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

GW CSPRI Newsletter

August 29, 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. 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.

-Aug. 30, 3:00 p.m., Extended deadline to submit comments to the National Institute of Standards and Technology (NIST) regarding the governance structure for its National Strategy for Trusted Identities in Cyberspace (NSTIC). See, notice in the Federal Register, Vol. 76, No. 158, Tuesday, August 16, 2011, at Page 50719.

-Aug. 31, 7:30 a.m. - 11:15 a.m., **Cybersecurity Risks for Non-Technical Executives** - This half-day forum will address a variety of timely questions facing organizations as they plan for cybersecurity risks, including the impact of cybersecurity legislation, and how to cope with and be prepared for a data breach. Keynote speaker will be Phil Dunkelberger, former president and CEO of PGP Corp. Other speakers include Rodney Joffe, senior vice president and senior technologist, Neustar; Scott Algiers, executive director, IT-ISAC; and Hugo Teufel, former chief privacy officer for the U.S. Department of Homeland Security. The Boeing Company, 1200 Wilson Blvd, Arlington, Va. More information.

-Sept. 1, 10:00 a.m. - 2:30 p.m., **Legal Policy Shifts Since 9/11** - The American Constitution Society for Law and Policy will host an event. From 10:00 - 11:30 a.m. there will be a panel titled "Surveillance". The speakers will be Kenneth Wainstein, former head of the DOJ's National Security Division; Jeffrey Rosen, George Washington University law school; Michael German ACLU; Gregory Nojeim (Center for Democracy and Technology), and Suzanne Spaulding (Bingham Consulting Group). William Lietzau, deputy assistant secretary of defense for rule of law and detainee policy, will be the lunch speaker. National Press Club, 13th floor, 529 14th St., NW. More information..

-Sept. 1 12:00 noon - 1:00 p.m., Shannon Rossmiller, an independent online terrorism investigator, will give a speech. Heritage Foundation, 214 Massachusetts Ave., NE. More information.

Legislative Lowdown

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

Cyber Security Policy News

-A Chinese government propaganda video about hacking may have inadvertently confirmed what security experts have long asserted but which Chinese officials deny at every turn: that China is systematically attacking U.S. targets electronically. The Epoch Times -- a publication that has been critical of Chinese censorship -- first called attention to the oversight, which appears to include video footage of a computer screen showing a Chinese military university engaged in cyberwarfare against entities in the United States. Finnish security firm F-Secure has published a breakdown of what exactly is in the video and why it matters. The Chinese government removed the video shortly after dozens of news media outlets picked up the story.

-An international cybercrime gang stole $13 million from a Florida-based financial institution earlier this year, by executing a highly-coordinated heist in which thieves used ATMs around the globe to cash out stolen prepaid debit cards, KrebsOnSecurity.com writes. Crooks broke into Jacksonville, Fla. based Fidelity National Information Services, and gained access to funds and to nearly two dozen prepaid debit cards. The thieves eliminated the daily withdrawal limits on the cards, and cloned them, distributing them to co-conspirators across Europe. Over a 24 hour period beginning late Saturday, Mar. 5, the attackers withdrew roughly $13 million via dozens of ATMs, adding more stolen funds to the compromised cards whenever their balances reached near zero.

-Google has agreed to a $500 million settlement with the government for allowing online Canadian pharmacies to illegally place advertisements on its AdWords service, the Justice Department said last week. The Hill writes that the fine is one of the largest forfeitures ever and represents the revenue Google received from the pharmacy ads plus the revenue the pharmacies made from selling drugs in the United States.

- The DNI's Intelligence Advanced Research Projects Activity office is asking for research proposals on sophisticated software and other tools that can, among other things, sort through "noisy data" to discern patterns that precede specific events. More information on the IARPA solicitation is available here.

-Street demonstrations and looting have long been common features of protests. But over the past year, and especially in recent months, protests have played out in increasingly brazen cyberattacks online. Now many analysts say as social unrest continues around the world, cyberattacks in the name of political or commercial causes will only increase, NextGov reports.

-Agencies that have been hewing to the federal government's guidelines on making it easier for employees to telework experienced fewer problems in the wake of last week's 5.8 East Coast earthquake, writes Federal News Radio's Emily Kopp. The U.S. Patent and Trademark Office was among the few agencies that was not plagued by clogged parking lots, long commutes and uncertainty about whether employees should come to work the day after the quake. The USPTO has apparently had a telework policy for 14 years, while other agencies are just beginning to let employees work from home.

-The Public Utilities Commission of the State of California adopted an order that contains rules to protect the privacy and security of customer data generated by so-called "smart meters" concerning the usage of electricity that are deployed by Pacific Gas and Electric Company (PG&E), Southern California Edison Company, and San Diego Gas & Electric Company. The rules regulate access to power data by third parties, data breach notification, data security practices, data minimization, and customer access to data.

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.