left users open to tracking for three years [6]**

  A feature of HTML5 that allows sites to detect battery life on a visitor's device can also be used to track behaviour, a piece of research has revealed.

- **Sick of Flash security holes? HTML5 has its own [7]**

  HTML5 has been billed as the natural, standards-based successor to proprietary plug-ins such as Adobe's Flash Player for providing rich multimedia services on the Web. But when it comes to security, one of Flash's major weaknesses, HTML5 is no panacea.

  In fact, HTML5 has security issues of its own. Julien Bellanger, CEO of application security monitoring firm Prevoty, says HTML5 makes security more complex, not simpler. HTML5 security has been a question mark for years, and it has not improved over the stretch, he says.

- **Attackers can access Dropbox, Google Drive, OneDrive files without a user's password [8]**

  The attack differs from traditional man-in-the-middle attacks, which rely on tapping data in transit between two servers or users, because it exploits a vulnerability in the design of many file synchronization offerings, including Google, Box, Microsoft, and Dropbox services.

- **SDN switches aren't hard to compromise, researcher says [9]**

  Onie is a small, Linux based operating system that runs on a bare-metal switch. A network operating system is installed on top of Onie, which is designed to make it easy and fast for the OS to be swapped with a different one.

- **Open Network Switches Pose Security Risk, Researcher Says [10]**

At the Black Hat show, a security expert demonstrates how vulnerable SDN switches that use the ONIE software are open to attacks by hackers.

- **OPM wins Pwnie, Google on Android security, DoJ on CFAA: Black Hat 2015 roundup** **[11]**

  Black Hat USA is finishing up in Las Vegas. News from its 18th year includes nuclear nightmares, Department of Justice on computer crime and research, Google on the state of Android security and much more.

- **on the detection of quantum insert** **[12]**

  The NSA has a secret project that can redirect web browsers to sites containing more sophisticated exploits called QUANTUM INSERT. (Do I still need to say allegedly?) It works by injecting packets into the TCP stream, though overwriting the stream may be a more accurate description. Refer to Deep dive into QUANTUM INSERT for more details. At the end of that post, there?s links to some code that can help one detect QI attacks in the wild. As noted by Wired and Bruce Schneier, among dozens of others, now we can defend ourselves against this attack (well, at least detect it).

Security

Source URL: http://www.tuxmachines.org/node/78810

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://lwn.net/Articles/653866/rss
[3] http://lwn.net/Articles/653742/rss
[4] http://www.eweek.com/security/black-hat-researchers-hacked-rifles-for-fun.html
[5] http://www.itwire.com/business-it-news/security/68920-and-even-wintel-is-not-safe
[6] http://www.wired.co.uk/news/archive/2015-08/04/privacy-hole-in-firefox
[7] http://www.infoworld.com/article/2956193/html5/sick-of-flash-security-holes-html5-has-its-own.html
[8] http://www.zdnet.com/article/dropbox-google-drive-onedrive-files-man-cloud-attack/#ftag=RSSbaffb68
[9] http://www.networkworld.com/article/2956777/security/sdn-switches-arent-hard-to-compromise-researcher-says.html
[10] http://www.eweek.com/networking/open-network-switches-pose-security-risk-researcher-says.html
[11] http://www.zdnet.com/article/opm-wins-pwnie-google-on-android-security-doj-on-cfaa-black-hat-2015-roundup/
[12] http://www.tedunangst.com/flak/post/on-the-detection-of-quantum-insert