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

# GW CSPRI Newsletter

August 23, 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

-Aug. 23, 11:00 a.m. - 2:00 p.m., **The National Institute of Standards and Technology's Smart Grid Advisory Committee** – Meeting by teleconference. More information.

-Aug. 23, 1:00 p.m. - 2:00 p.m., **Author Roundtable: Deep Dive on Cybercrime and Espionage** - Several authors and security experts discuss advanced online attacks, their success from the perspective of exploitation, and their presence within all industries. This online Webinar is free. More information.

-Aug. 24, 2:00 p.m. - 3:00 p.m., **Database Security and Protecting Against the Insider Threat** - A Webinar presented by McAfee on the principles of database security, activity monitoring, and both pro and reactive intrusion detection. More information.

-Aug. 30, 2:00 p.m., **Cyber Security: Pinpointing the DoD's Challenges** - A free Webinar to explore the Government Accountability Office’s recommendations for the development of a unified, inter-agency strategy. Topics to be covered will include: How GAO conducted its recent audits and determined the effectiveness of current cyber strategies; GAO’s recommendations to defense leaders on how to improve U.S. cyber capabilities; and where U.S. cyber strategy might be headed as government defines its cyber operations and bolsters its defenses. Speakers include Davi D'Agostino, director of defense capabilities and management, GAO; and Nelsie Alcoser, senior defense analyst, GAO. More information.

# Legislative Lowdown

-The House and Senate are in recess until Sept. 6 and 7, respectively.

# Cyber Security Policy News

-Major websites such as MSN.com and Hulu.com have been tracking people's online activities using powerful new methods that are almost impossible for computer users to detect, The Wall Street Journal reported last week. The new techniques, which are legal, reach beyond the traditional "cookie," a small file that websites routinely install on users' computers to help track their activities online. Hulu and MSN were installing files known as "supercookies," which are capable of re-creating users' profiles after people deleted regular cookies, according to researchers at Stanford University and University of California at Berkeley.

Following the story, Microsoft said it would disable supercookies on MSN.com. The revelations also stirred interest on Capitol Hill, where **Rep. Joe Barton** (R-Texas) said the use of supercookies should be illegal.

Rep. Barton also warned last week of privacy issues with Groupon, a popular online service that helps users find deals on merchandise and services. Barton and Edward Markey (D-Mass.), who co-chair the House Bipartisan Privacy Caucus, wrote a letter to Groupon in July that asked several questions about how the company collects and uses consumer information, and how much control consumers have in this process. Last week, the two lawmakers released the responses (PDF) they received from Groupon.

-The Web site for 2012 presidential candidate **Ron Paul** came under a sustained online attack on Saturday, the day the campaign had set aside for a major campaign donation fundraising effort. In a statement on the campaign's blog, the campaign said it was extending the fundraising effort—dubbed the "money bomb"—by an extra day due to the disruptive attack.

-A U.K. man has been sentenced to 15 months in prison for using information from his Facebook friends to steal money from their bank accounts, The Telegraph reports. Thirty-three-year-old Iain Wood stole £35,000 ($57,000) over two years from his neighbors by figuring out the answers to security questions on their bank accounts. The man befriended people living in his apartment block so that he could use their personal details posted on Facebook to get past online bank security checks. “He said he had figured out how to access online bank accounts,” prosecutor Neil Pallister. “He would go on and say he couldn’t remember the password and would be asked security questions about date of births and mother’s maiden names and he was able to give correct details in some cases.”

-A Department of Defense program that shares cyber-threat information with defense contractors and their network providers has already stopped "hundreds of intrusions" in its 90-day pilot phase, according to InformationWeek. The DoD soon plans to expand its Defense Industrial Base experimental program—which currently has 20 participants—to the remainder of the industry base, as well as "key areas of critical infrastructure," deputy secretary of defense William J. Lynn told attendees Tuesday at the Defense Information Systems Agency (DISA) Customer and Industry Forum in Baltimore.

-A group of technology companies blasted the Obama administration's cybersecurity plan, saying it won't protect networks and is too focused on punishing companies that suffer attacks. Under the White House plan, the Department of Homeland Security would be in charge of developing cybersecurity standards in consultation with private sector firms deemed critical infrastructure. Those firms would then be forced to comply with the new security regulations or face having the results of their security audits and news of attacks publicized by the government. According to The Hill, Larry Clinton, president and CEO of the Internet Security Alliance, said rather than encouraging firms to improve their security, the White House's "name and shame" approach would only encourage firms to ignore sophisticated intrusions buried deep in their systems. He said firms are aware of the steps needed to prevent the vast majority of basic attacks, but in many cases the cost is prohibitive.

*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.*