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

GW CSPRI Newsletter

October 31, 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

-Oct. 31, 8:00 a.m. - 5:00 p.m., **7th Annual IT Security Automation Conference** - Hosted by the National Institute of Standards and Technology (NIST), National Security Agency (NSA), Defense Information Systems Agency (DISA), and Department of Homeland Security (DHS). This conference will touch on using specific open standards and new security technologies across various domains of interest including continuous monitoring, software assurance, IT security threats, and network security. Hyatt Regency Crystal City, 2799 Jefferson Davis Highway, Crystal City, Va. More information.

-Nov. 7, 8:00 a.m. - 5:00 p.m., **Government Enterprise Architecture Conference** - Enterprise architecture (EA) practitioners will share strategies for applying EA methodologies to today's top government priorities, including cloud computing, information sharing, cybersecurity, and mobility. Ritz-Carlton Tysons Corner, 1700 Tysons Boulevard Tysons Corner, Va. More information.

-Nov 7, 9:00 a.m. - 2:00 p.m., **Cyber Defense: International Cooperation and Deterrence** - The Center for Strategic and International Studies hosts a discussion on the challenges and opportunities posed by the ideas of cyber deterrence and international cyber defense cooperation, their implications for the transatlantic security relationship, and their possible impact on relations between the alliance and non-NATO powers. CSIS, 1800 K St. NW. More information.

CSPRI Activities

-On Nov. 16, George Washington University's Cyber Security Policy and Research Institute will host a debate on whether cell phone and Internet blackouts by government agencies are unconstitutional and illegal, absent a declared national emergency. Debating for the argument will be Gregory T. Nojeim, senior counsel at the Center for Democracy & Technology and director of its Project on Freedom. Taking the contrary stance will be Paul Rosenzweig, an adjunct faculty member at GW’s Law School and founder of Red Branch Law & Consulting, PLLC. Mr. Rozenzweig formerly served as deputy assistant secretary for policy in the Department of Homeland Security and twice as acting assistant secretary for international affairs. The debate begins at noon. Lunch will be provided at 1 p.m. to accompany a roundtable discussion with the debaters and two commentators, GW University Professor Amitai Etzioni and Dr. Eric Burger, Georgetown University adjunct faculty member. There is no cost to the public but space is limited so register at https://csprieventblackouts.eventbrite.com, where there is also more detail on the speakers. GW Marvin Center, 800 21st St. NW, Room 302.

-On October 27, CSPRI was the academic sponsor for a Washington Post Live breakfast panel discussion on cybersecurity featuring Janet Napolitano, Secretary of the US Department of Homeland Security, and General Michael Hayden, former Director of the CIA, discuss the high-stakes public policy issues around cyber security that are important to us all. Other speakers included Rep. Mac Thornberry (R-TX); Gregory P. Schaffer, Acting Deputy Secretary for Cybersecurity, National Protection and Programs Directorate, Department of Homeland Security; and Tim McKnight, Vice President and CISO, Northrup Grumman Corporation. Material related to the event, including videos of some of the speakers is at http://washingtonpostlive.com/conferences/cybersecurity.

-CSPRI Assistant Director Costis Toregas presented his paper, “Overcoming Barriers to Effective Collaboration,” co-authored with Bob Spear and Vera Zdravkovich, at the ATE PI Conference October 26-28. Professor Toregas discussed his experiences developing partnerships for CyberWatch with the private sector. CyberWatch is a network of more than 75 two and four year academic institutions focusing on increasing the quantity and quality of the cyber security workforce of the nation.

Legislative Lowdown

-Rep. Jim Langevin (D-R.I.), co-founder of the bipartisan Congressional Cybersecurity Caucus, expressed optimism to The Hill recently that some form of legislation to improve the security of private sector networks would pass Congress this year. The White House and Senate appear to be in agreement on both the urgency and broad outline of cybersecurity legislation. At a classified meeting earlier this month Obama administration officials stressed the need to pass legislation to update federal standards this year. White House cybersecurity coordinator Howard Schmidt called the meeting "very encouraging" in a blog post published Friday emphasizing the urgent need for new federal cybersecurity regulations to cover private sectors deemed critical such as utilities, communications providers and financial institutions.

