GW CSPRI Newsletter

December 10, 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

-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. 10, 5:30 p.m. - 8:30 p.m., **NoVA Hackers Association Meetup** - This informal group of security professionals from around the NoVA/DC area coordinates one or two monthly events – an evening meetup with presentations on the second Monday of the month and various lunch or bar meetup. *Note that the location has changed since last week's newsletter.* QinetiQ, 11091 Sunset Hills Road, Reston, VA. More information.

-Dec. 11, 1:00 p.m. - 2:30 p.m., **Insuring for Data Security Threats: Everything a Business Lawyer Wants to Know But Is Afraid To Ask** - The American Bar Association will host a webcast and teleconferenced panel discussion. The speakers will be John Black (Boundas Skarzynski Walsh & Black), Erich Bublitz (Admiral Insurance Company), Janice Hugener, Winston Krone (Kivu Consulting), and Edward Morse (Creighton University School of Law). 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.

-Dec. 12, 7:30 a.m. - 4:00 p.m., **Federal Cross-Agency Management Conference** - This event will draw federal, state & local, association, and educational experts and managers together to explore interagency models, cross-sector collaboration, cultural challenges, leadership trends, and best practices. Speakers include Chris Inglis, deputy director, National Security Agency; Jim Cash, deputy commander, Coast Guard Cyber Command; Lev Kubaik, director, National Intellectual Property Coordination Center. George Washington University, Marvin Center, Grand Ballroom, 3rd Floor, 800 21st St. NW. More information.

-Dec. 12, 11:00 a.m. - 4:00 p.m., **ISACA Central Maryland Chapter Meeting** - The ISACA Central Maryland Chapter invites you to our annual joint training holiday event with the Associate of Government Accountants (AGA) on Wednesday, December 12, 2012. There are two topics for this training event: Governance and Risk in Cloud Computing and Achieving Data Warehouse Nirvana: The Critical Role of Information Controls. Snyder's Willow Grove Restaurant, 841 North Hammonds Ferry Road, Linthicum, MD, United States, 21090. More information.

-Dec. 13, 10:00 a.m., The House Intelligence Committee (HIC) will hold a closed business meeting. The agenda includes "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE". The announcement is available on the HIC website. See also, story titled "House Intelligence Committee Report Finds Huawei and ZTE Could Undermine US National Security" in TLJ Daily E-Mail Alert No. 2,461, October 15, 2012. Location: Room HVC-304, Capitol Visitor Center.

Announcements

-Dr. Carl E. Landwehr, Lead Research Scientist at George Washington University's Cyber Security Policy and Research institute (CSPRI), has been named an Institute of Electrical and Electronics Engineers (IEEE) Fellow. He is being recognized for contributions to cybersecurity. Dr. Landwehr's research achievements include contributions to security modeling and vulnerability characterization. Over the past decade, he initiated, guided, and managed major research programs for the National Science Foundation (NSF), IARPA, and DARPA. Dr. Landwehr joined CSPRI last spring. Most recently, he worked with CSPRI Director Lance Hoffman to organize a successful Principal Investigators meeting for nearly 400 researchers in the NSF Secure and Trustworthy Cyberspace program.

Legislative Lowdown

-The Senate Judiciary Committee is set to consider S. 1223 (PDF), the Location privacy Act of 2011, sponsored by Senator Al Franken. The bill would establish important privacy protections for cellphone users and require affirmative consent for the collection or disclosure of location data by service providers. Frankin said last week that the bill would "put an end to GPS stalking." The committee is expected to debate amendments to the legislation on Thursday and vote on the bill itself on Dec. 13.

Cyber Security Policy News

-Information on one of Japan's newest rockets was stolen from a desktop computer that was infected with malware, The New York Times reports. The Japan Aerospace Exploration Agency said that the virus in a computer at its Tsukuba Space Center northeast of Tokyo was found to be secretly collecting data and sending it outside the agency. The agency said that after the virus was detected by antivirus software on Nov. 21, it conducted an emergency sweep for viruses that showed no other computers at the center had been infected. The agency said it was unclear if the virus was a cyberattack. Japanese defense companies, however, have been recent targets of similar information-stealing viruses, some previously traced to China. .

-A measure granting the government expansive power to intercept electronic communications in the United States without a warrant is set to expire this month, setting up a sharp debate in the Senate over how to balance privacy against national security, The Washington Post reports. The government uses the measure, contained in a law known as the FISA Amendments Act, to intercept e-mails and telephone calls of foreigners located overseas under a blanket approval issued once a year by a special court. But communications of U.S. citizens talking with the foreigners also are being scooped up.

-The FBI is investigating a breach at Nationwide Insurance, where hackers recently accessed the sensitive information of about one million people, including policy and non-policy holders, SC Magazine writes. Elizabeth Giannetti, a Nationwide spokeswoman, confirmed that the incident, where a "portion" of the company's computer network was breached, affects customers, as well as people that requested quotes from Nationwide. Victims span all 50 states. So far, various officials have confirmed with media outlets that about 30,000 people in Georgia were affected, as well as more than 12,000 in South Carolina. The California Department of Insurance announced Wednesday in a release that approximately 5,050 residents of the Golden State were impacted and that information, such as names, Social Security numbers and other personal identifying data, were stolen in the breach, though no credit card information was accessed.

-Negotiations concerning an accord involving the United States, Russia and other countries requiring that each nation provide advance warning of government cyber operations that might otherwise spark unintentional conflict collapsed on Friday after Russia dissented. The 57-nation Organization for Security and Cooperation in Europe failed to reach the unanimous consensus needed to adopt the resolution. It was aimed at building trust and open communication to avoid cyberwar. The politically-binding agreement by the United Nations-recognized organization would have operated similarly to the way that Russia and America decades ago drew red lines to avoid nuclear war.

-In other international cyberpolicy news, Delegates from the United States are running out of time to bury proposals that could have a major effect on the Internet as a United Nations treaty conference heads into its final week. According to The Hill, the top item on the U.S.'s agenda is to confine the scope of the international treaty to telecommunications networks, so its regulations only apply to major operators like AT&T and Verizon. Members of the U.S. delegation, led by Ambassador Terry Kramer, are pushing back against proposals from Russia and other countries that want to include measures in the treaty that apply to the Internet. But with just days until the conference wraps up on Dec. 14, the matter remains unresolved.

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.