GW CSPRI Newsletter

May 7, 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

-May 8, 10:00 a.m., **Hearing on Identity Theft and Tax Fraud** - Subcommittees of the House Committee on Ways and Means will hold a joint hearing to examine how identity theft contributes to tax fraud, and whether the IRS and the SSA are doing enough to protect SSNs and prevent and detect false returns filed by identity thieves. 1100 Longworth House Office Building. More information.

-May 9, 12:00 noon, **Federal Cyber-Security Regulation: Critical Safety Measure, or Privacy Nightmare?** - This discussion will include viewpoints from Jim Harper, director of information policy studies, Cato Institute; Michelle Richardson, legislative counsel, American Civil Liberties Union; Ryan Radia, associate director of technology studies, Competitive Enterprise Institute. Luncheon to follow. The Cato Institute, 1000 Massachusetts Avenue, NW. More information.

-May 14, 5:00 p.m. – 6:30 p.m., **An Assessment of U.S. Cybersecurity** - General James E. Cartwright, USMC (Ret.), former Vice Chairman of the Joint Chiefs of Staff will share his thoughts on how he hopes U.S. cybersecurity will evolve moving forward --with a focus on

effective deterrence strategies, and a discussion of offensive capabilities. His remarks will place cyber issues and challenges into context, and convey insights relating to cyber strategy. Reception to follow. George Washington University Homeland Security Policy Institute, Elliott School of International Affairs, Seventh Floor, City View Room, 1957 E Street, NW. More information.

-May 16-17, **The Security Summit 2012 East** - The Security Network works closely with an expanding number of companies, countries, military and government agencies and sponsors and other partners to identify and promote rapid adoption of dual-usage security products and services from innovative companies around the world. The event will focus on topics including cybersecurity, anti-terrorism, GIS, port and maritime security, rapid technology fielding and international collaboration. Renaissance Arlington Capital View Hotel, 2800 South Potomac Ave. Arlington, Va. More information.

-May 16-17, **Counter Terror Expo** - This two day conference features several talks about emerging cyber threats, including attacks from hacktivist groups, corporate espionage, supply chain and information sharing. Washington Convention Center, 801 Mt. Vernon Pl., NW. More information.

-May 16, 12:00 noon – 2:00 p.m., **"Is America Ready to Vote on the Internet? Concerns for National Security".** The expert panelists will include Prof. Alex Halderman, University of Michigan; Dr. Costis Toregas, Assistant Director, George Washington University Cyber Security Policy and Research Institute and an advisor to local, national and global organizations; and Matt Masterson, Deputy Elections Administrator, Office of the Ohio Secretary of State. CSPRI Seminar Series. Details below in *Announcements*.

-May 17, 7:30 a.m. - 11:30 a.m., **Fortifying Cybersecurity: Focus on Risk Mitigation** - This half-day conference, put on by Federal Computer Week, will examine how agencies are working to defend their digital infrastructures with more robust network monitoring, threat detection, vulnerability analysis, identity management, and targeted cyber-defense solutions that are aligned with specific risk mitigation strategies. The Willard InterContinental Hotel, 1401 Pennsylvania Avenue NW. More information.

Announcements

-Please join us at 12 noon on May 16 for a discussion about the security of electronic voting machines titled, "Is America Ready to Vote on the Internet? Concerns for National Security". There are at least two major forces tugging at the success of new, modern electronic systems that will take advantage of all society knows about technology. One is the desire for an easy system with convenient access for all, minimal administrative barriers and allowing voters to participate in new ways that expand participation and bring people who could not or would not participate in the traditional election cycles. The other is the growing awareness of the almost remarkable ease with which systems can be hacked from near or (important to some) abroad, and the technology "fix" for this insecurity is not yet defined to every one's satisfaction. In addition, other concerns about the massive transition costs for procuring new, secure systems and training the primarily

volunteer work force that administers elections may at times sideline or ignore strong opinions about the use of new technology. These conflicting forces will be unveiled and explored in the upcoming CSPRI seminar, cosponsored by the Verified Voting Foundation.

The program will be moderated by Prof. Lance Hoffman, Director, GW Cyber Security Policy and Research Institute. The expert panelists will include Prof. Alex Halderman, University of Michigan Dept. of Electrical Engineering and Computer Science (who, with his students, carried out what some have called "a totally epic hack of the DC Internet voting system pilot program"); Costis Toregas, Assistant Director, George Washington University Cyber Security Policy and Research Institute and an advisor to local, national and global organizations; and Matt Masterson, Deputy Elections Administrator, Office of the Ohio Secretary of State.

The discussion will be held in Room 302, Marvin Center at 800 21st St. NW. A hot buffet lunch will be provided, but registration is required. More information and the RSVP form are available at http://www.cspri.seas.gwu.edu/internetvoting.html.

