THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE

Thoughtful Analysis of Cyber Security Issues

GW CSPRI Newsletter

November 14, 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

-Nov. 14, 5:00 p.m., **Deadline for comments on voluntary ISP/Botnet mitigation guidelines** - The Department of Commerce and Department of Homeland Security have asked for comment regarding creating a "voluntary" code for Internet service providers to follow regarding the detection, notification, and mitigation of botnets. More information.

-Nov. 15, 10:00 a.m., **Cyber Security: Protecting America's New Frontier** - The House Judiciary Committee's Subcommittee on Crime, Terrorism and Homeland Security will hold a hearing. Witnesses will include Richard Downing, deputy chief, Computer Crime and Intellectual Property Section, Criminal Division, US Department of Justice; Michael Chertoff, co-founder and managing principal, The Cherthoff Group; James Barker, lecturer on law,

Harvard University; Orin S. Kerr, professor of law, George Washington University. Rayburn House Office Bldg., Room 2141. More information.

-On Nov. 16, 12 noon – 2 p.m., CSPRI will host a debate on cell phone and Internet blackouts by government agencies. Debating for the argument that such actions are unconstitutional and illegal absent a declared national emergency 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, 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 with two additional experts, GW Prof. Amitai Etzioni, and Dr. Eric Burger, Georgetown University adjunct faculty member. Please RSVP to lunch and/or the seminar at https://csprieventblackouts.eventbrite.com. GW Marvin Center, 800 21st St. NW, Room 302.

-Nov. 17, 7:30 a.m. - 11:45 a.m., **ID Proofing and the Future of Government eAuthentication** - The discussion at this half-day conference will center on the federal government's National Strategy for Trusted Identities in Cyberspace (NSTIC), an identity management and authentication scheme codified this year into a new program office within the Department of Commerce. The Willard Hotel, 1401 Pennsylvania Avenue, NW. More information.

-Nov. 17, 2011, 8:00 a.m. - 5:00 p.m., **2011 ONC Annual Meeting** - The 2011 Office of the National Coordinator for Health Information Technology (ONC) Annual Meeting will bring together the awardees of all of its programs created through the Health Information Technology for Economic and Clinical Health Act. Talks will center on best practices and opportunities to drive a higher quality, safer, more efficient health care system enabled by health information technology. Renaissance Washington DC Hotel, 999 Ninth Street, NW. More information.

Legislative Lowdown

-The House Judiciary Committee is slated to hold a hearing on Tuesday on the “Stop Online Piracy Act,” an anti-piracy measure that critics and many experts say could endanger efforts to build a more secure Internet. The bill would grant the government greater power to shutter Web sites that host copyright-infringing content, by requiring Internet service providers to filter DNS requests for domains identified as hosting infringing content. Earlier this year, a coalition of academics and security industry experts, said it would be minimally effective and would represent technical challenges to important security initiatives, such as DNSsec. More information is above in Upcoming Events.

-Sens. John Kerry (D-Mass.) and John McCain (R-Ariz.) pressed the Department of Commerce and the Federal Trade Commission on Tuesday to release their final reports on consumer privacy protections, The Hill reports. Both agencies released draft reports last December that identified gaps in current privacy protections, but neither has issued its final report. Kerry and McCain introduced the Commercial Privacy Bill of Rights in April, which would spell out exactly how firms could use consumers’ personal information.

Announcements

The Team for Research in Ubiquitous Secure Technology (TRUST) is seeking 20 promising undergraduate students from diverse backgrounds and cultures, to participate in the Summer Undergraduate Research Experience—an eight–week program sponsored by the National Science Foundation, which provides an excellent opportunity for students to conduct research directly with our faculty located at four TRUST partner campuses: UC Berkeley, Cornell University, Stanford University, Vanderbilt University. With the guidance of graduate student and faculty mentors, students will be performing research and supporting activities in the area of information technology and TRUST related topics. The application deadline is FEBRUARY 17, 2012. Please see the **attached flyer** and the website for additional information.

