GW CSPRI Newsletter

March 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. 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

Legislative Lowdown

Cyber Security Policy News

Events

-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. The George Washington University, Marvin Center, Room 403, 800 21st St. NW. More information (PDF).

-Mar. 19, 6:30 p.m., **ISSA DC Meetup: SCADA Cyber Security for the Smart Grid** - The National Capital Chapter of the ISSA is comprised of information security professionals located in the Washington D.C. Metropolitan Area. Members are actively involved in information security in government agencies, the military, non-profit organizations, and in large and small companies. Dewan Chowdhury will give a lecture on how the power grid/smart grid works, the fundamentals of power delivery, and cyber threats to the power/smart grid. Government Printing Office, 732 N. Capitol St. NW. More information.

-Mar. 19, 10:00 a.m., **ECPA Part I: Lawful Access to Stored Content** - The House Judiciary Committee's Subcommittee on Crime, Terrorism, Homeland Security and Investigations will hold a hearing on the Electronic Communications Privacy Act. Witnesses will include Elana Tyrangiel, Department of Justice; Orin Kerr, The George Washington University Law School; Richard Littlehale, Tennessee Bureau of Investigation; and Richard P. Salgado, Google. Rayburn House Office Bldg., Room 2141. More information.

-Mar. 19, 1:00 p.m. - 2:00 p.m., **Privacy and Information Security Update** - The American Bar Association will host a teleconferenced panel. Panelists include Benita Kahn, Vorys, Sater, Seymour and Pease LLP; Harriet P. Pearson, Hogan Lovells US LLP; and Marcy Wilder, Hogan Lovells US LLP. More information (PDF).

-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, 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.

-Mar. 20, 2:00 p.m., **Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure** - The House Homeland Security Committee wil hold a hearing. Speakers include Frank J. Cilluffo, director, Homeland Security Policy Institute and co-director, Cyber Center for National and Economic Security, The George Washington University; Richard Bejtlich, chief security officer and security services architect, Mandiant; Ilan Berman, vice president, American Foreign Policy Council; Martin Libicki, senior management scientist, RAND Corp. Cannon House Office Bldg., Room 311. More information.

-Mar. 20, 6:00 p.m. - 9:00 p.m., **NovaInfosec Meetup** - An informal meetup of security professionals and whitehat hackers involved in the federal government and other regulated verticals like critical infrastructure, finance, and healthcare. Velocity Five Landsdowne, 19286 Promenade Dr., Leesburg, VA. More information.

-Mar. 21, 9:00 a.m., **Cyber Attacks: An Unprecedented Threat to U.S. National Security** - The House Committee on Foreign Affairs's Subcommittee on Europe, Eurasia, and Emerging Threats will host a hearing. Speakers include Richard Bejtlich, chief security officer and security services architect, Mandiant, and Greg Autry, senior economist, Coalition for a Prosperous America. Rayburn House Office Bldg., Room 2172. More information.

-Mar. 21, 10:00 a.m., **Protecting Small Businesses Against Emerging and Complex Cyber-Attacks** - The House Committee on Small Business's Subcommittee on Health & Technology will hold a hearing. Invited witnesses include William H. Weber, senior vice president & general counsel, Cbeyond; Justin Freeman, corporate counsel, Rackspace; and Phyllis A. Schneck, chief technology officer, public sector, McAfee. Rayburn House Office Bldg., Room 2360. More information.

-Mar. 22, 12:00 p.m. - 2:00 p.m., **Who is Bashing Whom?: China, Cyber-Attack, Democracy, and Retaliation** - This free lunch event, organized by the Trade and Internet Governance Project of GW, and the Minerva Initiative of the Department of Defense, will examine recent hacking news stories from several different perspectives: cyber-security, economics, trade, human rights, and global governance. Speakers include Ellen Nakashima of The Washington Post, Dr. Irving Lachow, Director, Technology and Security, Center for a New American Security, Delphine Halgand, Washington Office Director, Reporters without Borders, and Michael Nelson, Bloomberg Government. The George Washington University Elliott School of International Affairs, Lidner Commons, Room 602, 1957 E Street, NW. More information.

-Mar. 28, 4:00 p.m. - 5:30 p.m., **The Release of the Tallinn Manual: The International Law Applicable to Cyber Warfare** - The Atlantic Council will celebrate the release of a new treatise on the international law applicable to cyber warfare. Speakers will include Artur Suzik, director of the NATO Cooperative Cyber Defence Center of Excellence; Professor Michael Schmitt, chairman of the International Law Department at the US Naval War College; and Harvey Rishikof, chair of the American Bar Association Standing Committee on Law and National Security Advisory Committee. The University Club Ballroom, 1135 16th Street, NW. RSVP and more information.

Legislative Lowdown

- The Obama administration is drawing up plans to give all U.S. spy agencies full access to a massive database that contains financial data on American citizens and others who bank in the United States, according to a Treasury Department document seen by Reuters. The proposed plan represents a major step by U.S. intelligence agencies to spot and track down terrorist networks and crime syndicates by bringing together financial databanks, criminal records and military intelligence. The plan, which legal experts say is permissible under U.S. law, is nonetheless likely to trigger intense criticism from privacy advocates.

Cyber Security Policy News

-When James Clapper, the country's top intelligence official, visited Capitol Hill this week to discuss the major threats facing America, he put cyberattacks at the top of the list, National Journal reports. The lengthy discussion of cybersecurity marked a change from testimony Clapper gave in 2012 and 2011. In his annual assessments of worldwide risks in the two previous years, digital threats were mentioned only briefly and were further down on the list of dangers. Cybersecurity is a top priority this year for President Obama, who was planning a meeting Wednesday in the White House Situation Room with business executives to discuss the issue. Concerns are growing about a potential attack that could cripple the nation's infrastructure. Clapper, the director of national intelligence, told a Senate panel that it would be "hard to overemphasize" the significance of the threat. In that same hearing, Gen. Keith Alexander, the head of the U.S. Cyber Command at the Pentagon, told lawmakers that in the last six months, there have been 140 cyberattacks on Wall Street.

