GW CSPRI Newsletter

October 7, 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.

Call for Submissions: Attention CSPRI followers! CSPRI's blog, The CSPRI Byte, wants to hear from YOU! Have an interesting take on a topic in cyber security? Share it! Email your proposed articles to CSECblog@gwu.edu to get published!

Contents

Events

-Oct. 8, 9:00 a.m. - 10:30 a.m., **The Future of Cloud Services** - The Information Technology and Innovation Foundation will host a panel discussion. The speakers will include Rep. Greg Walden (R-Oreg.); Daniel Castro (ITIF); and Jim Blakely, cloud service division director, Intel. 1101 K Street, NW, 610 A. More information.

-Oct. 8-9, **Cyber Maryland 2013** - This two-day event at the epicenter of the nation's cybersecurity innovation and education, will create opportunities for networking and idea sharing amongst the many cyber leaders and professionals across the country, including: federal, state and local government agencies, academic institutions, cybersecurity entrepreneurs, and industry leaders of research and development. Baltimore Convention Center, One West Pratt Street, Baltimore, Md. 21201 More information.

-Oct. 8, 6:00 p.m. - 7:30 p.m., **Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia** - The New America Foundation will host a discussion of the book by the same title. NAF, Suite 400, 1899 L St., NW. More information.

-Oct. 9, 9:30 a.m. - 5:00 p.m., **NSA Surveillance: What We Know; What to Do About It** - The CATO Institute will hold a series of discussions. Keynote speakers include: Senator Ron Wyden (D-OR), member of the Senate's Select Committee on Intelligence; Rep. Justin Amash (R-MI); Rep. F. James Sensenbrenner (R-WI). Panelists include: Siobhan Gorman, Wall Street Journal; Spencer Ackerman, The Guardian; Barton Gellman, Washington Post; Charlie Savage, New York Times; Jameel Jaffer, ACLU; Laura Donohue, Georgetown University Law Center; David Lieber, Google; Jim Burrows, Silent Circle; Sharon Bradford-Franklin, Privacy and Civil Liberties Oversight Board; Jim Harper, Director of Information Policy Studies, Cato Institute; and Julian Sanchez, Research Fellow, Cato Institute. 1000 Massachusetts Ave, NW, Hayek Auditorium. More information.

-Oct. 10, 11:30 a.m. - 1:30 p.m., **Cybersecurity: A National Imperative, a Government Trust** - This panel of senior government leaders will discuss the role government plays in preserving the security of the country's most critical infrastructure. Speakers will include Maria Roat, FEDRAMP Director, GSA; John Streufert, director, federal network resilience, Department of Homeland Security; Adam Sedgewick, senior information technology policy advisor, National Institute of Standards and Technology. Clyde's of Gallery Place, 707 7th Street, NW. More information.

-Oct. 11, 8:30 a.m. - 10:30 a.m. **The National Cybersecurity Framework: - The First Major Milestone** - US Telecom will host an on site and webcast panel discussion. Patrick Gallagher, head of the National Institute of Standards and Technology (NIST), will give an opening speech, followed by a panel discussion moderated by Inside Cybersecurity reporter Charlie Mitchell, and including Donna Dodson, deputy cyber security advisory, NIST; Adam Sedgewick, senior information technology policy advisor, NIST; Robert Dix, vice president of government affairs, Juniper Networks; Sara Andrews, chief network security officer, Verizon Communications; and Rosemary Leffler, chair, communications sector coordinating council and director, national security, AT&T. Larry Clinton, president and CEO of Internet Security Alliance, will give a closing speech. Breakfast will be served. First Amendment Room, National Press Club, 529 14th St., NW. More information.

-Oct. 12-13, **Battle Hack** - PayPal Battle Hack is a 10-city hack-a-thon series for software and mobile app developers to come test their skills and change the world. Bring your best ideas for developing apps for social good, find some team members onsite, and make something awesome. Win one city heat, and you advance to the World Finals where 10 teams battle for $100,000 USD. Register, team up, and prove you're the Best Hackers in Washington during this 2 day hack-a-thon. 1133 15th St NW. More information.

-Oct. 14-16, **First IEEE Conference on Communications and Network Security** - This two-day conference features a number of keynotes, panel discussions and technical discussions on cybersecurity. Gaylord National Hotel and Convention Center, 201 Waterfront Street, National Harbor, MD 20745. More information.

-Oct. 16, 1:00 p.m. - 2:30 p.m., **Sharing Among Nations** - A Webcast discussion sponsored by the Industrial Control Systems Information Sharing and Analysis Center (ISC-ISCA) and FIRST (the Forum for Incident Response and Security Teams). The discussion will be led by a panel, including Larry Castro (Chertoff Group), Peter Allor (FIRST) and Oscar Acevedo (Guatemala CERT) – on the global implications of knowledge sharing. More information.

-Oct. 16-17, **Cybersecurity Symposium: Protect, Defend, Educate** - This two-day conference will consist of training for government and industry security professionals while simultaneously offering keynote speakers education, training, essential networking opportunities, and a technology exposition. The symposium sessions will have a special emphasis on security challenges facing today's security professionals and cyber awareness training for security professionals responsible for protecting sensitive and classified information from the ever increasing threats of mobile devices, espionage, terrorism, and cyber-attacks. BWI Airport Marriott, 1743 West Nursery Road, Linthicum, MD 21240. More information.

