GW CSPRI Newsletter

November 26, 2012

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. 27, 7:30 a.m. - 9:30 a.m., **Leveraging Public-Private Partnerships to Protect Critical Infrastructure** - A discussion about the lessons learned by DOE, DHS and their private sector partners for collaborating effectively to enhance national security. Discussion topics include an enhanced perspective on the current national security vulnerabilities that can be alleviated by private-public partnerships, and how cyber information sharing between the public and private sector can work under existing authorities. Speakers include Matthew Light, program manager, Office of Electricity Delivery & Energy Reliability, U.S. Department of Energy; Samara N. Moore, national security staff, cybersecurity director for critical infrastructure, Executive Office of the President; Thad Odderstol, critical infrastructure protection cyber security program, Department of Homeland Security; Mark Engels, enterprise technology security and compliance director, Dominion. National Press Club, 529 14th Street NW. More information.

-Nov. 28, 10:00 a.m. - 12 noon, **Homeland Security: A Look Back, and Ahead** - The Homeland Security Policy Institute and the Center for Strategic and International Studies

will collaborate on a discussion featuring Senator Joseph Lieberman, Chairman of the Senate Homeland Security and Governmental Affairs Committee. Senator Lieberman will look back and ahead, addressing key past events as well as homeland security challenges for the future. Other speakers include Dr. Steven Knapp, president, The George Washington University; Frank Cilluffo director, HSPI; and Rick "Ozzie" Nelson, director, Homeland Security and Counterterrorism Program, CSIS. The George Washington University, Jack Morton Auditorium, 805 21st St. NW. More information.

-Nov. 29, 7:00 p.m. - 10:00 p.m., **CharmSec Meetup** - Part of the CitySec movement, this is a monthly informal meetup of information security professionals in Baltimore. Slainte Irish Pub and Restaurant, 1700 Thames Street, Baltimore, MD. More information.

-Nov. 30, 1:00 p.m. - 5:00 p.m., **Privacy Multistakeholder Process: Mobile Application Transparency** - The Department of Commerce's (DOC) National Telecommunications and Information Administration will hold another in a series of meetings regarding consumer data privacy in the context of mobile applications. American Institute of Architects Building, 1735 New York Avenue NW, Washington, DC. More information.

-Dec. 5, 1:00 p.m. - 2:00 p.m., **Nine Critical Threats Against Mobile Workers** - In this Webinar, FS-ISAC and Marble Cloud look at the 9 critical security threats that are affecting mobile workers today, and the solutions businesses can implement to ensure they're protected. More information.

-Dec. 7-16, **SANS Cyber Defense Initiative 2012** - This event will feature more than 25 courses in IT security, security management, IT audit, software developer, and computer forensics. Hilton Washington, 1919 Connecticut Avenue, NW. More information.

-Dec. 11-13, **6th Annual Conference on Security Analysis and Risk Management** - This year's conference theme is "Professionalizing Security Risk Management." Specific subject areas will include the following: Community risk, critical infrastructure risk, and cybersecurity risk. George Mason University - Arlington Campus, Founders Hall, 3351 Fairfax Drive, Arlington, Va. More information.

Legislative Lowdown

-Rep. Ed Markey (D-Mass.) urged House Energy and Commerce Committee chairman Rep. Fred Upton (R-Mich.) in a letter last week to pass a bill aimed at securing the nation's electrical grid from cyberattacks, The Hill reports. Markey underscored the rising cyber threat the electric grid faces and described how it could take months to restore electricity after a crippling cyberattack.

He cited a recently declassified National Research Council report published five years ago that warned how a cyberattack could result in thousands of deaths if it disabled the power grid during a heat wave or cold spell.

-A Senate proposal touted as protecting Americans' e-mail privacy has come under controversy. CNET reporter Declan McCullagh reported Tuesday that the bill, which would update the 1986 Electronic Communications Privacy Act, had been quietly rewritten to give government agencies more surveillance power than they possess under current law. McCullagh reported that Sen. Patrick Leahy had reshaped his legislation in response to law enforcement concerns. Sen. Leahy, however, disputed the facts in McCullagh's article and published a response on his website: "The rumors about warrant exceptions being added to ECPA are incorrect. . . . The whole thrust of my bill is to remedy the erosion of the public's privacy rights under the rapid advances of technology that we have seen since ECPA was first enacted thirty years ago. In particular, my proposal would require search warrants for government access to email stored by third-party service providers – something that of course was not contemplated three decades ago." In response, McCullagh then reported that his original article was correct and that Sen. Leahy had abandoned his previous position "in response to a deluge of criticism." George Washington University law professor and CSPRI researcher Orin Kerr noted that "whether Leahy actually had that view and immediately caved, or Declan's first story was just wrong, it seems that the end result . . . is that Senator Leahy doesn't support the language after all." The bill, H.R. 2471, is scheduled for markup and a vote in the Senate Judiciary Committee this Thursday, November 29.