The testimony came as President Obama was hosting CEOs from banks and other top Wall Street firms, including JPMorgan Chase & Co., The LA Times writes. The White House wouldn't say who would be meeting with the president until after the event, but JPMorgan Chase & Co. confirmed that Jamie Dimon, its chairman and CEO, would attend in the wake of a wave of attacks on the bank by hackers. The so-called denial-of-service attacks, which overwhelm websites with phony requests, prevented Chase customers from accessing their online banking accounts.

-Hackers last week posted online the Social Security numbers, birthdays, previous addresses and other sensitive information on top government officials, including First Lady Michelle Obama, FBI Director Robert Mueller and U.S. Attorney General Eric Holder. The hackers claimed they'd accessed the data after pulling the targets' credit reports online.

As it turns out, the credit reports were being pulled by criminals fraudulently accessing credit reports at annualcreditreport.com, a Web site mandated by a 2003 anti-identity theft law that was designed to give consumers easier access to their credit reports, according to KrebsOnSecurity.com. The blog's author, Brian Krebs, showed how such fraud was being resold via fraudulent underground Web sites, and for this he paid a dear price. In a blog post published Friday, Krebs related how hackers upset over the story attacked his Web site, spoofed a letter from the FBI to his hosting provider, and then spoofed his cell phone number in a fake hostage call to the police. As documented by The Washington Post, Krebs became the latest victim of "SWATing," a highly dangerous stunt increasing with alarming regularity, in which hackers use caller ID spoofing services to trick authorities into responding to a phony hostage crisis.

-In other hacking reporters news, a Reuters.com editor maintained his innocence after being suspended with pay on Friday following a federal indictment on charges he aided members of the Anonymous hacking collective, Reuters reports. Matthew Keys, 26, a deputy social media editor, was indicted on Thursday by a federal grand jury in Sacramento, California, on three

criminal counts. The alleged events occurred before he joined Thomson Reuters, the indictment indicated.

-If you're going to run a Web site that seeks to index security vulnerabilities, you'd better make sure the site itself is secure: The federal government's official catalog of software vulnerabilities was taken offline last week after administrators discovered two of its servers had been compromised by malware that exploited a software vulnerability, Ars Technica reports. The National Vulnerability Database is maintained by the National Institute of Standards and Technology and has been unavailable since late last week, according to an e-mail sent by NIST official Gail Porter and published on Google+. The database was restored over the weekend.

-North Korea last week blamed South Korea and the United States for cyberattacks that temporarily shut down websites this week at a time of elevated tensions over the North's nuclear ambitions. Experts, however, indicated it could take months to determine what happened and one analyst suggested hackers in China were a more likely culprit. According to The Associated Press, Internet access in Pyongyang was intermittent on Wednesday and Thursday of last week, and Loxley Pacific Co., the broadband Internet provider for North Korea, said it was investigating an online attack that took down Pyongyang servers. A spokesman for the Bangkok-based company said it was not clear where the attack originated. North Korea's official Korean Central News Agency blamed the shutdown on the United States and South Korea, accusing the allies of expanding an aggressive stance against Pyongyang into cyberspace with "intensive and persistent virus attacks."

-Treasury Secretary Jack Lew will warn Chinese leaders this week that the country's cyber spying is endangering the country's growing trade relationship with the United States, writes The Hill. "This is an issue of very high concern and importance to the president," a senior Treasury Department official told reporters on a call previewing Lew's trip to China. "You can expect Secretary Lew to discuss our growing concerns about cybersecurity when he meets with Chinese officials, highlighting that this issue has become a growing challenge to our economic relationship."

CSPRI Announcements

-Dr. Costis Toregas, CSPRI Associate Director, recently gave the keynote lecture at a conference of the European Environment Agency, held March 4-6 in Dublin, Ireland. He spoke about inherent risks in sharing data across organizations and ways to use public-private partnerships to promote effective use of satellite data and GIS in making policy choices for the environment.

-Computer Science 6534, Cybersecurity in Governance, has to date only been open to CyberCorps students. A graduate level course that is also available to upper lever undergraduates with permission of the instructor, it will now be available to all GW students who

have passed a course in network security. It will be presented as a hybrid course this summer (June 24-August 17) with almost all of the material presented online. One session at the end of the course will be in face-to-face mode for the student presentations. Thus, in addition to traditional students, it may fit the needs of working professionals who want to take a for-credit course on this topic without giving up a lot of time from their daytime jobs.

A highlight of the course is the set of video presentations by various employees and contractors of the US Government and computer security practitioners from the private sector as they describe their challenges and opportunities in addressing cybersecurity issues. This course will introduce the concept of risk analysis and will present policies and structure for cybersecurity in the US government, including management charts. The course will address a variety of cyber issues including mobile and social networking security, cloud computing security, forensic analysis, and malware attacks. It will review information sharing processes within the government and the various cybersecurity policies. Students will acquire skills that can be applied to cybersecurity management.

The course is available for registration under Online Courses at http://my.gwu.edu/mod/pws/courses.cfm?campId=7&termId=201302&subjId=CSCI. Those who are not yet GW students and do not wish to apply for a degree program but just to take the course should follow the standard procedures outlined at http://www.gwu.edu/take-class to be admitted as a non-degree student.

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.