GW CSPRI Newsletter

January 27, 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

-On January 29, CSPRI hosts a talk by David Medine, Chair of the Privacy and Civil Liberties Board (PCLOB), with ample opportunity for questions and answers afterwards. As many readers know, the Privacy and Civil Liberties Board (PCLOB) issued its "Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court" on January 23. CSPRI's Privacy and Civil Liberties project page points to, among other relevant items, a short list of the Board's dozen recommendations and also a summary of points made by President Obama in his talk of January 17 about NSA surveillance. Chairman Medine will discuss the Board's report and recommendations on the NSA telephony metadata program and reform of the operations of the Foreign Intelligence Surveillance Court. He will also discuss the role of the Board going forward overseeing federal counterterrorism programs to ensure they strike the right balance between national security and privacy and civil liberties.

The event will take place in the Betts Auditorium of GW's Marvin Center, 800 21st St. NW, from 6:00 pm to 7:30 pm on Wednesday, January 29. Register for it now at this link to reserve your seat.

Events

-Jan. 28, 8:30 a.m., **State of the Net 2014** - The 10th Annual State of the Net Conference is the largest Internet policy conference in the nation. The 2014 State of the Net will focus on the enormous Internet policy challenges facing the next session of Congress, the Obama Administration, and the Internet community. The Newseum, 555 Pennsylvania Ave NW. More information.

-Jan. 28, 10:00 a.m., **A Roadmap for Hackers? Documents Detailing HealthCare.gov Security Vulnerabilities** - The House Committee on Oversight and Government Reform will hold a hearing. This hearing will examine the security testing of HealthCare.gov, including the adequacy of that testing, and the concerns HHS raised regarding the sensitive nature of Security Control Assessments (SCAs) conducted by contractors prior to the site being launched on October 1, 2013. At the hearing, members will vote to go into Executive Session, which would close the hearing to the public and the press. Witnesses will include Kevin Charest, Ph.D., chief information security officer, U.S. Department of Health & Human Services; and Milton Shomo, principal information systems engineer, cyber operations, The MITRE Corporation. Rayburn House Office Bldg., Room 2154. More information.

-Jan. 30, 7:00 p.m. - 10:00 p.m., **CharmSec Meetup** - An informal gathering of security professionals in the Baltimore area. Heavy Seas Alehouse, 1300 Bank St., Baltimore, Md. 21231. More information.

-Jan. 28-30, **2014 Cybersecurity Innovation Forum** - The goal of this event is to identify a principle-driven roadmap for the realization of an active cyber defense through integration of trusted computing, information sharing, and security automation technologies. Baltimore Convention Center, One West Pratt Street Baltimore, Maryland 21201. More information.

-Jan. 31, 1:30 p.m. - 3:30 p.m., **National Strategy for Trusted Identities in Cyberspace (NSTIC) Public Meeting** - NIST is soliciting applications from eligible applicants to pilot online identity solutions that embrace and advance the NSTIC vision: that individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity credentials to access online services in a manner that promotes confidence, privacy, choice, and innovation. Specifically, the Federal government seeks to initiate and support pilots that address the needs of individuals, private sector organizations and all levels of government in accordance with the NSTIC Guiding Principles that identity solutions will be (1) privacy-enhancing and voluntary, (2) secure and resilient, (3) interoperable, and (4) cost-effective and easy-to-use. NIST will fund pilot projects that are intended to test or demonstrate new solutions, models or frameworks that are not widely available in the marketplace today. Registration is required. NIST, 100 Bureau Drive, Gaithersburg, MD, 20899. More information.

-Feb. 4, 10:15 a.m., **Privacy In a Digital Age: Preventing Data Breaches and Combating Cybercrime** - The Senate Judiciary Committee will hold a hearing. Witnesses will include John J. Mulligan, executive vice president and chief financial officer, Target Corporation; Delara Derakhshani, policy counsel, Consumers Union; Edith Ramirez, chairwoman, Federal Trade

Commission; William Noonan, deputy special agent in charge, Criminal Investigative Division, U.S. Secret Service; Mythili Raman, acting assistant attorney general, Criminal Division, United States Department of Justice. Dirksen Senate Office Bldg., Room 226. More information.

-Feb. 5, 1:30 p.m., **System and Conscience: NSA Bulk Surveillance and the Problem of Freedom** - The Global Internet Freedom and Human Rights Distinguished Speaker Series hosts Yochai Benkler, the Berkman Professor of Entrepreneurial Legal Studies at Harvard Law School, and faculty co-director of the Berkman Center for Internet and Society at Harvard University. Microsoft Innovation & Policy Center, 11th Floor, 901 K Street, NW. More information.

-Feb. 6, 6:30 - 8:00, **OWASP NoVa Meetup** - A meeting of the Northern Virginia chapter of the Open Web Application Security Project. Meetings are free and open to anyone interested in learning more about application security. Systems Engineer Jerry Walton will discuss "Securing Wireless Channels in the Mobile Space." Living Social, 11600 Sunrise Valley Drive, Reston, VA, 20136.

