GW CSPRI Newsletter

September 10, 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.

Contents

Events

-Sept. 11, 8:00 a.m. - 1:30 p.m., **Trends in Technology Conference -** The Women in Government Relations will host an event. There will be panels titled "The Buzz with Tech Reporters", "Will Congress Pass Cyber Security Legislation?", and "Outlook for the Lame Duck and Prospect in the 113th Congress". Hyatt Regency Washington on Capitol Hill, 400 New Jersey Ave., NW. More information.

-Sept. 11, 1:00 p.m. - 2:00 p.m., **The Limits of the FTC's Data Security Program: Where is the line, and Where Should it Be?** - The American Bar Association will host a webcast panel discussion titled. The speakers will include Thomas Zych, of Thompson Hine LLP; Janis Kestenbaum, Federal Trade Commission; Michael Scott, Southwestern Law School; and David Zetoony, partner at Bryan Cave. More information (PDF).

-Sept. 11-12, **Cyber Resilience for National Security** - This event will focus on the latest prioritization efforts within the DoD's cyber security efforts, while bringing together government and industry leaders to discuss the most challenging threats to national cyber security in both the public and private sector. Sheraton Pentagon City Hotel, 900 South Orme Street, Arlington, VA. More information.

-Sept. 12, 10:00 a.m., **The EMP Threat: Examining the Consequences** - The House Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection, and Security Techologies will hold a hearing. Room 211, Cannon Bldg. More information.

-Sept. 13, 10:00 a.m. - 1:00 p.m., **National Security Threats Posed by Chinese Telecom Companies Working in the U.S.** - The House Intelligence Committee will hold a hearing. HVC-210, Capitol Visitor Center. More information.

Legislative Lowdown

-President Barack Obama’s administration is drafting an executive order that would create a program protecting vital computer networks from cyber attacks. According to Reuters, the program -- to be managed by the Department of Homeland Security -- would establish cybersecurity standards that companies could voluntarily adopt to better protect banks, telecommunication networks and the U.S. power grid from electronic attacks. The draft, which remains under review and could change, seeks to implement a key provision in a cybersecurity bill that failed to advance in the Senate last month. The administration is contemplating using an executive order because it isn’t clear Congress would pass a cybersecurity bill.

According to The Hill, the draft executive order would establish a voluntary program where companies operating critical infrastructure would elect to meet cybersecurity best practices and standards crafted, in part, by the government, according to two people familiar with the document. The concept builds off of a section in the cybersecurity bill from Sen. Joe Lieberman (I-Conn.) that was blocked last month by Senate Republicans, who called it a backdoor to new regulations. The draft has undergone multiple revisions and is brief, spanning no more than five pages. It is still being worked on and is subject to change, the people familiar with the draft stressed. It's also unclear whether the final product will get the president's approval to move forward. A new draft of the executive order is expected to be shared with agencies next week.

The proposed order comes amid increasingly strident and vocal calls for greater federal oversight of cybersecurity for the energy industry. In an interview with The Hill last week, Federal Energy Regulatory Commission Chairman Jon Wellinghoff told said he needs congressional approval to manage cybersecurity on the electric grid. As it is now, Wellinghoff said he can't communicate cyber threats to the utilities, and he has no enforcement authority to take action against a threat.

Cyber Security Policy News

-Secretary of State Hillary Clinton and Chinese Foreign Minister Yang Jiechi expressed interest last week in working together on issues like cybersecurity and theft of intellectual property, problems that have complicated the relationship between the two plugged-in countries, Nextgov reported. "Both the United States and China are victims of cyberattacks," Clinton said during a visit to Beijing. "Intellectual property, commercial data, national-security information is being targeted." A copy of their remarks is available at state.gov.

Meanwhile, Chinese telecoms equipment maker Huawei Technologies Ltd. has issued a report on cybersecurity that includes a pledge never to cooperate with spying in a fresh effort to allay concerns in the United States and elsewhere that threaten to hamper its expansion, the Associated Press reported last week. The report, written by a Huawei executive who is a former British official, calls for global efforts to create legal and technical security standards. It makes no recommendations for what standards to adopt but says current laws are inconsistent or fail to address important threats. Huawei, founded by a former Chinese military engineer in 1987, has grown to become the world's second-largest supplier of telecoms network gear after Sweden's LM Ericsson. Suspicions that Huawei might be controlled by China's Communist Party or military have slowed its expansion in the United States and it was barred from bidding to take part in an Australian broadband project.

-The Defense Information Systems Agency on Sept. 4 released its new strategic plan, a five-year strategy that promises to help the military shift toward Asia and increase its cyber operations. The document takes into account the Defense Department's shifting priorities and outlines the agency's goals and objectives through 2018. DISA said it will try out IT enterprise solutions before pushing the Pentagon to adopt them, Federal Computer Week writes. It will also encourage the military to move towards cloud computing and mobile devices. The agency pledges to consolidate data centers too. The just-released guidance is part of a new planning methodology for DISA, consisting of the development of the strategic plan, the campaign plan and a campaign implementation plan. In the past, the agency has released campaign plans.

-The Federal Trade Commission on Wednesday nudged application developers to take steps to protect consumer privacy. But many consumers seem to be already taking steps to guard their personal information from data-grabbing apps, The New York Times writes. A study by the Pew Research Center, released Wednesday, found that among Americans adults who use smartphone apps, half had decided not to install applications on their mobile phones because they demanded too much personal information. Nearly a third uninstalled an application after learning that it was collecting personal information "they didn't wish to share." And one in five turned off location tracking "because they were concerned that other individuals or companies could access that information." A customer's whereabouts can be extremely valuable to marketers trying to sell their wares, or government authorities trying to keep tabs on citizens' movements.

-Setting off a debate about digital arms dealing, a pair of security researchers say they've discovered new evidence that spyware sold by a British firm is being used by some of the most repressive regimes in the world. Google security engineer Morgan Marquis-Boire and Berkeley student Bill Marczak were investigating spyware found in email attachments to several Bahraini activists, The Register reports. In their analysis they identified the spyware infecting not only PCs but a broad range of smartphones, including iOS, Android, RIM, Symbian, and Windows Phone 7 handsets. The spying software has the capability to monitor and report back on calls and GPS positions from mobile phones, as well as recording Skype sessions on a PC, logging keystrokes, and controlling any cameras and microphones that are installed. They report the code appears to be FinSpy, a commercial spyware sold to countries for police criminal investigations. FinSpy was developed by the German conglomerate Gamma Group and sold via the UK subsidiary Gamma International. In a statement to Bloomberg, managing director Martin Muench denied the company had any involvement.

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.