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

GW CSPRI Newsletter

May 2, 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

-May 3, 12:15 - 1:30 p.m., **Consumer Privacy -- Is there an App for That?** - The DC Bar Association and the Federal Communications Bar Association will host a brown bag lunch. Speakers will include Angela Giancarlo, chief of staff to FCC Commissioner Robert McDowell, and Patricia Poss, an attorney for the Federal Trade Commission's Bureau of Consumer Protection. Latham & Watkins, Suite 1000, 555 11th St. NW. More information.

-May 4, 9:30 a.m., **The Threat of Data Theft to American Consumers** - The House Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade will hold a hearing Room 2322, Rayburn Building. More information.

-May 4, 8:00 a.m. - 5:00 p.m., **Washington Caucus** - The Computer and Communications Industry Association will host an event that will feature talks from several tech-oriented lawmakers, including **Sen. Ron Wyden** (D-CA), **Rep. Bob Goodlatte** (R-VA), **Rep. Mike Honda** (D-CA), **Rep. Anna Eshoo** (D-CA), **Rep. Doris Matsui** (D-CA), **Rep. Zoe Lofgren** (D-CA), and **Rep. Maxine Waters** (D-CA). Other speakers will include **Larry Strickling**, head of the Commerce Department's National Telecommunications and Information Administration, and FTC Commissioner **Julie Brill**. The Newseum, 555 Pennsylvania Ave. NW. More information.

-May 4-5, **Industry Control Systems Security and Looking at Cyber for Nuclear Power Plants** - This event, the Maryland Cybersecurity Center's first workshop, focuses on the critical infrastructure and the commercial nuclear power industry. Academic leaders at the university together with individuals from the Nuclear Regulatory Commission, the commercial nuclear power industry, and other research institutions will explore new regulatory and industry-led initiatives to protect nuclear power plants from cyber-based threats. More information.

-May 5, 7:30 a.m. - 4:30 p.m., **Government IT Leadership Forum** - Chief information officers from civilian, defense, and intelligence agencies will discuss cybersecurity, open government, cloud computing, data center consolidation, and more. Newseum, Knight Conference Center 555 Pennsylvania Ave NW. More information.

Announcements

-Six more students were “launched” from GW’s CyberCorps program in a ceremony at GW’s Mount Vernon campus on April 28. This program, supported by the National Science Foundation and the Defense Department with participation also from the Department of Homeland Security has now placed 54 graduates in cyber security positions in 30 agencies throughout the federal government since 2003. Our multidisciplinary academic program in information assurance, our signature government guest lecturer Seminar, and our location at the center of the government cyber security workforce make this effort attractive for both students and the government. This year’s graduates are going to the Justice Department, the State Department, the Defense Information Systems Agency (DISA), and the Space and Naval Warfare Systems Command. Six other students who are returning in September are going to summer internships at the House of Representatives, the National Institutes of Standards and Technology, the Defense Media Activity, DISA, and MITRE (a Federally funded research and development center). And five more students will join the scholarship program in September.

Currently, this program only supports students who commit to working for the government upon graduation. However, at this event, two representatives from the private sector were present to consider similar programs for their firms. GW encourages private sector employers who want to “lock in” similar quality graduates in the future to contact CSPRI’s assistant director, Dr. Costis Toregas, to discuss what it takes to do this.

Compared with other recruiting and screening costs, you may be surprised at how cost-effective this is.

Legislative Lowdown

-Prompted by a disclosure from Sony of a breach that may have jeopardized the personal and financial data in as many as 77 million consumers, **Rep. Mary Bono Mack** (R-Calif.) said last week that she plans to introduce legislation to protect consumer data on the Internet. Bono Mack, the leader of the Energy and Commerce Trade subcommittee, has previously called for heightened scrutiny of how companies use online data, but had yet to announce the need for a bill, according to The Hill.

