THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY
AND RESEARCH INSTITUTE
Thoughtful Analysis of Cyber Security Issues

GW CSPRI Newsletter

May 23, 2011

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

Upcoming Events

-May 24, 10:00 a.m. - 5:00 p.m., The Social Security Administration's Future Systems Technology Advisory Panel will meet to report to and provide the Commissioner of Social Security independent advice and recommendations on the future of systems technology and electronic services at the agency five to ten years into the future. Hyatt Regency Crystal City, 2799 Jefferson Davis Highway, Arlington. More information.

-May, 24, 6:30 p.m. - 8:00 p.m., **Overview of the NIST Risk Management Framework as Described in SP 800-37** - What was the Guide for the Security Certification and Accreditation of Federal Information Systems is now the Guide for applying the Risk Management Framework to Federal Information Systems. This talk, given by Lance

Kelson from the Department of Interior, will address the differences between the two frameworks. MITRE, Room 1N100, 7515 Colshire Dr., McLean, Va. More information.

-May 25, 10:00 a.m., **Cybersecurity: Innovative Solutions to Challenging Problems** - The House Judiciary Committee's Subcommittee on Intellectual Property, Competition and the Internet and Subcommittee on Crime, Terrorism and Homeland Security will hold a hearing. Rayburn House Office Building, Room 2141. More information.

-May 25, 10:00 a.m. - 12:00 noon, **IRS E-File and Identity Theft** - The House Oversight and Government Reform Committee's Subcommittee on Government Organization, Efficiency, and Financial Management will hold a hearing. Rayburn House Office Building, Room 2154. More information.

-May 25, 10:00 a.m. - 12:00 noon, **Protecting Information in the Digital Age: Federal Cybersecurity Research and Development Efforts** - The House Science Committee's Subcommittee on Technology and Innovation and Subcommittee on Research and Science Education will hold a hearing. Rayburn House Office Building, Room 2318. More information.

-May 25, 1:30 - 3:30 p.m., **Cybersecurity: Assessing the Immediate Threat to the United States** - The House Oversight and Government Reform Committee Subcommittee on National Security, Homeland Defense and Foreign Operations will hold a hearing. Location: Rayburn House Office Building, Room 2154. More information.

-May 25, 2:00 p.m., **The Spread of Tax Fraud by Identity Theft: A Threat to Taxpayers, A Drain on the Public Treasury** - The Senate Finance Committee's Subcommittee on Fiscal Responsibility and Economic Growth will hold a hearing. Dirksen Senate Office Building, Room 215. More information.

May 26, 1:00 p.m., **Cloud Computing Security** - The US Telecom will host a free Webcast seminar. Speakers will include **Glenn Biery Jr.** and **John Hatem**, cloud security consultants for Verizon. More information.

June 2, **Cyber Security Conference & Expo** - This free government cyber security event will review government and industry best practices for protecting data, strengthening identity and authentication procedures, and keeping systems tightly locked. Speakers will include **Stephen Elky**, deputy director for IT services, Library of Congress; **Patrick Howard**, director/chief information security officer, Nuclear Regulatory Commission; **Michele Iversen**, chief information system security officer, Department of Education; **John Kropf**, deputy chief privacy officer, Department of Homeland Security liaison; **Chuck McGann**, corporate information security officer, U.S. Postal Service. Ronald Reagan Building, The Pavilion Room, 1300 Pennsylvania Ave., NW. More information.

Legislative Lowdown

-**Senate Judiciary Committee Chairman Patrick Leahy** (D-Vt.) last week unveiled a legislative proposal to update one of the nation's dominant privacy laws, a statute enacted back in 1986, before the dawn of the commercial Internet and many of the technologies we rely on each day. Leahy's bill would amend the Electronic Communications Privacy Act to ensure that the government must obtain a warrant before accessing an individual's email, digital communications or geolocation information. Leahy said the current law's privacy protections are geared more towards networks and computing resources that are physically accessible, while today data is increasingly stored and accessed remotely.

The law has been "out-paced by rapid changes in technology and the changing mission of our law enforcement agencies" since the Sept. 11, 2001, terrorist attacks on the U.S., Leahy said in a statement. "Under the current law, a single email could be subject to as many as four different levels of privacy protections, depending upon where it is stored and when it was sent." Gautham Nagesh writes for The Hill that proposed amendments would -- among other things -- prohibit wireless and remote service providers from voluntarily disclosing the contents of user's email or other electronic communications to the government. It requires a search warrant based on probable cause to access all emails, digital messages, and geolocation data remotely stored.

Cyber Security Policy News

-The new Obama administration policy for tightening global defenses against computer attacks places cybersecurity on equal footing with military and economic threat, Bloomberg reports. The International Strategy for Cyberspace, unveiled at a White House event last week, calls for the U.S. government to work with other countries on standards to protect intellectual property, prevent theft of private information and ensure cooperation among foreign law enforcement agencies when a cybercrime is being investigated. The plan also recommends setting consequences for countries and groups that don't comply with the standards and strengthens the U.S. position on its response to a cyber attack.

Heading up the administration's effort to sell this new strategy abroad is Chris Painter, a cybersecurity veteran from the U.S. Justice Department who was picked to lead a newly created State Department Office of the Coordinator for Cyber Issues. GovInfoSecurity features an interview with Painter, who discusses the role he and his office will play in promoting cybersecurity diplomacy.

-Initial tests of a controversial cellular broadband network planned by Reston, Va. based **LightSquared** showed the company's system knocked out Global Positioning System receivers used by first responders. NextGov.com writes that the wireless provider tested its system last month at Holloman Air Force Base, N.M., with the participation of state police vehicles and county ambulances, both of which experienced outages from the company's cell tower. The Defense and Transportation Departments have serious concerns about the impact LightSquared's national network of 40,000 cell towers will have on GPS receivers. LightSquared maintains the interference is not caused by its system, but by sensitive GPS receivers that "see" into the frequency band the network uses.

-The head of a company that makes a downloadable application enabling users to pinpoint police drunken-driving checkpoints says his sales have doubled after efforts by four senators to restrict such apps, USA Today reports. Steve Croke, CEO of Fuzz Alert, also said he might remove the checkpoint locating capability to prove that the app is not designed to help people drive drunk.

Fuzz Alert joins a number of other mobile applications that are causing concern among lawmakers on Capitol Hill who are already concerned about the privacy implications presented by the ubiquity of mobile technologies, including apps that allow drivers to pinpoint such police enforcement tools as red-light and speeding cameras, speed traps and sobriety checkpoints. Democratic Sens. **Charles Schumer** of New York, **Harry Reid** of Nevada, **Frank Lautenberg** of New Jersey and **Tom Udall** of New Mexico all have asked smartphone makers Apple, Google and Research in Motion to quit selling apps that allow drivers to locate checkpoints, or to disable that function.

-A network engineer found guilty of holding the San Francisco city technology infrastructure hostage three years ago has been released from prison and now faces nearly $1.5 million in fines. In the summer of 2008, Terry Childs was arrested after a lengthy dispute with his boss in which he refused to turn over the pass codes needed to get on the system he designed, which linked the city's various computer operations. Childs ended up giving the passwords to then-Mayor Gavin Newsom after nine days in jail.

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.