GW CSPRI Newsletter

December 2, 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.

Contents

Events

*GWU specific events are in red.

-Dec. 3, 5:30 p.m. - 6:30 p.m., **Information session for GW CyberCorps cybersecurity scholarship program -** for US citizens who are or will be full-time students. Brief summary of program. Program website. An excellent opportunity to get questions answered well before an application is submitted (they are due January 31, 2014). GW Computer Science Department Conference Room, 736 Phillips Hall, 22nd and I St. NW.

-Dec. 4, **The Joint Federal Cyber Summit 2014** - The U.S. Department of Commerce and the Federal Business Council will host the Joint Federal Cyber Summit (JFCS), set to take place Wednesday, December 4, 2013 at the Department of Commerce HQ in Washington DC. This collaborative government wide event is truly one of a kind, with speakers and attendees anticipated to represent more than 10 federal government agencies. Department of Commerce, Herbert C. Hoover Building, 1401 Constitution Avenue NW More information.

-Dec. 4, 11 a.m., **Operationalize Threat Intelligence** - Forrester Research Principal Analyst, Rick Holland, joins Lookingglass CEO, Chris Coleman as they explore proactive cyber threat intelligence in this free Webinar. More information.

-Dec. 5, 12 p.m. - 2 p.m., **Strengthening the NIST Cyber Framework Against Advanced Threats -** NIST's Cybersecurity Framework has tremendous value for risk management and defines best practices to block known threats. This discussion at the Center for Strategic & International Studies (CSIS) will share intelligence about campaigns by sophisticated cyber threat actors that have targeted critical infrastructure companies and discuss how well the Framework stacks up against advanced and new, unknown threats. Lunch will be served. More information.

-Dec. 4-5, **Security Innovation Network** - Supported by the Department of Homeland Security, Science & Technology Directorate SINET programs are designed to build community of interest and bridge the gap between innovative early stage and emerging IT security solution providers and representatives from the investment, research, system integration, industry and Federal Government communities. National Press Club 529 14th Street, N.W., 13th floor. More information.

-Dec. 8-11, **Health Technology Summit** - This three-day conference features several tracks on the intersection between modern healthcare and cybersecurity. Gaylord National Hotel, 201 Waterfront Street. National Harbor, MD, 20745. More information.

-Dec. 10, 8:00 a.m. - 12:30 p.m., **Cybersecurity Forum: The Implications of Privacy to Cybersecurity** - Grand Hyatt Washington, 1000 H Street, NW. More information.

-Dec. 11, 1:00 p.m., **Ernst & Young's 2013 Global Information Security Survey: More money, More Problems?** - Financial institutions continue to increase their investment in cybersecurity, with 47% reporting an increase of at least 5% over the last year. But with greater scrutiny from the board, regulators and other stakeholders, the real measure is the return on those investments, a figure that proves elusive for even the most sophisticated organizations. When it comes to cybersecurity, there is no magic number and more money doesn't always mean less problems. This webinar will discuss ways to re-evaluate and reallocate investments to better meet today's threats. More information.

-Dec. 11-12, **Law Enforcement, Homeland Security Forum and Technology Expo** - This conference will feature several talks on cybersecurity. The speakers will include Joseph Demarest, assistant director, FBI, Cyber Division; Daniel Gerstein, assistant undersecretary, Department of Homeland Security, Science and Technology; and David Aucsmith, senior director, Institute for Advanced Technology in Governments, Microsoft Corporation. National Reconnaissance Office (NRO), J.D. Hill Conference Center, 14675 Lee Road, Chantilly, VA 20151-1715 More information.

Legislative Lowdown

-Pressure is mounting on top House Republicans to allow a vote on legislation that would curb the National Security Agency (NSA). Speaker John Boehner (R-Ohio) has defended the NSA's spying programs, but a growing bloc of his conference is signing on to a bill that would end the NSA's practice of collecting records on virtually all U.S. phone calls, which was revealed in leaks by Edward Snowden. "One House Democratic aide argued that the Republican leaders are boxed in," The Hill's Brendan Sasso reports. "If they don't allow a vote on standalone NSA reform legislation, the aide said, members will demand NSA-related amendments to must-pass legislation like the defense and intelligence authorization bills."

Cyber Security Policy News

-Microsoft is taking steps to increase protection of its users' data following reports that the National Security Agency was intercepting Google and Yahoo traffic, The Washington Post reports. Unnamed officials at the Redmond, Wash. software giant told the Post that Microsoft is fearful that the NSA might have similarly intercepted its traffic. "The tech industry's response to revelations about NSA surveillance has grown far more pointed in recent weeks as it has become clear that the government was gathering information not only through court-approved channels in the United States — overseen by the Foreign Intelligence Surveillance Court — but also through the massive data links overseas, where the NSA needs authority only from the president," the Post wrote. "That form of collection has been done surreptitiously by gaining access to fiber-optic connections on foreign soil. Smith, the Microsoft general counsel, hinted at the extent of the company's growing encryption effort at a shareholders meeting last week. 'We're focused on engineering improvements that will further strengthen security,' Smith said, 'including strengthening security against snooping by governments.'"

-US authorities considered exposing details of visits to online porn sites to discredit prominent Islamist radicals, according to a new document leaked by NSA whistleblower Edward Snowden and published by the Huffington Post. According to that publication, the NSA has been gathering records of online sexual activity and evidence of visits to pornographic websites as part of a proposed plan to harm the reputations of those whom the agency believes are radicalizing others through incendiary speeches. HuffPost said the leaked document "identifies six targets, all Muslims, as 'exemplars' of how 'personal vulnerabilities' can be learned through electronic surveillance, and then exploited to undermine a target's credibility, reputation and authority."

-Lawyers for secure email provider Lavabit last week filed the reply brief in a case that could determine whether an internet company can be compelled to turn over the master encryption keys for its entire system to facilitate court-approved surveillance on a single user, Wired.com reports. According to Wired, the government said it needed the master keys "to facilitate a 'pen register' order allowing the FBI to collect email metadata — like 'from' and 'to' lines — on a particular unnamed target, believed to be NSA leaker Edward Snowden. Levison had offered to collect the email metadata himself and transmit it to the government after 60 days. But the

government was insistent that he turn over the SSL key for the site, promising it would use the key only to monitor the targeted user, and not Lavabit's 400,000 other users."

-Privacy breaches at three separate state exchanges set up to help Americans gain access to healthcare under the Affordable Care Act illustrate the challenges of securing the sprawling network. GovInfoSecurity.com reports about incidents in North Carolina, Oregon and Vermont that involved individuals being able to access the personal information of other applicants. Reports indicate that the problems seemed to occur after multiple applicants were able to select the same username.

-While lawmakers in Congress debate the privacy and security issues of allowing more personalized drones to fly in civilian airspace, Amazon's CEO says the company is working on a plan to use drones to make same-day deliveries to customers. In an interview with 60 Minutes, Amazon chief Jeff Bezos said the company is testing delivering packages using drones. As detailed by USA Today, "Bezos played a demo video on 60 Minutes that showed how the aircraft, also known as octocopters, will pick up packages in small yellow buckets at Amazon's fulfillment centers and fly through the air to deliver items to customers after they hit the buy button online at Amazon.com." However, the company estimates that putting the service into play would take several years, as the company develops the technology further and waits for the Federal Aviation Administration to come up with rules and regulations."

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.