Cyber Security Policy News

-**Sen. Richard Blumenthal** (D-Conn.) called for the Justice Department to launch a full investigation into those responsible for the data breach that brought down Sony's PlayStation Network last week, The Hill reports. The senator also is urging the Justice Department to examine whether Sony's delay in notifying customers makes the firm liable for any resulting damage to consumers. For its part, Sony says it still is not sure how many of the 77 million user accounts may have been compromised, although it said customer credit card information was encrypted and that the company's servers did not store credit card security codes. The entertainment giant said over the weekend that it hopes to have its PlayStation network fortified against hackers and back online within a week.

-Employees who breach their employers' acceptable computer use policy could be opening themselves up to felony violations of federal computer fraud and abuse act statutes, according to a reading of an opinion rendered last month by the Ninth Circuit Court of Appeals. Writing for The Volokh Conspiracy, **George Washington University law professor Orin Kerr** argues that the decision was unconstitutional. "The checking of personal e-mail, viewing a weather report, or loading up a new site is the modern equivalent of getting up to stretch, or to talk briefly with a coworker," Kerr explained. "It is downtime, time spent recharging mental batteries. And yet because it uses a computer, it is also technically 'accessing' a protected computer. Each visit, each checking, and each viewing involves entering a command into a computer network and retrieving information from a server. Assuming that using a computer to retrieve information 'accesses' that computer, the interpretation that courts give to lack of authorization ends up determining whether these keystrokes amount to federal crimes."

-**Senate Commerce Committee Chairman Jay Rockefeller** (D-W.Va.) said he plans to hold hearings this month on consumer privacy on mobile phones. The announcement follows the discovery that popular smart phones from Apple and Google and store information about users' whereabouts. “Reports of mobile devices tracking the location of users is just the latest in a string of concerns raised in the mobile marketplace. This committee has investigated this in the past, and it is appropriate to review it again," Rockefeller said in a statement. "Consumers deserve to know exactly what information is being collected about them, how it is being used, and should be able to say no to undesired collection of information." The hearing notice is just the latest in a series of calls from other lawmakers for deeper congressional inquiries into mobile location tracking and privacy, writes the National Journal.

-A government review of the FBI agents who investigate national security-related computer intrusions found about a third of them lack the required technical skills to do their jobs, Bloomberg reports. Of 36 agents interviewed for the review, 13 were deficient in at least some of the necessary capabilities, the U.S. Justice Department inspector general's report (PDF) found. Five of the agents told the inspector general's office that they viewed themselves as unqualified to conduct investigations of computer hacking involving national security.

The Federal Bureau of Investigation warned this week that cyber thieves have stolen approximately $20 million over the past year from small to mid-sized U.S. businesses through a series of fraudulent wire transfers sent to Chinese economic and trade companies located near the country's border with Russia, KrebsOnSecurity.com writes. The FBI said that between March 2010 and April 2011, it identified twenty incidents in which small to mid-sized organizations had fraudulent wire transfers to China after their online banking credentials were stolen by malicious software.

-Iran said last week that its government computers were being attacked by yet another piece of malicious software that is targeting its domestic infrastructure. An official from Iran's civil defense office said the malware strain was called "Stars," although Iranian officials have offered no more information about the claim. Meanwhile, U.S.-based anti-virus firms say they have yet to see a copy of the virus. Iran is widely considered to have been the intended target of "Stuxnet," an unusually complex computer worm that experts say appears to have been designed to infect and sabotage systems responsible for managing large industrial plants, including nuclear power plants.

-Inflated public conception of the threat that the United States faces from cyber attacks and vulnerabilities may lead to unnecessary and unfounded regulation of the Internet, according to a new white paper authored by researchers at George Mason University's Mercatus Center. "The rhetoric of 'cyber doom' employed by proponents of increased federal intervention, however, lacks clear evidence of a serious threat that can be verified by the public," wrote GMU's **Jerry Brito** and **Tate Watkins**, in the first of a mulit-part series of policy papers on the subject. "As a result, the United States may be witnessing a bout of threat inflation similar to that seen in the run-up to the Iraq War. Additionally, a cyber-industrial complex is emerging, much like the military-industrial complex of the Cold War. This complex may serve to not only supply cybersecurity solutions to the federal government, but to drum up demand for them as well."

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.*