GW CSPRI Newsletter

November 18, 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

-Nov. 18, 3:00 p.m., **Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies** - The Senate Homeland Security and Government Affairs Committee will hold a hearing. Speakers will include Jennifer Shasky Calvery, director, Financial Crimes Enforcement Network, U.S. Department of the Treasury; Mythili Raman, acting assistant attorney general, Criminal Division, U.S. Department of Justice; Edward W. Lowery III, special agent in charge, Criminal Investigative Division; U.S. Secret Service, U.S. Department of Homeland Security; Ernie Allen, president and chief executive officer, The International Centre for Missing & Exploited Children; Patrick Murck, general counsel, The Bitcoin Foundation, Inc.; Jeremy Allaire, CEO, Circle Internet Financial, Inc.; Jerry Brito, senior research fellow, The Mercatus Center, George Mason University. Dirksen Senate Office Bldg., Room 342. More information.

-Nov 18, 5:30 p.m. - 8:00 p.m., **NoVA Hackers Association Meetup** - This informal group of security professionals from around the NoVA/DC area coordinates one or two monthly events – an evening meetup with presentations on the second Monday of the month and various lunch or bar meetups. 4350 Fair Lakes Court, Fairfax, 22033. More information.

-Nov. 19, 10:15 a.m., **The Security of Healthcare.gov** - The House Energy & Commerce Committee's Subcommittee on Oversight and Investigations will hold a hearing. Rayburn House Office Bldg., Room 2128. More information.

-Nov. 19, 10:00 a.m., **Is My Data on Healthcare.gov Secure?** - The House Science Committee will hold a hearing. The witnesses will include Morgan Wright, chief executive officer, Crowd Sourced Investigations, LLC; Fred Chang, Bobby B. Lyle Centennial Distinguished Chair in Cyber Security, Southern Methodist University; Avi Rubin, director, Health and Medical Security Laboratory Technical Director, Information Security Institute, Johns Hopkins University; and David Kennedy, CEO, TrustedSEC, LLC. Rayburn House Office Bldg., Room 2318. More information.

-Nov. 19, 9:30 a.m., **Surveillance and Foreign Intelligence Gathering in the United States: The Current State of Play** - The Center and the National Security Law Society will co-host the second event in a three part series. The speakers will be William Treanor, dean, Georgetown Law; Rep. Jim Sensenbrenner (R-Wisc.); Jameel Jaffer - director, American Civil Liberties Union, Center for Democracy; Robert Litt - general counsel, Office of the Director of National Intelligence; Matthew Olsen, former general counsel, National Security Agency; Marc Rotenberg, president and executive director, Electronic Privacy Information Center; and Laura K. Donohue - professor, Georgetown Law (moderator). Georgetown University Law Center, Hart Auditorium, Center on National Security and the Law, 600 New Jersey Ave., NW. More information.

-Nov. 19, **The FTC's Internet of Things Conference** - The Federal Trade Commission will hold a public workshop to explore consumer privacy and security issues posed by the growing connectivity of devices. The workshop will bring together academics, business and industry representatives, and consumer advocacy groups to explore the security and privacy issues in this changing world. The workshop will serve to inform the Commission about the developments in this area. The workshop will be free and open to the public. No pre-registration is required. Seating is limited and seats are available on a first-come, first-served basis. The workshop will be webcast. 601 New Jersey Avenue, N.W. More information.

-Nov. 19, 2:00 p.m., **The New European Data Privacy Regulation and What It Means for Global Privacy and the Internet Industry: A Presentation From European Commission Officials** - Join the Congressional Bi-Partisan Privacy Caucus and the Congressional Internet Caucus for a Congressional staff presentation by European Commission officials on the massive update to European Union's Data Protection Directive, the major privacy framework that governs the privacy and transatlantic data flows of the personal information of European citizens. The new regulation is a comprehensive update of the EU's 1995 data privacy protection directive. Rayburn House Office Bldg., Room 2226. More information.

-Nov. 19, 3:30 p.m., **The Present and Future Impact of Virtual Currency: National Security and International Trade and Finance** - The Senate Commitee on Banking, Housing and Urban Affairs will hold a hearing. Speakers will include Jennifer Shasky Calvery, director, Financial Crimes Enforcement Network; David Cotney, commissioner of banks, Massachusetts Division of Banks; Anthony Gallippi, co-founder and CEO, BitPay, Incorporated; Chris Larsen, founder and

CEO, Ripple Labs; Sarah Jane Hughes, university scholar and fellow in commercial law, Indiana University Maurer School of Law; Paul Smocer, BITS President, Financial Services Roundtable. Dirksen Senate Office Bldg., Room 538. More information.