Cyber Security Policy News

-As the U.S. Supreme Court readied to hear a case about the constitutionality of federal law enforcement using GPS location tracking devices to monitor suspects without a warrant, Wired.com ran a story about a young man in California who revealed that he found not one but two different devices on his vehicle recently. According to Wired, the 25-year-old resident of San Jose, California, says he found the first one about three weeks ago on his Volvo SUV while visiting his mother in Modesto, about 80 miles northeast of San Jose. After contacting Wired and allowing a photographer to snap pictures of the device, it was swapped out and replaced with a second tracking device. A witness also reported seeing a strange man looking beneath the vehicle of the young man's girlfriend while her car was parked at work, suggesting that a tracking device may have been retrieved from her car.

-Researchers have demonstrated a vulnerability in the computer systems used to control facilities at federal prisons that could allow an outsider to remotely take them over, doing everything from opening and overloading cell door mechanisms to shutting down internal communications systems, Ars Technical reports. The research, presented on October 26 at the Hacker Halted information security conference in Miami, centered around attacks that can take control of prisons' industrial control systems and programmable logic controllers. The researchers said they spent less than $2,500 and had no previous experience in dealing with those technologies.

-The Defense Advanced Research Projects Agency, the Pentagon's far-out research arm, and its brand new military command for cyberspace made a public plea last week for outside researchers to help the military secure its networks. DARPA last week convened a cyber colloquium at a northern Virginia hotel on Monday for what it called a "frank discussion" about the persistent vulnerabilities within the Defense Department's data networks. According to reporters from Wired.com who were at the event, the agency said the Pentagon can't defend those networks on its own. "Because it's the blue-sky research agency that helped create the internet, DARPA framed the problem as a deep, existential one, not a pedestrian question of insecure code," the publication reports. "It is the makings of novels and poetry from Dickens to Gibran that the best and the worst occupy the same time, that wisdom and foolishness appear in the same age, light and darkness in the same season," mused Regina Dugan, DARPA's director. She's talking about

the internet. “These are the timeless words of our existence. We know it is true of everything.” The full story is here.

Indeed, America’s critical computer networks are so vulnerable to attack that it should deter U.S. leaders from going to war with other nations, a former top U.S. cybersecurity official said Monday. Richard Clarke, a top adviser to three presidents, joined a number of U.S. military and civilian experts in offering a dire assessment of America’s cybersecurity at a conference, saying the country simply can’t protect its critical networks, the Associated Press reported last week. Clarke said if he was advising the president he would warn against attacking other countries because so many of them - including China, North Korea, Iran and Russia - could retaliate by launching devastating cyberattacks that could destroy power grids, banking networks, or transportation systems.

-NATO is working to get all its agencies and commands under a single cyber roof by the end of 2012, but lacks a strategy to respond to an all-out assault on civilian critical infrastructure throughout the European Union, Defense News reports. Cecilia Malmstrom, the EU's commissioner for Home Affairs, said the EU has developed relations with NATO in the area of civilian critical infrastructure protection. But when asked whether there was an EU-NATO plan in place to respond to an Estonia-type cyberattack by another state or terrorist organization, she said “there was no strategy.”

-Facebook, Inc. is close to a settlement with the U.S. government over charges that it misled users about its use of their personal information—the latest sign of widening public concern over privacy in the digital age, according to a report in The Wall Street Journal. The paper reports that the settlement would require Facebook to obtain users’ consent before making “material retroactive changes” to its privacy policies. That means that Facebook must get consent to share data in a way that is different from how the user originally agreed the data could be used.

-Online advertiser ScanScout has entered into a consent agreement with the Federal Trade Commission in connection with claims it made that consumers could opt out of receiving targeted ads by changing their computer’s web browser settings to block cookies, Libbie Canter writes for InsidePrivacy.com. According to the FTC, these claims were deceptive with respect to the use of so-called “Flash cookies” since browser settings did not allow users to remove or block the Flash cookies used by the company. Flash cookies generally cannot be controlled through browser privacy settings, in contrast to traditional “HTTP” cookies. Under the terms of the proposed settlement, ScanScout must post a prominent notice on its home page stating the following: “We collect information about your activities on certain websites to send you targeted ads. To opt out of our targeted advertisements, click here.” The company must provide a hyperlink to an opt-out mechanism that offers users the ability – through a single click – to change a browser setting.

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.