GW CSPRI Newsletter

September 9, 2013

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.

Announcement: CSPRI's blog, The CSPRI Byte, has gone live! Our blog is student-and- alumni-run on all things cybersecurity. Check out our articles written by CSPRI affiliates to find out how cybersecurity plays a role in intelligence, diplomacy, business, healthcare, education, and more!

Contents

Events

-Sept. 8-14, **2013 ASE/IEEE International Conference on Privacy, Security, Risk and Trust** - The goal of this week-long conference is to provide an international forum for information privacy, risk, trust, and security researchers and practitioners to explore solutions to profound challenges on privacy, risk, trust, and security issues and exchange recent progresses. Hilton Alexandria Mark Center, 5000 Seminary Road, Alexandria, Va. 22311. More information.

-Sept. 11, 7:30 a.m. - 5:00 p.m., **Angel Venture Forum, Cyber Security & Healthcare Investment Conference**. With the increasing adoption of cloud computing, mobile devices and web-based applications, hackers have more opportunities than ever to infiltrate and crash network systems, especially in healthcare. The two greatest areas of opportunity for investment capital and the start-up community are in healthcare and cyber security. The nexus of these two sectors provides an even greater, more focused set of opportunities for investment. The Angel Venture Forum brings together roundtables of experts to discuss the topics and the opportunities herein. Jones Day Terrace & Conference Center, 51 Louisiana Ave, NW. More information.

-Sept. 11, 1:00 p.m., **A New Vision for Fraud Prevention: Marrying Threat and Behavior Data** - This free Webinar is related to the financial sector. It will present ideas for integrating and analyzing multi-channel customer account data, transactional data, threat intelligence, and layers of security to more accurately determine risk within and across accounts. More information.

-Sept. 11, 2:00 p.m., **The Threat to Americans' Personal Information: A Look into the Security and Reliability of the Health Exchange Data Hub** - The Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will hold a hearing. Witness list TBA. This hearing will be Webcast. 311 Cannon House Office Bldg. More information.

-Sept. 12, 12:00 noon, **What to Do about Data Security? A Discussion of the FTC's LabMD & Wyndham Cases** - Tech Freedom will host a panel discussion on the unique aspects of the LabMD case. Highlighted will be the FTC's decision not to prosecute filesharing services like Limewire for unfair trade practices in configuring their software to trick users into sharing files unintentionally. The FTC eventually reversed this decision, but not until it finally brought an enforcement action against Frostwire in 2011 for the same unfair practice. The panel will also discuss the larger legal issues raised by the LabMD case, the FTC's pending litigation with Wyndham Hotels, and other recent cases settled by the FTC. Lunch will be served, but RSVPs requested. TF, 110 Maryland Ave., NE. More information.

-Sept. 17-19, **Navigating the National Cybersecurity Education Interstate Highway** - This workshop, put on by the National Initiative for Cybersecurity Education (NICE), will highlight cybersecurity education concepts, tools, and best practices with a focus on successes at the state and federal levels. The goal is to highlight cybersecurity awareness, education, and training programs that can be adopted, copied, or used, or built-on by small businesses, educational institutions, industry, and government at the states, local, tribal and federal levels to advance the strategic goals of NICE. NIST, 100 Bureau Drive, Gaithersburg, Md. 20899. More information.

-Sept. 17-19, **Software Assurance Forum, Fall 2013** - Build Security In is a collaborative effort that provides practices, tools, guidelines, rules, principles, and other resources for software developers, architects, and security practitioners so security can be built into software at every phase of its development. This event is open to the public and free, but registration is required. 7525 Colshire Drive, McLean, Va. 22102. More information.

-Sept. 18, 1:00 p.m. - 2:30 p.m., **Emergent Properties of Doing: An ICS-ISAC Public Briefing** - A Webinar panel discussion facilitated by ICS-ISAC Chair Chris Blask on the Situational Awareness Reference Architecture (SARA) pilot currently being executed by the Center and its membership. In this session, representatives from the vendors, integrators, and industry experts involved -- including Adam Vincent (CyberSquared), Matt Jonkman (EmergingThreats), Jon Stanford (PwC) and Michael Glover (Prime Controls) -- will discuss the pilot as well as the opportunity for lessons learned from construction of a real-time knowledge sharing network needed to secure critical infrastructure. More information.

-Sept. 18, 4:30 p.m., **NovaSec Networking Event** - This gathering will bring together security professionals from commercial and government organizations with members of local Northern

Virginia businesses and associations to allow participants to meet, interact on key issues and provide a unified forum to network with like-minded individuals. Iris Lounge, 1524 Spring Hill Rd., McLean, VA 22102. More information.