-Nov. 19-20, **Cyber Education Symposium** - Both the public and the private sectors suffer from a lack of highly trained and effective cyber security leaders. In response, the government, businesses, and academic institutions are all exploring ways to retrain the existing workforce and develop a new pool of cybersecurity professionals capable of meeting the needs of tomorrow. Hyatt Regency Crystal City, 2799 Jefferson Davis Hwy, Arlington, VA 22202. More information.

-Nov. 20, 3:00 p.m. - 5:00 p.m., **Cyber Risk Wednesday** - The next Cyber Risk Wednesday will feature Catherine Mulligan, senior vice president of the Management Solutions Group, Specialty Products at Zurich, for a moderated discussion on cyber risk management and risk transfer, including the role of insurance in the evolving threat landscape. 1030 15th Street, NW, 12th Floor. More information.

Legislative Lowdown

-Leaders in the financial industry collectively encouraged senators to press ahead with cybersecurity legislation as part of a bid to breathe new life into a policy priority that has been sidelined by revelations on the extent of the National Security Agency's domestic surveillance activities, The Wall Street Journal writes. "In a letter Wednesday to senior members of the Senate Select Committee on Intelligence, three financial-industry trade groups said their ability to prevent cyberattacks will be hindered unless Congress acts," the Journal reports. "The industry's main concern is liability: Will private-sector firms expose themselves to lawsuits if, in responding to cyber-threats, they share customers' information with the government or halt certain financial transactions?"

Cyber Security Policy News

-Move over NSA. The New York Times reports that the Central Intelligence Agency is collecting bulk data records of international money transfers going through companies like Western Union -- including transactions flowing in and out of the United States. According to The Times, the CIA is invoking the same law that let the NSA hoover up huge volumes of Americans' phone records. "The C.I.A. financial records program, which the officials said was authorized by provisions in the Patriot Act and overseen by the Foreign Intelligence Surveillance Court, offers evidence that the extent of government data collection programs is not fully known and that the national debate over privacy and security may be incomplete," The Times wrote.

-Former U.S. National Security Agency contractor Edward Snowden leaked as many as 200,000 classified U.S. documents to the media, reports Reuters. The revelation came in a question-and-answer session following a speech to a foreign affairs group in Baltimore by NSA Director General Keith Alexander. The general was asked what steps U.S. authorities were taking to stop

Snowden from leaking additional information to journalists. The story, which includes a photo of Snowden's new Russian passport, quoted Alexander as saying, that the documents were being leaked in a way that does the "maximum damage to NSA and our nation. I wish there was a way to prevent it," Alexander said. "Snowden has shared somewhere between 50 (thousand) and 200,000 documents with reporters. These will continue to come out."

-Meanwhile, Wired.com continues its coverage of the legal challenge surrounding the case of Lavabit, an encrypted email service that closed its doors earlier this year in response to legal requests from the government for email information related to Snowden's account there. According to Wired, U.S.-based email providers can promise theirs users all the security and privacy they want, but they still need to do whatever it takes to give the government access. At least, that's how Wired reads the Justice Department's brief in the case. "In the brief, the government defends its use of a search warrant and a grand jury subpoena to obtain the private encryption keys for Lavabit's email service and website, and tacitly impugns Texas-based proprietor Ladar Levison for shutting down the site and thwarting the FBI's surveillance plans," the publication reports.

-Between January and June 2013, the U.S. government issued almost 11,000 requests to Google for user information -- roughly 42 percent of the global total requests to Internet providers, the company reported last week. India came in a distant second with 2,700 government requests for data, Google said. And those numbers are conservative, the search giant was quick to point out: "And these numbers only include the requests we're allowed to publish," Google said in a blog post, referring to gag orders such as those that accompany National Security Letters issued by the U.S. government.

-Activist hackers linked to the collective known as Anonymous have secretly accessed U.S. government computers in multiple agencies and stole sensitive information in a campaign that began almost a year ago, according to a story published by Reuters last week. The publication said it saw a confidential FBI memo linking the group to a slew of intrusions that exploited vulnerabilities in Adobe's ColdFusion Web application development software. The disclosure of the memo follows a series of stories broken by investigative journalist Brian Krebs regarding recent data breaches involving ColdFusion weaknesses, including a hack at the National White Collar Crime Center, PR Newswire, Adobe, and a limo service that catered to the rich and famous.

-California has shut down a host of Web sites that spoofed the state's official insurance exchange under ObamaCare. According to The Hill, the state shuttered at least 10 sites designed to lure unsuspecting insurance-seekers to the phony sites, using similar words and phrases as the state's official site -- CoveredCA.com.

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.