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

GW CSPRI Newsletter

September 26, 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

-Sept. 27, 7:30 a.m. - 12 noon, **Cloud with Confidence** - A free, half-day conference on cloud security. Speakers include experts from Cisco and Lockheed Martin. The Willard Hotel, 1401 Pennsylvania Ave. NW. More information.

-Sept. 27, 8:30 a.m. - 5:00 p.m., **2nd Annual Cybersecurity Summit** - Some of the industry's leading experts and government insiders discuss vital strategies, tactics, and tips for protecting both government and private-industry cyber infrastructure. 1777 F. St. NW. More information.

-Sept. 27, 2:00 p.m., **Securing the Government's Domain Name System with DNSSEC** - The White House issued a mandate for all federal agencies to implement Domain Name System Security – otherwise known as DNSSEC. This Webinar is about what it takes to implement DNSSEC and the value it brings to securing Internet infrastructure and enabling the business of government. More information.

-Sept. 28, 8:00 a.m. - 5:00 p.m., **FedCyber.com Government-Industry Summit** - This conference will focus on crafting action-oriented strategies that will help the federal and security community shape models for the next decade of national cyber defense. This event is free for government cyber practitioners. Newseum, 555 Pennsylvania Ave. NW. More information.

Announcements

-GW was recently awarded $125,719 for scholarships under the Information Assurance Scholarship Program administered by the National Security Agency. Two GW students are studying on these now. The new competition for these scholarships and for Scholarships for Service funded by the National Science Foundation and the Department of Homeland Security begins in late November and the deadline for applying for them is January 31, 2012, but potential applicants can start filling out their applications online now. Details about GW's cyber security scholarship programs are at www.seas.gwu.edu/cybercorps.

-GW was also recently awarded $170,843 in a grant from the National Science Foundation for a two year collaborative proposal with the University of Washington and the University of Hawaii, Manoa. Entitled "Teaching Strategic, Operational, and Defensive Cybersecurity to the Next Generation from Sea to Shining Sea", the project makes available through videos, notes, and ultimately instructor guides GW's required Seminar for CyberCorps students that highlights Federal and industry experts. It develops a Cyber Security Library of Content that is part of a comprehensive approach to the teaching of strategic, operational, and defensive cyber security. Students are trained in many current policies so that they can hit the ground running when they arrive at their internship or job in the government. This material will first be provided to two partner institutions and, ultimately, to the entire national CyberCorps community. The GW principal investigators for this project are Professors Lance Hoffman, Rachelle Heller, and Costis Toregas of Computer Science. The principal instructor involved is Lecturer Mischel Kwon of Computer Science.

-CSPRI has received a 9 month extension to the existing subagreement with Prince George's Community College to provide management support services to CyberWatch, a network of more than 75 two and four year institutions whose aim is to increase the quantity and quality of the cybersecurity workforce of the nation. The project co-PIs are Shelly Heller and Costis Toregas, and the tasks in this extension include support of a Collegiate Cyber Defense Competition and the exploration of a possible National Cyber League that would provide continuous opportunities for cyber learning using a weekly "football league" model. Another task is to provide general management services for the entire network, as well as liaison services to private industry interested in forging partnerships with academic institutions in cyber security.

Current Research

-Associated CSPRI researchers have produced numerous papers over the past year. Claire Monteleoni (with Kamalika Chaudhuri and Anand Sarwate) has written about differentially private empirical risk minimization. Hoeteck Wee has researched threshold and revocation cryptosystems via extractable hash proofs. Nan Zhang (with Xin Jin, Aditya Mone, and Gautam Das) has written about randomized generalization for aggregate suppression over hidden web databases. For links to these and other works, see the CSPRI website.

