GW CSPRI Newsletter

March 4, 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. To change your subscription settings, please email cspriaa@gwu.edu with your request.

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

-Mar. 5-6, **Big Data Conference** - This conference brings together the key government and industry experts who are shaping the direction of big data research and development across the Federal Government. They will provide an in-depth understanding of federal agency strategy and plans, the status and forecast for key big data initiatives, and the latest tools and technologies being developed to exploit the massive amounts of information being collected at the federal level. Holiday Inn Rosslyn at Key Bridge, 1900 North Fort Myer Drive, Arlington, Va. More information.

-Mar. 5-7, **Software Assurance Forum** - The Software Assurance Program of the Department of Homeland Security's Office of Cybersecurity and Communications (CS&C) co-sponsors SwA Forums semi-annually with organizations in the Department of Defense and the National Institute for Standards and Technology. The purpose of the forums is to bring together members of government, industry, and academia with vested interests in software assurance to discuss and promote integrity, security, and reliability in software. National Institute of Standards & Technology, 100 Bureau Dr., Gaithersburg, Md. More information.

-Mar. 6, 10:30 a.m., **DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure** - The House Homeland Security Committee will hold a hearing. Witnesses will include Janet Napolitano, secretary, U.S. Department of Homeland Security; Anish Bhimani, chairman, Financial Services Information Sharing and Analysis Center; Gary W. Haynes, chief information officer, Centerpoint Energy; and Dean Garfield, president and chief information officer, Information Technology Industry Council. Cannon House Office Bldg., Room 311. More information.

-Mar. 6-8, **IAPP Global Privacy Summit** - Join privacy, data protection and security experts from around the globe for three days to discuss privacy challenges and delve into new concepts in privacy. Washington Marriott Wardman Park, 2660 Woodley Rd. NW. More information.

-Mar. 7, 8:00 a.m. - 1:30 p.m., **The Cyber 9/12 Project: Cyber Statecraft After a Catastrophe** - The Atlantic Council and Science Applications International Corporation (SAIC) will discuss the day-after response to a cyber incident. A small group of experts will represent various sectors, including government, finance, telecom, and press to discuss the decision-making process in light of a serious cyber security breach. During the course of the half-day conference, the scenario will continue to evolve, forcing experts to focus on key priorities and sector-specific concerns during a major cyber attack against the United States. RSVP to press@acus.org to attend. Knight Studio at the Newseum, 555 Pennsylvania Avenue, NW. More information.

-Mar. 7, 6:00 p.m. - 7:45 p.m., **Mindforge Meetup** - An informal gathering of hackers, inventors, engineers, techies, developers and makers who love all things IT and security. Everyone is welcome – from advanced hardware hackers to those who would like to learn what can be done with these new technologies in the arts, sciences, healthcare, gaming, academia, and business venture opportunities. This month's event is a hands-on class called "BASH scripting 101 for Penetration Testers." Bechtel Conference Center, 1801 Alexander Bell Dr., Reston, Va. More information.

-Mar. 8, **Tech@state: Internet Freedom** - The U.S. Department of State's Office of eDiplomacy is proud to present its 10th Tech@State event on March 8th, 2013, in conjunction with the Global Internet Freedom and Human Rights Distinguished Speaker Series of the George Washington University Law School. Day One by hearing opening remarks from senior officials from both the State Department and GW's Law School, followed by a keynote address from Andrew McLaughlin, the former Deputy Chief Technology Officer of the United States from

2009-2011. The rest of the morning will be dedicated to a plenary panel discussion which will focus on how the latest technological tools can be employed not only to foster and enhance free and open access to the Internet, but also repress it. Jack Morton Auditorium, George Washington University, 805 21st St. NW. More information.

-Mar. 13, 10:45 a.m. - 4:00 p.m., **ISACA Meetup -** The monthly meetup of the Central Maryland chapter of ISACA, a group of dedicated volunteers offering IT, information systems, security and audit and financial professionals local education events, resource sharing, advocacy, and professional networking. CCMIT, 692 Maritime Boulevard, Linthicum Heights, Md. More information.