Legislative Lowdown

-Senate lawmakers eager to pass some form of comprehensive cybersecurity legislation this year are quietly revamping their proposals to gain enough Republican votes to bring the measure to the floor, The Hill's Brendan Sasso writes. The House passed its own measure, the Cyber Intelligence Sharing and Protection Act (CISPA), last month despite a veto threat from the White House. The goal of CISPA is to help companies beef up their defenses against hackers who steal business secrets, rob customers' financial information and wreak havoc on computer systems. The bill would remove legal barriers that discourage companies from sharing information about cyber threats. But the White House and Senate Democrats argue that CISPA lacks adequate privacy protections and would fail to protect critical infrastructure, such as electrical grids, banks or water supplies. They have endorsed an alternative bill from Sens. Joe Lieberman (I-Conn.) and Susan Collins (R-Maine) that includes tougher privacy protections and would authorize the Homeland Security Department to set mandatory security standards for critical infrastructure, but some key Senate GOP members say it smacks of government overreach.

Meanwhile, Mozilla, a nonprofit foundation that makes the popular Firefox Web browser, has come out against CISPA, citing concerns over privacy, says The Hill. The announcement puts Mozilla on the opposite side of the issue from many Silicon Valley heavyweights, including Facebook, Microsoft, IBM, Oracle and Symantec. Trade associations TechAmerica and the Information Technology Industry Council also back the bill.

Cyber Security Policy News

-The Justice Department submitted 1,745 applications to the Foreign Intelligence Surveillance Court, a 10.5% increase over 2010, according to an analysis of the 2011 Foreign Intelligence Surveillance Act (FISA) Report, conducted by the Electronic Privacy Information Center (EPIC). Of the 1,745 FISA search applications, 1,676 concerned electronic surveillance. The

FISA court did not deny any applications, though it did modify 30 applications. Also in 2011, the FBI made 16,511 National Security Letter requests for information pertaining to 7,201 different U.S. persons. This is a substantial decrease from the 24,287 national security letter requests concerning 14,212 U.S. persons in 2010. The annual report on FISA, released by the Department of Justice, is far less extensive than the annual wiretap report, produced by the Administrative Office of the US Courts, EPIC found.

-Visa and MasterCard have sent alerts to card-issuing banks warning them that the data breach at card processor Global Payments dates back to at least June 2011, KrebsOnSecurity.com writes. The break-in was acknowledged several weeks ago. The initial warning from Visa and MasterCard said the window of the breach spanned January 21, 2012-February 25, 2012. In the half-dozen alerts since, the companies have gradually widened that window. Global Payments has not provided much information beyond its initial statement that 1.5 million payment cards may have been compromised. Global Payments CEO Paul Garcia said in a letter, responding to questions from a US Senator, that the breach was detected internally on March 8, 2012.

-The Google programmer at the center of the Google Street View privacy scandal is a highly regarded software engineer in the field of Wi-Fi networking and security, The New York Times divulged last week. Google Street View is a component of Google Maps that allows users to view certain streets as recorded by fleets of special Google cars that are equipped with video and still cameras. Yet privacy experts discovered that the project also was mapping local wireless networks along the way. The Times notes that while Google declined to identify the software engineer responsible for the wireless aspect of the project, the Federal Communications Commission revealed him as Marius Milner, who is perhaps best known for his "Netstumbler" software, a free program that was the world's first usable 'Wardriving' application for Windows.

-Senior military leaders are recommending that the Pentagon's two-year-old cyberwarfare unit be elevated to full combatant command status, sending a signal to adversaries that the U.S. military is serious about protecting its ability to operate in cyberspace, officials told The Washington Post. The elevation of Cyber Command to a level on a par with commands protecting entire regions and continents would give the nation's top cyberwarriors more direct access to General Martin E. Dempsey, chairman of the Joint Chiefs of Staff, and Defense Secretary Leon E. Panetta, allowing them more clout in the struggle for resources.

The Defense Department for the first time is using cyber teams like they use aircraft — to attack and to defend. Federal News Radio writes that Gen. Keith Alexander, commander of U.S. Cyber Command and director of the National Security Agency, said in a letter to Sen. John McCain (R-Ariz.) that DoD is employing cyber teams to execute offensive and defensive missions. Previously, the military focused on offensive capabilities or defensive capabilities, but not both for one team. He said DoD recently held the Cyber Flag exercise where about 300 servicemen and women worked in a virtual environment against a realistic adversary. The goal of the drill was for teams to take part in realistic training across a full spectrum of cyber operations. The Pentagon also wanted to integrate the services' cyber components and other government organizations while focusing on standard processes for future cyber missions. The letter to McCain came after Alexander testified in late March before the Senate Armed Services Committee about cyber threats and what DoD is doing about it.

-Iran has demonstrated a willingness to attack the United States and the intent to develop a cyber war capability, eclipsing Russia and China as a threat to the nation, a panel of policy and technical experts told House lawmakers last week, Government Computer News reports. Ilan Berman, vice president of the American Foreign Policy Council, called an Iranian plot to assassinate the Saudi ambassador to the United States, uncovered in October, credible and said it is an example of the country's willingness to carry out attacks on U.S. soil. He said it would be unreasonable to expect Iran could balk at a cyberattack against U.S. critical infrastructure. Frank Ciluffo, Director of GW's Homeland Security Policy Institute, was the first witness; his testimony is available at http://www.gwumc.edu/hspi/policy/testimony4.26.12_cilluffo.pdf.

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.