Cyber Security Policy News

-The dust-up over the proposed privacy law changes comes amid increasingly contentious legal battles over privacy rights in the digital age. A story published on the front page of The New York Times this week delves into several cases coursing through the state courts on warrantless wiretapping of cell phones. It notes that judges and lawmakers across the country are wrangling over whether and when law enforcement authorities can peer into suspects' cellphones, and the cornucopia of evidence they provide. A Rhode Island judge threw out cellphone evidence that led to a man being charged with the murder of a 6-year-old boy, saying the police needed a search warrant. A court in Washington compared text messages to voice mail messages that can be overheard by anyone in a room and are therefore not protected by state privacy laws. In Louisiana, a federal appeals court is weighing whether location records stored in smartphones deserve privacy protection, or whether they are "business records" that belong to the phone companies.

In related news, a New York state appellate court recently ruled that a company does not have the right to access a former employee's personal iPhone during discovery in employment litigation, according to InsidePrivacy. As a financial analyst for AllianceBernstein, L.P., William Atha used his personal iPhone to contact clients, and he stored some clients' contact information on the iPhone. Shortly after Atha left for another firm, AllianceBernstein sued him for breach of employment contract, alleging that he misappropriated the firm's confidential information and used it to solicit clients for his new employer. During discovery, AllianceBernstein

sought Atha's iPhone call logs. The state trial court directed Atha to deliver his iPhone to AllianceBernstein's counsel. On November 15, the New York Appellate Division reversed the trial court, concluding that ordering production of Atha's iPhone "is tantamount to ordering the production of his computer," and that the iPhone "would disclose irrelevant information that might include privileged communications or confidential information." The appellate court ordered Atha to deliver his iPhone to the court for the judge "to determine what if any information contained on the iPhone is responsive to plaintiff's discovery request."

-The U.S. Embassy in Paris on Wednesday "categorically" denied claims in a French magazine report that the U.S. government was behind a hacking attack against computers in the French president's palace earlier this year, the Associated Press writes. The French government also played down the report in L'Express magazine. Many countries — including France and the United States — see cyber-attacks as a major threat in the 21st century, and have sought to boost their defenses against intrusions into their computer systems. An array of reported hacking attacks recently in places like Iran and Saudi Arabia have highlighted the menace. According to L'Express, hackers masquerading as Facebook friends of presidential palace employees duped them into giving up internal passcodes, then used them to spread a computer worm on Elysee Palace computers in May, including one used by then-President Nicolas Sarkozy's chief-of-staff.

-Gov. Nikki R. Haley said on Tuesday that South Carolina officials had not done enough to stop computer hackers who recently stole millions of personal financial records. The New York Times reports that the cyberattack, which resulted in the theft of 3.8 million Social Security numbers and 387,000 credit and debit card numbers, was the largest ever against a state government agency. the computer security firm Mandiant released a report with new details about the attack. Hackers broke into the agency's computer system by sending state employees spam e-mail that contained an embedded link. If employees clicked on the link, software was activated on their computers that stole their user names and passwords, Mandiant found. Using this information, the hackers were able to log in as tax officials and steal the data. The report revealed two basic security flaws: state employees did not need multiple passwords and user names to obtain sensitive tax data, and the state did not encrypt Social Security numbers, which could have reduced the harm if any were stolen.

-Several senior police officials and the former deputy interior minister of Georgia have been arrested on suspicion of spying on former opposition leaders and attempting to influence the result of October's parliamentary elections. The arrests come after new prime minister Bidzina Ivanishvili's coalition swept to power at the election, ending the nine-year rule of the government of president Mikheil Saakashvili, who remains in his post until October 2013.

-President Barack Obama has issued new agency standards for protecting classified information from insider threats. Federal News Radio reports that in a Presidential Memorandum issued last week, Obama provided the heads of executive branch departments and agencies the new National Insider Threat Policy as well as the minimum standards to be employed by each agency in standing up its own insider-threat programs. Details on the new policy and the standards

were not made public. In an October 2011 executive order, the President created the Insider Threat Task Force charged with setting government-wide policy for the "deterrence, detection and mitigation" of insider threats. The order also called on the task force to create minimum standards governing agencies' individual insider-threat programs.

-The FBI is reminding shoppers to be wary of Internet fraud during the holiday shopping season. Some of the most frequent scams that tend to increase in frequency and sophistication around the holidays include creating fraudulent auction sales, reshipping merchandise purchased with a stolen credit card, selling fraudulent or stolen gift cards through auction sites at a discounted price and using phishing e-mails to advertise brand-name merchandise for bargain prices or e-mails to promote the sale of merchandise that is counterfeit. The FBI said one of the most common scams involves fly-by-night websites created to sell specific items in high demand. "Typically, the cardholders never receive the product, but the credit card information they entered is used for fraudulent purchases," the FBI warned an advisory issued last week. "It is important to only make purchases with companies and sellers who have a history and can be identified when searching reviews and ratings."

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.