GW CSPRI Newsletter

August 18, 2014

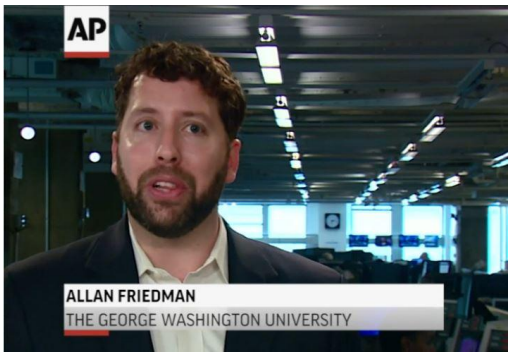
From the **Cyber Security Policy and Research Institute** of **The George Washington University**, www.cspri.seas.gwu.edu.

This newsletter is a weekly summary of events related to cyber security policy and research, with a special focus on developments and events in the Washington, DC area.

Faculty and student readers of this newsletter with new and important cyber security research to report (especially new papers or results by GW faculty and students) are encouraged to send notifications of this to cspriaa@gwu.edu. A short (up to three sentences) description of why you think the research is important is required.

Contents

Announcements



CSPRI Research Scientist, Dr. Allan Friedman was featured in AP News expressing some skepticism about the true nature of Snowden's new claims of an automatic Internet defense system. Click **here** for the video.

Events

-Aug. 19, 6:30 p.m. – 8:00 p.m., **ISSA DC Meetup: Combating Today's Targeted Attacks** – Targeted attacks can only be thwarted by increasing the level of discomfort of the adversary to a point where they cannot expend the resources to maintain persistence. Advanced persistent response is the future of cyber security. The speaker will be Tom Kellerman, vice president of cyber security at Trend Micro. Center for American Progress, 1333 H Street, NW. More information.

-Aug. 20, 1:00 p.m. – 2:30 p.m., **NIST Cybersecurity Framework: Lessons Learned at the Six-Month Mark** - Join ISC-ISAC and DCT Associates for an important webinar that reviews the crucial lessons learned about the benefits and challenges of implementing the framework and how the framework continues to evolve. Hear from government officials, industry experts and top technologists the best methods for ensuring that the framework can help your organization improve your cybersecurity practices and minimize threats. More information.

-Aug. 20, 6:00 p.m. – 9:00 p.m., **NovaInfosec Meetup, West** - If you are in the IT security business, like the idea of meeting to discuss the foibles of the industry, demo your recent discovery and conquest, or just drink a beer with like minded folks, then this meeting is for you. Lost Rhino Brewing Co., 21730 Red Rum Drive #142, Ashburn, VA, 20147. More information.

-Aug. 28, 7:00 p.m., **Build It, Break It, Fix It** - security contest aims to teach students to write more secure programs. The contest evaluates participants' abilities to develop secure and efficient programs. The contest is broken up into three rounds that take place over consecutive weekends. During the Build It round, builders write software that implements the system prescribed by the contest. In the Break It round, breakers find as many flaws as possible in the Build It implementations submitted by other teams. During the Fix It round, builders attempt to fix any problems in their Build It submissions that were identified by other breaker teams. Each round will respectively start on August 28th**,** September 4th, and September 12th**.** More information.

-Aug. 28, 7:00 p.m. – 10:00 p.m., **CharmSec Meetup** – An informal, all-ages, citysec-style meetup of information security professionals in Baltimore. Heavy Seas Alehouse, 1300 Bank Street, Baltimore, MD, 21231. More information.

-Sept. 3, 6:30 p.m. – 8:30 p.m., **OWASP Meetup: The World of Ruby on Rails Security** – Take a quick trip through the world of Ruby on Rails security! The journey will start with an overview of security features offered by the popular web framework, then detour through dangerous pitfalls and unsafe defaults, and finally end with suggestions for improving security in Rails apps and integrating improvements into the development process. Uber, 1200 18th Street NW, Suite 700. More information.

Legislative Lowdown

-The House and Senate are away for August recess.

Cyber Security Policy News

-The latest revelation from NSA whistleblower Edward Snowden is that the United States runs a secret program called "MonsterMind" designed to detect and automatically respond to threats. The program — which, according to Wired.com has never before been revealed – can reportedly intercept all foreign communications to people in the U.S., detect and disarm cyberattacks, and can "automatically fire back, with no human involvement." Snowden told wired that MonsterMind was the straw that broke the camel's back – basically the secret program that caused him to break his silence and start disclosing the government's surveillance secrets.

Snowden remains in exile in Russia, where Russian Prime Minister Dmitry Medvedev has just signed a decree prohibiting the anonymous use of wireless Internet access. As ZDNet reports, people using public wi-fi in Russia now must provide identification before they are allowed to access the network.

-Wired.com dropped another bombshell in the government's use of technology last week, with a story detailing how the FBI has been using drive-by downloads to identify people who visit certain suspicious websites. According to Wired, the Justice Department is using the method to identify people who visit child pornography websites hiding in the Tor network. Apparently, the tactic has been successful for the agency - more than a dozen people are now facing trial as part of a push called "Operation Torpedo." Not everyone is thrilled. Privacy and security experts accuse the FBI of glossing over the technique when describing it to judges, and hiding its use from defendants.

Meanwhile, the National Journal covers a report released by the inspector general at the Justice Department, which found that the FBI had unintentionally spied on the communications data of some Americans who were not targets of investigations because of typographical errors. "We found that the FBI's corrective measures have not completely eliminated potential intelligence violations resulting from typographical errors in the identification of a telephone number, email address, or social security number in an NSL," the report reads. "These typographical errors cause the FBI to request and, in some instances receive, the information of someone other than the intended target of the NSL." Read more here.

-AOL has decided that it won't honor "do-not-track" signals from visitors' and users' browsers, the company acknowledged last week. Politico reports that the mostly ad-supported AOL made the announcement in an update to its privacy policy, saying the company won't honor do-not-track because there is no standard for it. "A new California privacy law requires companies to clarify how they will respond to 'do not track' signals

sent by Web browsers," Politico wrote in a news roundup. "AOL also said it is consolidating all its privacy policies into one, starting in mid-September. Previously, the company had separate policies for a lot of its services, which include TechCrunch, MapQuest, AOL.com and The Huffington Post."

-The US Department of Homeland Security has long talked about the value and importance of agencies and private sector partners sharing information on the latest cyber threats. But according to a report released by the DHS Office of Inspector General (OIG), just three of 16 identified industries that support elements of the country's critical infrastructure have joined a DHS threat information-sharing program. NextGov reports that the Enhanced Cybersecurity Service program, originally limited to Pentagon contractors, was expanded early last year to include the critical infrastructure industries. So far, however, the program hasn't caught on in the private sector. Only the energy, communications service, and the defense industrial base have joined the program.

-Nicole Wong, one of the Obama administration's top people on technology and privacy, is leaving the White House, reports The Washington Post. "Prior to joining the Obama administration, Wong was director of legal products at Twitter and deputy general counsel at Google," The Post's Hayley Tsukayama writes. "At Google, she earned the nickname 'The Decider' — a reference to the role she took in helping to determine when to censor results on the company's search engine or clips on its YouTube video service that governments claimed ran afoul of local laws."

The Cyber Security Policy and Research Institute (CSPRI) is a center for GW and the Washington area to promote technical research and policy analysis of problems that have a significant computer security and information assurance component. More information is available at our website, http://www.cspri.seas.gwu.edu.