-Mar. 14, 6:30 p.m. - 8:00 p.m., **OWASP NoVA Meetup -** Meetings of the Open Web Application Security Project are open to anyone interested in learning more about software security. 11600 Sunrise Valley Dr., Reston, Va. More information.

-Mar. 18-20, **7th Annual IFIP WG11.10 International Conference on Critical Infrastructure Protection -** This conference features numerous talks on cybersecurity, including workforce, power grid cyber attacks, cyber threats posed by aging infrastructure and cyber warfare. Room 403, Marvin Center, George Washington University, 800 21st St. NW. More information.

-Mar. 19-21, **FISSEA Conference -** The Federal Information Systems Security Educators' Association (FISSEA), founded in 1987, is an organization run by and for information systems security professionals to assist federal agencies in meeting their information systems security awareness, training, education, and certification responsibilities. FISSEA became a NIST program under the National Initiative for Cybersecurity Education (NICE) in March 2011. National Institute of Standards and Technology (NIST), 100 Bureau Drive, Gaithersburg, Md. More information.

-Mar. 19-20, **Cybersecurity & Infrastructure Protection -** This symposium brings together the senior level U.S. government and industry cybersecurity experts from the critical infrastructure sectors – including the energy, homeland security, defense, transportation, IT/communications, postal, emergency services & banking, and finance who creating the latest tools, techniques and solutions for protecting national resources from internal and external cyber terrorism. Sheraton Pentagon City, 900 S. Orme Street, Arlington, Va. More information.

Legislative Lowdown

-House Intelligence Committee Chairman Mike Rogers (R-Mich.) said last week he is aiming to wrap up talks with the White House and privacy advocates about measures in his information-sharing cybersecurity bill by April so it can move to a markup, The Hill reports. The Intelligence Committee Chairman and ranking member Rep. Dutch Ruppersberger (D-Md.) re-introduced a cybersecurity bill this month, the Cyber Intelligence Sharing and Protection Act (CISPA), that is designed to remove the legal hurdles preventing private companies and the government from sharing intelligence about cyber threats with one another in real time. Last year the White House issued a veto threat the day before the bill went to the House floor for a vote, arguing that it lacked sufficient privacy protections and measures addressing security gaps in the computer systems of critical infrastructure. The bill ultimately passed the House last spring and went untouched in the Senate.

-Senator John D. Rockefeller IV (D-W.Va.) last week introduced a bill called the Do-Not-Track Online Act of 2013, designed to give Internet users the right to opt out of online tracking. According to The New York Times, the bill would require the Federal Trade Commission to establish standardized mechanisms for people to use their Internet browsers to tell Web sites, advertising networks, data brokers and other online entities whether or not they were willing to submit to data-mining. The bill would also require the F.T.C. to develop rules to prohibit online services from amassing personal details about users who had opted out of such tracking.

Cyber Security Policy News

-Cyberspies linked to China's military targeted nearly two dozen US natural gas pipeline operators over a recent six-month period, stealing information that could be used to sabotage US gas pipelines, according to a restricted US government report and a source familiar with the government investigation. In an piece published last week, The Christian Science Monitor wrote that from December 2011 through June 2012, cyberspies targeted 23 gas pipeline companies with e-mails crafted to deceive key personnel into clicking on malicious links or file attachments that let the attackers slip into company networks, says the Department of Homeland Security (DHS) report. The report does not mention China, but the digital signatures of the attacks have been identified by independent cybersecurity researchers as belonging to a particular espionage group recently linked to China's military.