Legislative Lowdown

-Sen. Dianne Feinstein (D-Calif.), the chairwoman of the Senate Intelligence Committee, is vowing to kill a competing bill offered by Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.), who has promised to champion legislation that would end the National Security Agency's controversial program to collect records on all U.S. phone calls. According to The Hill, Feinstein has argued that the phone data program is critical for protecting national security, and that if it had been the norm back in 2001, it could have prevented the 9/11 attacks. "She acknowledged that leaks about the extent of the NSA's surveillance activities have eroded public trust in the agency, and she said some reforms are needed," The Hill's Brandon Sasso wrote. "She is preparing her own legislation that would require more transparency about the NSA's activities but would preserve the NSA's bulk collection of phone data."

Leahy's bill, outlines of which have been circling among lawmakers, is to be called the "USA Freedom Act," and is set to be co-sponsored by Rep. Jim Sensenbrenner, the Wisconsin democrat and House Judiciary ranking member who was among the main authors of the USA PATRIOT Act. According to an outline of the bill obtained by Politico, the purpose of the legislation would be “to rein in the dragnet collection of data by the National Security Agency and other government agencies, increase transparency of the Foreign Intelligence Surveillance Court, provide businesses the ability to release information regarding FISA requests and create an independent constitutional advocate to argue cases before the FISC."

Cyber Security Policy News

-Revisiting an interesting bit of history, Wired.com's David Kravets traces the legal justification for the NSA's domestic spying programs back to an obscure case of common purse snatching back in 1979, long before the emergence of the commercial Internet that most of know and depend upon today. "The perp, Michael Lee Smith, was apprehended weeks later, thanks in part to the police department’s use of a machine known as a 'pen register' to track the threatening

phone calls the assailant had started making to his victim," Kravets writes. "The court wrangling that followed, however, would continue for three years, and eventually land on the docket of the U.S. Supreme Court. In 1979 the court upheld Smith's conviction, and his 10-year prison term. Almost 35 years later, the court's decision — in a case involving the recording of a single individual's phone records — turns out to be the basis for a legal rationale justifying governmental spying on virtually all Americans. Smith v. Maryland, as the case is titled, set the binding precedent for what we now call metadata surveillance. That, in turn, has recently been revealed to be the keystone of the National Security Agency's bulk collection of U.S. telephone data, in which the government chronicles every phone call originating or terminating in the United States, all in the name of the war on terror."

Wired's coverage of the obscure case is a prologue to another piece about the U.S. government's efforts to gather personal information on NSA whistleblower Edward Snowden. In August, Lavabit -- one of the companies that Snowden used for email -- said it was closing its doors, noting that the company's founder Ladar Levison did not want to "become complicit in crimes against the American people." The New York Times writes that Levison briefly staged a protest against the government's request for the encryption key that would unlock Snowden's messages: Instead of sending the key digitally, Levison reportedly sent over five, 2,560 character SSL encryption keys, printed on an 11-page printout on illegible 4-point type. The court overseeing the case was apparently not amused, and levied a $5,000 a day fine on Levison, who ultimately relented and handed over digital copies of the keys.

-Prosecutors in New York last week seized control over the Silk Road, a sprawling underground Web site that has earned infamy as the "eBay of drugs." On conjunction with the seizure, federal agents in San Francisco arrested the Silk Road's alleged mastermind. Prosecutors say 29-year-old Ross William Ulbricht, a.k.a "Dread Pirate Roberts" (DPR), was charged with a range of criminal violations, including conspiracy to commit drug trafficking, and money laundering. The Silk Road is an online black market that as late as last month was hosting nearly 13,000 sales listings for controlled substances, including marijuana, LSD, heroin, cocaine, methamphetamine and ecstasy. In a bizarre twist, the government's complaint also details a scenario in which Ulbricht allegedly hired a Silk Road vendor to kill another Silk Road member who was threatening to release information on the identities of several top users of the site. In the online chat allegedly between Ulbricht and the hired hit man, Ulbricht reportedly complained about the $150,000 price tag of the hit, saying he'd previously ordered a hit for as little as $80,000. According to a separate complaint (PDF) unsealed in Maryland last week, the guy Ulbricht hired in the original $80,000 hit job was in fact a federal agent.

The Silk Road is not available via the regular Internet. Rather, it is only reachable via the Tor network, an anonymity network that bounces its users' communications across a distributed network of relays run by volunteers all around the world. It turns out that the NSA has been trying to penetrate the Tor network for several years, with limited success. The Wall Street Journal's AllThingsD blog notes that in a statement posted online last week, the Director of National Intelligence James Clapper acknowledged NSA's "'interest in tools used to facilitate anonymous online communication.' However, media coverage of the work fails to point out that 'the Intelligence Community's interest in online anonymity services and other online communication and networking tools is based on the undeniable fact that these are the tools our

adversaries use to communicate and coordinate attacks against the United States and our allies.' And that's the traffic that the NSA is hoping to capture and analyze. Clapper argues in the post that intelligence agencies are interested only in '… communication related to valid foreign intelligence and counterintelligence purposes.'"

-Wondering what the impact of the federal shutdown may be having on the government's cybersecurity posture? Many people are asking the same question, and coming away with different answers after hearing one response from Steven VanRoekel, the federal chief information officer. VanRoekel gave an interview with The Wall Street Journal, in which he was quoted as saying that among the 800,000 federal government employees furloughed during the partial shutdown that started on Oct. 1 are hundreds -- if not thousands of IT and security personnel that VanRoekel maintains are vital. Van Roekel told the WSJ he advised agencies to exempt cybersecurity staffers from the furloughs, but that it was up to each agency to decide which employees are essential, and many agencies decided to keep only skeleton staffs to maintain vigilance over federal systems. But Federal News Radio cites some experts calling these fears overblown.

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.