-Sen. Jay Rockefeller (D-W.Va.), chairman of the Senate Commerce, Science and Transportation Committee, sent letters to MasterCard and Visa on Thursday, questioning the credit card companies about a report that they plan to provide customer data to third-party advertisers. The Wall Street Journal reports that the two largest credit-card networks, Visa Inc. and MasterCard Inc., are pushing into a new business: using what they know about people's credit-card purchases for targeting them with ads online. Their plans, if implemented, would represent not only a technological feat—tying people's Internet lives with shopping activities—but also an erosion of the idea of anonymity on the Web. It's an effort by the two companies to profit by selling access to the insights they gather about people with every credit-card transaction.

Cyber Security Policy News

-Computer hackers, possibly from the Chinese military, interfered with two U.S. government satellites four times in 2007 and 2008 through a ground station in Norway, according to a congressional commission. Bloombergs' Tony Capaccio and Jeff Bliss write that the intrusions on the satellites, used for earth climate and terrain observation, underscore the potential danger posed by hackers, according to excerpts from the final draft of the annual report by the U.S.-China Economic and Security Review Commission. The report is scheduled to be released next month.

-The Energy Department paid more than $2 million to recover from several recent cyberattacks, NextGov reports. An annual review of Energy's unclassified cybersecurity observed network weaknesses have increased 60 percent between fiscal 2010 and fiscal 2011, the department's inspector general reports. The security holes include weak access controls, software flaws and poor employee training, among other deficiencies. Tests at 25 facilities, including headquarters, revealed 32 previously unidentified vulnerabilities plus an additional 24 left unresolved from the prior year. The report does not say where the four breaches occurred or name the specific weaknesses discovered elsewhere due to security concerns, the document states.

-The National Security Agency has begun providing Wall Street banks with intelligence on foreign hackers, a sign of growing U.S. fears of financial sabotage, according to a Reuters report. The assistance from the agency that conducts electronic spying overseas is part of an effort by

American banks and other financial firms to get help from the U.S. military and private defense contractors to fend off cyber attacks. NSA Director Keith Alexander, who runs the U.S. military's cyber operations, told Reuters the agency is currently talking to financial firms about sharing electronic information on malicious software, possibly by expanding a pilot program through which it offers similar data to the defense industry. He did not provide further details on his agency's collaboration with banks.

-A security researcher has devised an attack that hijacks nearby insulin pumps so he can surreptitiously deliver fatal doses to diabetic patients who rely on them, The Register writes. The attack on wireless insulin pumps made by medical devices giant Medtronic was demonstrated Tuesday at the Hacker Halted conference in Miami. It was delivered by McAfee's Barnaby Jack, the same researcher who last year showed how to take control of two widely used models of automatic teller machines so he could to cause them to spit out a steady stream of dollar bills. Jack's latest hack works on most recent Medtronic insulin pumps, because they contain tiny radio transmitters that allow patients and doctors to adjust their functions.

-The National Institute of Standards and Technology has expanded its list of standards, guidance, and proposals for Smart Grid Interoperability, according to Federal News Radio. The NIST Framework and Roadmap for Smart Grid Interoperability Standards 2.0 builds upon the first cyber outline the agency released. The previous version laid out the initial plan for transforming the nation's aging electric power system into a network integrating information and communication technologies with a power-delivery infrastructure.

-New research from Carnegie Mellon University's Software Engineering Institute provides further evidence why information security isn't just the problem of an enterprise's IT security organization but of its top non-IT leadership as well, GovInfoSecurity reports. The research reveals that a significant class of insider crimes - theft of intellectual property - results in tangible losses in the form of stolen business plans, customer lists and other propriety information. Researchers from the institute's CERT Insider Threat Center reached that conclusion after analyzing more than 600 cases it has amassed over the past decade. One remarkable finding: much of the pilfering of secrets occurs within 30 days of the insider's last day on the job.

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.