Much of the discussion at the giant RSA Security conference last week in San Francisco centered around this and a rash of other reports about Chinese cyberspies breaking into U.S. government and commercial entities to swipe intellectual property, trade and state secrets. But according to The SANS Institute, a research and training group based in Bethesda, Md., Clearly, the uncontrolled anxiety over cyberattacks from China misses the point: Don't worry about China. Worry instead if the pitiful state of your information security defenses will allow any attacker to wield nothing more than malicious email attachments to steal valuable intellectual property or even state secrets. Information Week quotes several SANS experts telling companies wringing their hands over the hacks to turn the focus inward. "The continuous China bashing simply reflects the inability of watchers to see evidence of the stealthier attacks coming from many nations that may take a different approach to penetrating our telecommunications and banking and power systems and stealing our national wealth," SANS's research director Alan Paller told the publication. "The number of bad actors, spread among nations, terrorists, anarchists and criminals, is so great that their identity is not as important as what we do to defend our systems -- because they usually exploit the same weaknesses."

In its newsletter to subscribers, SANS wrote: "The recent focus on China as the source of cyberespionage attacks against US government and industry organizations has not addressed the underlying issue - that US computer systems remain vulnerable to attacks. The focus on the Chinese-attributed attacks also neglects the "stealthier attacks coming from many nations that may take a different approach to penetrating [sensitive] systems." The point is not who is launching the attacks; the point is whether or not systems are robustly protected from cyberattacks. The vast majority of attacks are launched using basic exploits. Australia's Defense Signals Directorate and the US's national Security Agency (NSA) put together a list of 35 cyber defense techniques that successfully block more than 85 percent of known attacks. In fact, just four of the measures - whitelisting; restricting PCs and serves to run only approved applications; quickly patching applications and operating systems; and minimizing the number of administrator accounts - can prevent a significant number of targeted attacks."

- The Homeland Security Department is distributing details about hacks to critical infrastructure operators in response to continuing cyber assaults that, according to people familiar with the cases, involve recent breaches at Apple, Microsoft and other technology firms. NextGov writes that the intelligence sharing also fulfills part of a Feb. 12 cybersecurity executive order. The policy required agencies to exchange information on threats to private computers running critical U.S. assets and asked businesses to do the same. The bulletin notifies energy suppliers, hospitals and other sectors vital to society that confidential guidance is available on “ongoing malicious cyber activity against U.S. government and private sector entities.” To receive the sensitive information, the companies or their Internet service providers must use "secure channels," according to the alert.

DHS also wants government and private sector workers to jump on cyber security threats with a new online one-stop resource for career, training and education information, Government Security News reports. The agency launched what it calls a “national initiative for cyber security careers and studies” through its new National Initiative for Cybersecurity Careers and Studies (NICCS) program. NICCS, said the agency, was developed in close partnership between DHS, the National Institute of Standards and Technology, the Office of the Director of National Intelligence, the Department of Defense, the Department of Education, the National Science Foundation, and the Office of Personnel Management. DHS said the initiative will help it retain and continually train top talent, while it moves to create more opportunities for Cyber staff and continue support for its Centers of Academic Excellence around the country that cultivate a growing number of professionals with expertise in various disciplines, including Cyber security.

The DHS and other agencies are struggling to find talented cybersecurity experts, in large part because the demand for them far outstrips the supply, according to The National Journal's Brian Fung. "The United States doesn't have nearly enough people who can defend the country from digital intrusions. We know this, because cybersecurity professionals are part of a larger class of workers in science, technology, engineering, and math--and we don't have nearly enough of them, either," Fung writes. "We're just two years into President Obama's decade-long plan to develop an army of STEM teachers. We're little more than one year from his request to Congress for money to retrain 2 million Americans for high-tech work (a request Republicans blocked). And it has been less than a month since the Pentagon said it needed to increase the U.S. Cyber Command's workforce by 300 percent--a tall order by any measure, but one that's grown even more urgent since the public learned of massive and sustained Chinese attempts at cyberespionage last month. Where are Cyber Command's new hires going to come from? Even with so many Americans out of work, it isn't as though there's a giant pool of cyber professionals tapping their feet, waiting to be plucked up by federal agencies and CEOs who've suddenly realized they're naked in cyberspace. In fact, over the next couple of years, the manpower deficit is only going to get worse as more companies come to grips with the scale of the danger."

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.