Cyber Security Policy News

-Top encryption and information security academics are calling for the Obama administration to prevent spy agencies from conducting massive surveillance on people and weakening cybersecurity standards, The Hill reports. "In an open letter published on Friday, 50 top scholars from around the country called for the aggressive programs at the National Security Agency (NSA) to be reformed. Signers to the letter included authors, think tank fellows and professors from Yale, Harvard and the Massachusetts Institute of Technology, among other schools."

Meanwhile, The White House rejected several of the dozen recommendations in a report from an oversight board that concluded the government's surveillance program is illegally collecting phone records of Americans and recommended the practice be discontinued. ABC News writes that the report by the Privacy and Civil Liberties Oversight Board comes one week after President Obama introduced his suggestions for reforming the National Security Agency's surveillance practices, including transferring the storage of metadata away from the government. "The PCLOB's majority maintains that the Bush and Obama administrations have subverted the law, applying a section of the PATRIOT Act which the administration claims allows the NSA to collect and store vast troves of data on Americans' phone calls," the publication writes. "What the government has been doing, the panel says, 'bears almost no resemblance' to the text of Sec. 215 of the PATRIOT Act, and is therefore illegal." (The Board's chairman will speak at GW Wednesday evening – register to attend at http://www.eventbrite.com/o/cyber-security-policy-and-research-institute-1099000527?s=21330237.)

Republican leaders appear to be seizing on the issue. The National Journal notes that last week the Republican National Committee passed a resolution urging Republicans in Congress to pass legislation that would restrict the National Security Agency's sweeping data-collecting muscle. "The short, 500-word proclamation espouses several libertarian ideals before asking Republican lawmakers to form a special committee to investigate domestic surveillance practices and 'hold accountable those public officials who are found to be responsible for this unconstitutional surveillance," the story observes. The National Journal said the RNC's stance "also could signal a libertarian-leaning shift in the way Republican operatives hope to appeal to voters in coming elections."

-A federal judge in California who ruled last year that the government's use of ultra-secret National Security Letters is unconstitutional has defied her own ruling by enforcing other NSLs in the wake of that judgment, Wired.com writes. "U.S. District Judge Susan Illston ruled last March that the letters — a kind of self-issued FBI subpoena that comes with a gag order on the recipient — are an unconstitutional impingement of free speech, and ordered the government to stop using them," Wired's Kim Zetter writes. "She also ordered the government to cease enforcing the gag provision in other cases in which an NSL had already been issued. Despite the ruling, the government has continued to attempt to enforce NSLs and gag orders even against the same company that successfully got NSLs ruled unconstitutional."

-Lawmakers have united in their indignation over Target's historic data breach, according to Politico. "At least three Senate committees want a piece of the recent catastrophe that exposed millions of customers' credit cards, email addresses and other personal information," writes Jessica Meyers and Kevin Cirilli. "Lawmakers, who have failed repeatedly to pass data security legislation, see an opportune moment to revisit the controversial topic. And more important, it offers Congress a well-publicized chance to play the good guys."

Even more recent disclosures of breaches in the retail over the weekend are likely to add fuel to the fire. Independent security blogger Brian Krebs reported Saturday that Michaels Stores, an arts & crafts chain that has more than 1,200 stores nationwide, may have suffered a security breach that exposed customer cardholder data. Michaels issued a statement saying that it "recently learned of possible fraudulent activity on some U.S. payment cards that had been used at Michaels, suggesting that the Company may have experienced a data security attack." The U.S. Secret Service has confirmed it is investigating.

-Earlier this week, a huge chunk of Chinese websites were redirecting users to a blank page run by a company in the US. According to The New York Times, 500 million Chinese Internet users found they were unable to access websites hosted either in China or overseas that were part of top level domains like .com, .net, and .org. "Technology experts say China's own Great Firewall — the country's vast collection of censors and snooping technology used to control Internet traffic in and out of China — was most likely to blame, mistakenly redirecting the country's traffic to several sites normally blocked inside China, some connected to a company based in the Wyoming building," The Times' Nicole Perlroth reports. "The China Internet Network Information Center, a state-run agency that deals with Internet affairs, said it had traced the problem to the country's domain name system. One of China's biggest antivirus software vendors, Qihoo 360 Technology, said the problems affected about three-quarters of the country's domain-name system servers."

-A security breach at a Web portal for the U.S. Department of Homeland Security has exposed private documents and some financial information belonging to at least 114 organizations that bid on a contract at the agency last year. "The letter was sent to organizations that bid on a 2013 contract to help DHS’s Science & Technology division develop new communications technologies for first responders," writes KrebsOnSecurity.com. "According to DHS, the documents were downloaded from a department Web portal by unauthorized persons outside of the agency, although it hasn’t yet determined the cause or source of that access. A spokesperson for DHS said that as a result of this unauthorized access, 520 documents including white papers/proposals, decision notification letters, documents regarding contract and award deliverables and other supporting materials were improperly accessed."

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.