GW CSPRI Newsletter

October 29, 2012

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.

Events

-Oct. 29, 6:00 p.m. - 9:00 p.m., **Defending Against Cyber-Intrusions from Both State-Sponsored and Civilian Hackers** - The DC Bar Association will host a reception and panel discussion. The speakers will include Michael Hayden, former head of the NSA and CIA, and Eliana Davidson, deputy general counsel for intelligence, Dept. of Defense. DC Bar Conference Center, 1101 K St., NW. More information.

-Oct. 30, 10:00 a.m. - 1:00 p.m., The Privacy and Civil Liberties Oversight Board will hold a partially closed meeting. GSA National Capital Region Building, Conference Room 6067B, 301 7th St., SW. More information.

-Oct. 30, 12 noon - 1:00 p.m., **Cyber Security & Transformational Technologies: Keeping Systems and Data Safe** - This webcast will explore the results of the research, including how government is managing cyber security priorities and where they are investing limited funds to keep their systems and data safe while serving the needs of their agencies. More information. Speakers include Scott Andersen, director of secure cloud computing strategies Lockheed Martin Information Systems & Global Solutions, and Cynthia Poole, director of research services, Market Connections. More information.

-Oct. 30-Nov. 1, **NICE Workshop Shaping the Future of Cybersecurity Workshop Connecting the Dots in Cyberspace** - The NICE Initiative is focused on enhancing the overall cybersecurity posture of the United States by accelerating the availability

of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population. The 2012 Workshop will focus on Connecting the Dots between Government, Academia, Industry and the Public in the cybersecurity education arena. NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD. More information.

-Oct. 31, 7:30 a.m. - 9:30 a.m., **Leveraging Public-Private Partnerships to Protect Critical Infrastructure** - This two-hour event will cover a number of topics, including how cyber information sharing between the public and private sector can work under existing authorities, and how a collaborative approach to cyber standards - heavily involving industry - can be effective. Speakers include Lisa Kaiser, program manager, Control Systems Cybersecurity Standards and Tools, Department of Homeland Security; and Mark Engels, enterprise technology security and compliance director, Dominion. National Press Club, 529 14th Street NW. More information.

-Nov. 7, 7:15 a.m. - 6:30 p.m., **No Boundaries: Global, Connected, Secure** - This all day conference by Symantec will cover cyber security intelligence, tactical security, compliance and consolidation, as well as continuous monitoring, virtualization, and cloud data security. Walter E. Washington Convention Center, 801 Mount Vernon Place, NW. More information.

-Nov. 15, 7:30 a.m. - 4:30 p.m., **FedCyber.com Cyber Security Summit** - Talks at this year's conference will focus on three key areas: threat intelligence, adversary characterization, and information sharing; cyber workforce challenges; and emerging technologies that will change the cyber security landscape. Ronald Reagan Building, 1300 Pennsylvania Ave. NW. More information.

Legislative Lowdown

-Cybersecurity legislation faces long odds of passing Congress this year despite forceful calls for action from the White House and Defense Secretary Leon Panetta. The Hill reports that after Panetta warned in a speech last month that the cyber threat facing the United States represents a "pre-9/11 moment," Senate Majority Leader Harry Reid (D-Nev.) said he planned to bring cybersecurity legislation to the floor in November and take another shot at clearing a bill through the upper chamber. But there are several roadblocks that could prevent a bill from even reaching the Senate floor, and observers say Congress will likely punt the issue to next year. One of the chief complicating factors is the packed docket of legislation the Senate needs to complete before adjourning at the end of the year.

Not to worry, though, says Homeland Security Secretary Janet Napolitano. The DHS chief said last week that the executive branch stands ready to issue an executive order on cybersecurity if Congress fails to pass legislation that boosts the defenses of critical infrastructure against a cyberattack. The Hill's Jennifer Martinez wrote that Napolitano observed that Senate Majority Leader Harry Reid (D-Nev.) plans to revive efforts to pass cybersecurity legislation in November and said the administration will be keeping a close eye on whether Congress can make any progress.

Cyber Security Policy News

-The U.S. Department of Homeland Security is warning that a witches brew of recent events make it increasingly likely that politically or ideologically motivated hackers may launch digital attacks against industrial control systems. The alert was issued the same day that security researchers published information about an undocumented software backdoor in industrial control systems sold by hundreds different manufacturers and widely used in power plants, military environments and nautical ships, writes KrebsOnSecurity.com. Potentially aiding would-be attackers are specialized search engines like Shodan and the Every Routable IP Project, which were designed specifically to locate online devices that may be overlooked or ignored by regular search engines. “Multiple threat elements are combining to significantly increase the ICSs threat landscape,” DHS warned. “Hacktivist groups are evolving and have demonstrated improved malicious skills. They are acquiring and using specialized search engines to identify Internet facing control systems, taking advantage of the growing arsenal of exploitation tools developed specifically for control systems. In addition, individuals from these groups have posted online requests for others to visit or access the identified device addresses.

-A cyberattack on South Carolina Department of Revenue's information systems this summer exposed some 3.6 million Social Security numbers and 387,000 credit and debit card numbers, including 16,000 unencrypted ones, the state reported Oct. 26. GovInfoSecurity quotes Revenue Director James Etter as saying the state Division of Information Technology informed him of the cyberattack on Oct. 10. "We worked with them throughout that day to determine what may have happened and what steps to take to address the situation," Etter said in a statement. "We also immediately began consultations with state and federal law enforcement agencies and briefed the governor's office."

-The New York Times published a story last week examining a Saudi oil firm that U.S. officials believe was the work of Iran. The virus erased data on three-quarters of Aramco’s corporate PCs — documents, spreadsheets, e-mails, files — replacing all of it with an image of a burning American flag. United States intelligence officials say the attack’s real perpetrator was Iran, although they offered no specific evidence to support

that claim. But the secretary of defense, Leon E. Panetta, in a recent speech warning of the dangers of computer attacks, cited the Aramco sabotage as "a significant escalation of the cyber threat." In the Aramco case, hackers who called themselves the "Cutting Sword of Justice" and claimed to be activists upset about Saudi policies in the Middle East took responsibility.

-At least 20,000 users have fallen victim to a spam campaign that uses shortened links to legitimate government sites to carry out a hoax, SC Magazine reports. In the scams, users receive emails containing "1.usa.gov" short links and are redirected twice upon clicking -- first, immediately past a legitimate government site, then, to websites that look like CNBC news articles touting "$4,000 a month" home-based business opportunities. Once at the fake CNBC site, victims are lured into clicking on links on the page that direct them to a home-based business site also owned by attackers.

-A consumer group looking to overturn a $22.5 million Federal Trade Commission fine against Google to settle allegations of violating the terms of a 2011 consent decree is now arguing that Google continues to benefit from data it collected during the violation, according to the National Journal. An FTC complaint in August alleged that Google improperly bypassed privacy protections on Apple's Safari browser and placed tracking cookies on users' computers. Google agreed to settle the case, but didn't admit wrongdoing. FTC Commissioner Thomas Rosch dissented from the settlement, arguing that Google should admit wrongdoing and that the fine was small relative to Google's revenues.

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*