GW CSPRI Newsletter

July 23, 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

-July 24, 10:00 a.m., **Securing Federal Facilities: An examination of FPS Progress in Improving Oversight and Assessing Risk** - The House Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies will host a hearing. Cannon House Office Bldg., Room 311. More information.

-July 25, 9:30 a.m. - 11:00 a.m., **Transatlantic Perspectives on Digital Rights and Online Privacy** - The New America Foundation will host a forum and panel discussion. NAF, Suite 400, 1899 L St., NW. More information.

-July 25, 12 noon, **The Surveillance Iceberg: The FISA Amendments Act and Mass Spying without Accountability** - The CATO Institute will host a discussion featuring Sen. Ron Wyden (D-OR); Eric Lichtblau, Washington bureau reporter, New York Times; and Michelle Richardson, legislative counsel, American Civil Liberties Union. A luncheon will follow. This event will be webcast at cato.org/live. The Cato Institute, 1000 Massachusetts Avenue, NW. More information.

-July 25, 3:30 p.m., **Digital Warriors: Improving Military Capabilities for Cyber Operations** - The House Armed Services Committee's Subcommittee on Emerging Threats and Capabilities will hold a hearing. Witnesses will include Vice Admiral Michael S. Rogers, commander, U.S. Fleet Cyber Command and commander, U.S. Tenth Fleet, U.S. Department of the Navy; Lt. Gen. Rhett A. Hernandez, commander, U.S. Army Cyber Command, U.S. Department of the Army; Lt. Gen. Richard P. Mills, deputy commandant, Combat Development and Integration, commanding general, U.S. Department of the Marine Corps; Maj. Gen. Suzanne M. Vautrinot, commander 24th Air Force and commander, Air Force Network Operations, U.S. Department of the Air Force. Rayburn House Office Bldg., Room 2118. More information.

Announcements

-GW has been awarded $87,491 to develop the program for a significant meeting of the Principal Investigators of the National Science Foundation's new Secure and Trustworthy Cyberspace (SaTC) program. The program seeks effective collaborations among computer scientists, electrical engineers, economists, psychologists, sociologists, and others working on cybersecurity. The project will identify and recruit a stimulating program of speakers and activities for the meeting which will take place in late November. The meeting will broaden the perspectives of researchers from all of the fields involved, help them begin to form new partnerships and collaborations, and help them to better understand how their discoveries and advances may be transitioned into practice. It will also help put researchers with diverse backgrounds from diverse institutions on a common footing. GW's principal investigator is Prof. Lance Hoffman and the senior lead research scientist on the project is Dr. Carl Landwehr, both of CSPRI.

Legislative Lowdown

-Revisions that Sen. Joe Lieberman (I-Conn.) made to his Cybersecurity Act seem to have appeased privacy advocates who lobbied against an earlier version of the bill, The Hill's Brendan Sasso writes. The revised Lieberman bill narrows the definition of what can be shared and requires that any information shared with the government must go to civilian, not military, agencies. The privacy groups argue that the legislation should not empower the CIA and the National Security Agency (NSA) to collect Americans' personal computer information. The bill also dictates that the information can only be used for addressing cybersecurity threats and not other purposes, such as national security or criminal investigations.

But not everyone is happy with this latest compromise. The U.S. Chamber of Commerce said on Friday that it isn't sold yet on the revised version of the cybersecurity bill, arguing that it would take an "overly prescriptive" approach towards protecting the nation's critical infrastructure from cyberattacks.

Lawmakers have been scrambling to get the bill passed before Congress shuts down for the August recess. The Lieberman bill would establish a program where critical infrastructure operators would certify that they meet a set of performance standards in exchange for various incentives, such as liability protections. The idea was hatched by a bipartisan working group that was led by Sens. Sheldon Whitehouse (D-RI) and Jon Kyl (R-Ariz.). President Obama penned an op-ed on the need to pass the bill, an entreaty that was published last week in The Wall Street Journal.

The Hill's Sasso cites a Senate aide saying that Majority Leader Harry Reid (D-Nev.) will likely move to the bill this week once the upper chamber finishes up votes on taxes. That could come as early as Wednesday or Thursday, while a procedural vote to move the bill to the floor is expected the following Monday.

-At 12:30 on Wednesday, July 25, The House Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade is expected mark up HR 6131, a bill to extend the "Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers Beyond Borders Act of 2006" or "SAFE WEB Act".

Cyber Security Policy News

-Government efforts to ensure the cybersecurity of the nation’s increasingly networked electric grid are hampered by a cumbersome regulatory process and a lack of enforcement, government and industry witnesses told a Senate panel last week. Government Computer News reports on testimony from representatives at the Federal Energy Regulatory Commission and the North American Electric Reliability Corp. (NERC), who described a system under which federal regulators lack the ability to establish standards and requirements, and the industry group creating the standards lacks the ability to enforce them. All sides complained of a lack of useful information about cyber threats facing an electric grid that is becoming more integrated and tied into the Internet.

Meanwhile, Sens. Joseph Lieberman (I-CT), the chairman of the Senate Homeland Security Committee, and Susan Collins (R-ME), the panel's senior Republican, are calling for a federal investigation of the power grid's potential cybersecurity vulnerabilities after an article in the security trade press raised concerns. That story, from CNet, quoted Jesse Hurley, co-chair of the North American Energy Standards Board's Critical Infrastructure Committee, as complaining that the mechanism for creating digital signatures is insufficiently secure because not enough is being done to verify identities and some companies are attempting to weaken standards to fit their business models. "These certificates protect access to control systems," Hurley said. "They protect access to a $400 billion market. They protect access to trading systems. They also protect access to machines that do things like turn generators off. If you issue a fraudulent certificate or you're lax... the consequences could be disastrous." The U.S. electrical grid has already become a target of cyberattacks, with Chinese and Russian hackers reportedly penetrating it over the Internet.

Speaking of re-keying locks, the Pentagon is helping civilian agencies block access to federal classified networks by anyone who does not have a new smart card, military officials announced Thursday night, in the wake of recent information leaks, according to NextGov. During a closed-door House committee hearing earlier in the day, Defense Secretary Leon Panetta briefed lawmakers on the action -- part of a new top-down agenda to prevent the exposure of government secrets. Defense Department officials already had announced the ongoing distribution of the new tokens that military employees will need to enter the Secret Internet Protocol Router Network, which handles the military's classified data.

-The Department of Homeland Security is warning the public to be especially on guard for cyber scams that take advantage of public interest in the 2012 Summer Olympics in London to peddle flimsy offers of discounted tickets, free merchandise, exclusive videos, or breaking news. "Hackers frequently take advantage of large, highly-publicized events and popular news stories to get users to click on fraudulent links and unknowingly download malware or other viruses onto their computers, smart phones, tablets, and other wireless devices," DHS warned. "Hackers often use search engine optimization tricks to ensure that malicious sites appear on a search result page for certain keywords, and use clever tricks to convince Internet users to give out their credit card and personal information."

-National security officials say American companies need to report cyber attacks in order to help better protect the nation's networks, reports Federal News Radio. The Bipartisan Policy Center reports that more than 50,000 cyber attacks against public and private networks are reported to the Department of Homeland Security in a year — just a fraction of the total number of attacks. Many companies do not want to admit they've been the victim of cyber attacks because they fear the stigma and potentially a loss of business, according to the report.

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.