GW CSPRI Newsletter

February 13, 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

*-CSPRI EVENT: Feb. 15, 12 noon - 2:00 p.m., **The End of K Street Deals?: Is Netizen Direct Lobbying the New Norm?** - Panelists include Susan Aaronson, Associate Research Professor at GW's Elliott School of International Affairs; Dean C. Garfield, President and CEO of the Information Technology Industry Council; Michael Nelson, Research Associate for the CSC Leading Edge Forum and Visiting Professor of Internet Studies at Georgetown University; and Mitch Glazier, Senior Executive Vice President, Recording Industry Association of America. Lance Hoffman, Director, GW Cyber Security Policy and Research Institute, will facilitate the discussion. Sign up for seminar and the following lunch (provided by CSPRI) at http://netizenlobbying.eventbrite.com.*

-Feb. 15, 7:30 a.m. - 11:25 a.m., **Secure Cyber Operations Start Here: Who Are You and How Can I Be Sure?** - Speakers from the Department of Defense, Health and Human Services and a number of private companies address how they are proceeding to support secure, scalable identity protection and management systems for government enterprises. The Willard InterContinental Hotel, 1401 Pennsylvania Ave NW. More information.

-Feb. 16, 8:15 a.m. - 6:00 p.m., **Gov/Cloud 2012** - A conference on the selection of cloud technologies and services and their secure implementation across the .gov domain. 1400 M Street NW. More information.

-Feb. 16, 10:00 a.m., **DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy** - The House Homeland Security Committee's Subcommittee on Counterterrorism and Intelligence will hold a hearing. Room 311, Cannon Building. More information.

-Feb. 16, 2:30 p.m., **Securing America's Future: The Cybersecurity Act of 2012** - The Senate Homeland Security and Government Affairs Committee will hold a hearing on pending legislation. Room 342, Dirksen Building. This hearing will also be webcast. More information.

Legislative Lowdown

-Rep. Greg Walden (Ore.) said his subpanel -- the House Energy and Commerce subcommittee on Communications and Technology -- will dig into issues like supply-chain vulnerability, hacking and botnet attacks in the year ahead, The Hill reports. The review will begin Wednesday with a cybersecurity hearing that will feature testimony from security experts and industry representatives. Several committees in the House are moving forward with cybersecurity legislation in hopes of bringing a bill to the floor before the election. Leaders in both chambers have largely struck a bipartisan tone on cybersecurity, framing it as a national security matter.

-A bill that assigns the Homeland Security Department key cybersecurity responsibilities and sets up a nonprofit for public-private information sharing unanimously cleared a subcommittee vote last week, writes Federal News Radio. The bill — Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2011 (H.R. 3674) — designates DHS as the "single focal point for protecting federal networks and systems," as well as for private sector critical infrastructure, said bill sponsor Rep. Dan Lungren (R-Calif.), chairman of the Committee on Homeland Security's Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies. The proposal sets up a not-for-profit organization called the National Information Sharing Organization to facilitate voluntary cyber collaboration between the federal government and private entities.

Cyber Security Policy News

-Hackers released the source code for some older products made by security giant Symantec Corp., after the company reportedly declined to give in to extortion demands. Reuters reports that the release followed failed email negotiations over a $50,000 payout to the hacker calling himself YamaTough to destroy the code. The email thread was published on Monday, but the hacker and the company said their participation had been a ruse. YamaTough said he was always going to publish the code, while Symantec said law enforcement had been directing its side of the talks. The incident has raised fears that others could find security holes in the product and

attempt takeovers of customer computers, although Symantec has said the source code is limited to products that are several years old.

-A federal lawsuit filed in Massachusetts could test the question of whether individuals who leave their wireless networks unsecured can be held liable if someone uses the network to illegally download copyrighted content. The lawsuit was filed by Liberty Media Holdings LLC, a San Diego producer of adult content. The company has accused more than 50 Massachusetts people, both named and unnamed, of using BitTorrent file-sharing technology to illegally download and share a gay porn movie.

-The Pentagon is expected to soon clear Apple and Android mobile devices such as commercial tablet computers for use in a range of missions, according to NextGov. Mark Orndorff, program executive officer for mission assurance and network operations at DISA, said the guidelines will cover both Google's Android operating system and Apple's iOS, which powers the iPhone and iPad. The guidelines, expected as soon as this August, may mitigate many of the security concerns that have precluded the devices' widespread use on Defense networks, although restrictions could prevail in some sensitive mission areas.

-Media reports suggest that Iran has cut off access to the Internet, leaving millions of people without access to e-mail and social networks. An individual inside the country told CNET that Facebook, Gmail, Hotmail, and Yahoo email were no longer available. So far the government has not made any announcement about the service interruption, but cyber-sophisticated Iranians are still able to circumvent the government by using proxy servers over VPN connections.

-Privacy advocates filed a federal lawsuit to stop Google from consolidating more than 60 privacy policies across the range of its products. The Electronic Privacy Information Center (EPIC) argues that the combination of information could make users easier targets for behavioral advertisers. The suit alleges Google violated a settlement agreement reached with U.S. regulators last March that requires consent from the user if Google collects information under one privacy policy and then changes the policy. A federal judge granted EPIC an accelerated briefing schedule last week in a bid to give the Federal Trade Commission and EPIC time to weigh in on the matter before the changes take effect on March 1.

-The General Services Administration on Tuesday released extensive new details on FedRAMP, a program the Obama administration hopes will accelerate the adoption of cloud computing and cut security costs, Information Week reports. The GSA-led FedRAMP is a soon-to-be-mandatory government-wide program that standardizes the government's approach to authorizing cloud services for use by federal agencies and monitoring those services to ensure that they continue to meet federal cybersecurity requirements. According to the 47-page concept of operations document, popular collaboration and infrastructure-as-a-service tools will be the first applications to run through the FedRAMP authorization process.

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.