-Sept. 18-19, **Cyber Security and Infrastructure Protection Symposium** - This symposium brings together the senior level U.S. Government and Industry Cyber Security experts from the Critical Infrastructure Sectors – including Energy, Homeland Security, Defense, Transportation, IT/Communications, Postal, Emergency Services & Banking, and Finance -- who are taking infrastructure protection to a new level and are creating the latest tools, techniques, and solutions for protecting our resources from internal and external cyber terrorism. Holiday Inn Rosslyn at Key Bridge 1900 North Fort Myer Drive, Arlington, Va. 22209. More information.

Legislative Lowdown

The House and Senate have been in recess and return to Washington this week.

Cyber Security Policy News

-The National Security Agency has broken the protections that surround some of the most important security and privacy tools available, according to reporting by The New York Times and other publications last week. The agency has circumvented much of the encryption, or digital scrambling, that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world. Many users assume that their data is safe from prying eyes. The N.S.A treats its recent successes in deciphering protected information as among its most closely guarded secrets, restricted to those cleared for a highly classified program code-named Bullrun, according to the documents, provided by Edward J. Snowden.

-The American Civil Liberties Union's lawsuit against the NSA is gaining steam — and the support is coming from some interesting quarters. High-profile conservatives have begun filing amicus briefs on behalf of the ACLU, The Washington Post reports. Among them is the National Rifle Association, which argues that the NSA's surveillance activity could allow the government to identify gun owners and potentially circumvent the Second Amendment. The NRA isn't the only right-leaning amicus in ACLU v. Clapper. Representative Jim Sensenbrenner (R-Wis.), author of the Patriot Act, who previously said he never meant the NSA to go as far as it did, has also filed a brief. Sensenbrenner accuses the Obama administration of assuming Congress was okay with the surveillance, simply because it didn't object. However, much of Congress never had an opportunity to debate the program.

Yahoo became the latest Web company on Friday to reveal statistics about how often governments request data on its users, The Hill reports. The U.S. government issued 12,444 requests for data covering 40,322 accounts in the first half of 2013, Yahoo said. The company rejected 2 percent of those requests and found no data for 6 percent of the requests. For 55

percent of the cases, Yahoo only disclosed "non-content" information, such as subscriber data or email addresses.

All these revelations about the breadth of the NSA's domestic and international surveillance programs is seeding distrust in the private sector's evaluation of the NSA, distrust that could undermine efforts to secure systems running utilities and other vital U.S. industries, writes NextGov, citing former administration officials. NSA, maker of arguably the best encryption tools to protect data, now is attracting more attention for decrypting everyone else's data, after disclosures by ex-NSA contractor Edward Snowden of massive Internet surveillance," Aliya Sternstein writes. "NSA has postured itself as a neutral arbiter who could provide these capabilities to the private sector and really didn't necessarily want much in return," said Christopher Finan, a former White House and Pentagon official who, until July, was involved in a Defense Department cyber offense research program called Plan X. "I don't know if they can present themselves as the same honest broker now that we're seeing the enormous quantities of data that they are actually taking in."

At the same time, it's not clear that the Obama administration has a clear and effective battle plan for defending the nation's critical infrastructure from concerted cyberattack, according to CSO Online. The latest draft of the Cyber Security Framework (CSF) mandated by President Barack Obama in February fails to provide an effective battle plan for defending the nation's critical infrastructure, experts said last week. Ralph Langner, a renowned Hamburg, Germany-based consultant on ICS security, said the application of the CSF as it is written would provide no "measurable cybersecurity assurance." In favoring a self-regulatory approach with industry, the proposed CSF provides no specific methodologies for securing the industrial control systems (ICS) found in water treatment facilities, power and manufacturing plants and energy pipelines, critics say. The National Institute of Standards and Technology (NIST), which Obama put in charge of working with industry in formulating the CSF, published the draft last week.

-Privacy watchdogs are asking federal regulators to block proposed changes to Facebook policies that they say would allow the company to use the names and images of its nearly 1.2 billion users without their consent to endorse products in ads. The Los Angeles Times writes that in a letter to the Federal Trade Commission on Wednesday, the Electronic Privacy Information Center and five other consumer groups said the changes would permit Facebook "to routinely use the images and names of Facebook users for commercial advertising without their consent." Facebook insists that it is not changing its policies, just clarifying the language in them.

The move by privacy groups comes as more Americans are stockpiling their privacy. According to a new Pew survey, 86 percent of Internet users across the country have taken measures to delete or mask their digital footprints. The National Journal reports that a sizable 21 percent of Internet users have had their e-mail or social-media accounts hacked. Recent hacks of major publications and corporations' websites and Twitter accounts show that no one is safe, not even the king bee Mark Zuckerberg, whose Facebook page was compromised last month to reveal a security flaw. The Pew survey revealed that people "clear their cookies, encrypt emails, and log on to networks that obscure their IP addresses" to delete their digital footprints.

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.