Legislative Lowdown

-Legislation aimed at protecting the nation's financial networks and power grids from computer hackers and safeguarding consumer data online won approval from a U.S. Senate panel in a party-line vote, Bloomberg reports. The Senate Judiciary Committee approved three bills on Thursday aimed at setting national standards for security breaches involving personal data. Committee Chairman Patrick Leahy (D-Vt.) offered S. 1151 (PDF), which would require business entities to develop a data privacy and security plan for protecting sensitive personally identifiable information, require agencies and business entities to notify U.S. residents in the event of a security breach involving such information, and impose criminal penalties for intentionally and willfully failing to provide notice of a security breach. The InsidePrivacy Blog has more detail on the Leahy bill, as well as two others approved by the committee last week.

But the party-line vote on the measures may complicate efforts to move them to the Senate floor, according to NextGov. The three measures are similar in that each would require companies to take reasonable steps to secure personal information about consumers and to notify consumers when their personal data has been stolen as a result of a security breach. The measures are being met with resistance by some lawmakers who feel the bills would impose too many costly compliance burdens on businesses. Senate Judiciary ranking member Chuck Grassley (R-Iowa) offered several amendments, including one that would set minimum sentences for hackers that was adopted by the panel. The committee rejected other Grassley amendments, including one that would limit the ability of state attorneys general to bring civil suits over a data breach and another that would require that any funds stolen and recovered as a result of a data breach go toward deficit reduction. Grassley told National Journal after the markup that supporters will have a difficult time moving the bills to the Senate floor unless more changes are made.

Cyber Security Policy News

-Internet service providers may be asked to create an industry standard for fighting computer viruses known as botnets under a proposal from U.S. regulators, Bloomberg reports. The Homeland Security and Commerce departments are seeking comments through Nov. 4 on the creation of a voluntary program that would "reduce the harm that botnets inflict on the nation's computing environment," according to a notice published last week in the Federal Register.

-A concerted cyberattack on Japan's top defense contractors prompted strong words from U.S. diplomats. An online assault on defense contractors including Mitsubishi Heavy Industries, which builds F-15 fighter jets and other American-designed weapons for Japan's Self-Defense Forces, began in August, but only came to light last week, prompting rebukes from Japanese officials over the timing of the disclosure, the New York Times writes. The breach came less than two weeks after a Japanese air traffic controller was questioned for posting secret American flight information on his blog. The data including detailed flight plans for Air Force One last November, as well as data on an American military reconnaissance drone, officials said.

-The United States is engaged in cyber "cyber cold war" thanks to the constant barrage of attacks from its enemies and must build up its capacity to respond in order to deter such attacks, according to an op-ed published Friday in The Hill by retired Air Force Lt. Gen. Harry Raduege. "The real danger is the prospect that an enemy could one day launch a strategic-level attack in cyberspace — one that causes large-scale death, destruction, damage, disruption or devastating economic loss for our country," Raduege wrote.

-Democratic Sens. Al Franken (Minn.) and Chris Coons (Del.) urged OnStar last week to reconsider changes to its privacy policy that would allow the navigation provider to continue tracking the location of vehicles even after users cancel their service. OnStar sent emails to its customers last week notifying them of the changes to the company's policies. The senators requested answers to a series of questions, including whether OnStar has suffered a breach of its customers' data and how it plans to use the location data.

-Big firms increasingly are borrowing a page from the playbook of the State Department, according to The Wall Street Journal. State, an agency responsible for protecting computer networks for 400 U.S. embassies and offices across 24 time zones, faces a cybersecurity challenge that in many ways mirrors that of a multinational company. Siobhan Gorman notes that State's cybersecurity program differs from commercially available network-monitoring programs in that it uses a market-based approach to create incentives to fix security gaps. It quantifies a range of security risks and "monetizes" them into a "common currency" that assigns the most points to the highest-priority security gaps to be fixed. "Since launching its system three years ago, State has received a growing number of inquiries from an array of companies, including Microsoft Corp., General Electric Co., J.P. Morgan Chase & Co., the computer security firm RSA and Heartland Payment Systems Inc., a credit-card payment processor and victim of a major cyber attack a few years ago," Gorman wrote.

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.