GW CSPRI Newsletter

March 5, 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

-Mar. 7, 10:00 a.m., **Cybersecurity: The Pivotal Role of the Communications Networks** - The Subcommittee on Communications and Technology has scheduled a hearing. Room 2123, Rayburn House Office Bldg. More information.

-Mar. 7-9, **IAPP Global Privacy Summit** - Privacy, security and data protection experts from around the globe discuss and debate the latest privacy issues and challenges. Washington Marriott Wardman Park, 1900 Connecticut Ave. NW. More information.

-Mar. 7-9, **Military Cyber Security** - This conference brings together senior level military, government and industry experts who are defining the requirements and shaping the solutions in cyber security and computer network defense. Holiday Inn Rosslyn at Key Bridge, 1900 North Fort Myer Drive, Arlington, VA. More information.

-Mar. 13, 7:30 a.m. - 9:30 a.m., **Advancing the Intelligence Community: Harnessing the Power of Cloud Computing** - This panel will explore the impact that cloud computing has already had on security communities, and what lies ahead. Speakers will include Jim Heath, senior science advisor to the director, National Security Agency; Terry Roberts, INSA cyber council chair, Carnegie Mellon University, and former deputy director of Naval Intelligence. National Press Club, 529 14th Street, NW. More information.

-Mar. 13, 10:30 a.m., **The Freedom of Information Act: Safeguarding Critical Infrastructure Information and the Public's Right to Know** - The Senate Judiciary Committee will hold a hearing. Witness will include Melanie Pustay, director, Office of Information Policy, Department of Justice; Miriam Nisbet, director, Office of Government Information Services, National Archives and Records Administration; Kenneth Bunting executive director, Missouri School of Journalism, National Freedom of Information Coalition; and Jerry Ensminger, retired Marine sergeant, Camp Lejeune Marine Base. Dirksen Senate Office Building, Room 226. More information.

-Mar. 14, 8:30 a.m. - 5:00 p.m., **Doing Business in a Global Economy: What is a Trusted Supply Chain?** - This all-day conference will seek to answer several questions about the supply chain security problem, including: Which policy and legislation approaches are best in addressing this problem; What are new policies and models for trusting suppliers, their supply chains and systems? Are current policies and those under consideration regarding suppliers and counterfeiting really going to be effective? What are the unintended consequences of physical and cyber intersections for supply chains? Hilton Crystal City, Crystal City at National Airport, 2399 Jefferson Davis Hwy., Arlington, VA More information.

-Mar. 14-17, CyberWatch Mid-Atlantic Collegiate Cyber Security Competition – Held at Johns Hopkins University's Applied Physics Lab in Laurel, MD, in the Kossiakoff Center, this popular competition, expected to draw 500 students, educators and even high schoolers eager to learn about cyber security, will open with an all-day Speaker Symposium on security aspects of Healthcare IT on Wednesday March 14. There is no prior registration required, and details, including speakers and topics, can be found at http://www.midatlanticccdc.org/CCDC/2012-speaker-symposium/. (CSPRI provides some management services to CyberWatch).

Announcements

-On Mar. 21, 12 noon - 2:00 p.m., the CSPRI will continue its 2011-12 Seminar Series with a discussion session titled, "Developing the Cybersecurity Workforce - Different Perspectives." Two noted experts will present opposing points of view:

View 1: We Need Lots of People, Chosen and Developed Properly: "A holistic approach to developing the cybersecurity workforce is needed, based on careful integration of workforce development strategies into a plan that involves educators, career professionals, employers, and policymakers. A critical element of a robust cybersecurity strategy is having the right people at every level to identify, build and staff the defenses and responses. And that is, by many accounts, the area where we are the weakest." (From "Holistically Building the Cybersecurity Workforce" by Lance J. Hoffman, Diana L. Burley, and Costis Toregas, IEEE Security & Privacy Magazine, March-April 2012).

View 2: A Human in the Loop May Not be a Failsafe but a Liability ". . . We security professionals make a claim to the salary we draw because of our 'judgment' and 'skill.' I suggest that the demand for that judgment, that skill will soon wither in the face of the second [machine to machine] economy. We see computers doing things right now—Amazon or Netflix recommendations, Zillow estimates—that a decade ago would have required a human to intervene. The networked security militias of the second economy do not wait for humans, and it's possible to argue that for the scale and speed at which a networked security collective operates, a human in the loop is not a failsafe but a liability" (see http://geer.tinho.net/geer.suitsandspooks.8ii12.txt).

Presenting the first point of view will be Diana Burley, Associate Professor in the Graduate School of Education and Human Development at The George Washington University (GW). Her research and scholarly activities advance understanding of knowledge management initiatives, IT/cyber security education and workforce development strategies, and the impact of IT- enabled change on individuals, organizations and society (social informatics). Presenting the second point will be Daniel Geer, who is currently the chief information security officer for In-Q-Tel, a not-for-profit venture capital firm that invests in technology to support the intelligence community. Visit http://cyberworkforce.eventbrite.com/ to RSVP for this event.

Legislative Lowdown

-A group of Republican senators on Thursday unveiled their response to an omnibus cybersecurity bill now circulating in the Senate, taking a decidedly more hands-off approach to the regulation of private industry. In comparison to the competing cyber bill by Sens. Lieberman and Collins, the GOP proposal -- dubbed the SECURE IT Act (PDF), would grant no new authorities to the Department of Homeland Security or any other agency to enforce cyber safeguards on privately-owned critical infrastructure such as power grids and Internet service providers.

According to Computerworld, the Collins-Lieberman bill would allow the secretary of the U.S. Department of Homeland Security to designate some private networks as critical infrastructure and require them to submit security plans to the agency. But the SECURE IT Act has no such regulations, instead focusing on encouraging private companies and the federal government to share more information about cyberthreats, sponsors said. The new bill would give legal protections to private groups that share information about cyberthreats. The older bill also includes some information-sharing provisions, but critics have said legal protections would cover only businesses that share information with the U.S. government. The new bill would also increase the prison terms for many cybercrimes, with the prison sentence for knowingly accessing a computer without authorization and obtaining national defense information increased from 10 to 20 years. The penalty for intentionally accessing a federal computer without authorization or a computer containing financial records would increase from one to three years, or from five to 10 years if the offense was committed for purposes of private financial gain.

Cyber Security Policy News

-The FBI has turned off 3,000 GPS tracking devices in the wake of a recent Supreme Court ruling, according to reporting by The Wall Street Journal. The January 23, 2012 decision said that placing a GPS device on an individual's car qualifies as a search and therefore requires a warrant. These devices were often stuck underneath cars to track the movements of the car owners. In U.S. v. Jones, the Supreme Court ruled that using a device to track a car owner without a search warrant violated the law.

-Colorado federal authorities have decrypted a laptop seized from a bank-fraud defendant, rendering unnecessary a judge's order that the defendant unlock the hard drive so the government could use its contents as evidence against her. Wired.com's Threat Level blog reports that the development ends a contentious legal showdown over whether forcing a defendant to decrypt a laptop is a breach of the Fifth Amendment right against compelled self incrimination.

-The command codes for the International Space Station were among the data sets compromised recently at NASA. The revelations came from NASA Inspector General Paul Martin, who detailed to lawmakers more than 5,000 computer security breaches in the last two years. The purloined space station codes were on an unencrypted laptop that was stolen in March 2011. Martin's full testimony and report on the breaches is available here (PDF).

-The director of the FBI told an annual gathering of cyber-security professionals on Thursday that the agency needs the private sector to help combat what he believes is becoming the nation's No. 1 threat, the Associated Press reports. Speaking at the annual RSA Security Convention in San Francisco last week, FBI Director Robert Mueller said the dangers posed by organized cyber-crime, rogue hacktivists and computer breaches backed by foreign governments have become a focus for the FBI. Counterterrorism is still the agency's top priority, Mueller said, but the agency has retooled to prepare for Internet-based aggressors. Cyber-squads in every FBI field office now monitor for crimes ranging from mortgage and health care fraud to child exploitation and terror recruiting, he said.

-The National Security Agency has begun a pilot program to demonstrate secure classified communications over commercial equipment, but it is having trouble finding standards-based off-the-shelf products that are interoperable and meet its needs, Government Computer News writes. The standards and protocols exist to provide the security that NSA requires, but they are not being implemented consistently by vendors, Margaret Salter, a technical director in NSA's Information Assurance Directorate, said Feb. 29 at the RSA Conference. Network World describes the technology in greater detail, which is said currently depends on Google Android smartphones, though the NSA contends it doesn't want to be wedded to any particular smartphone operating system. The agency's current "Fishbowl" phones, as they are called, are beefed-up highly secured Motorola Android smartphones that use double-encryption for voice traffic and a unique routing scheme for 3G network traffic back to the NSA first for security purposes.

-The National Institute of Standards and Technology released the first draft of special publication 800-53 revision 4 last week. The update was a year-long effort by NIST, the Defense Department and the intelligence community, Federal News Radio reports. SP 800-53, as it's commonly known, tries to address the current state of cyber threats, vulnerabilities and risks.

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.