# GW CSPRI Newsletter

October 1, 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 1-3, **Military Cyber Security Conference** - This conference brings together the senior level military, government and industry experts who are defining the requirements and shaping the solutions in cyber security and computer network defense. The conference will examine the role and status of new defense organizations, the latest threats, and emerging tools/techniques for continuous risk monitoring and management. Sheraton Pentagon City, 900 South Orme Street, Arlington, VA. More information.

-Oct. 3, 10:00 a.m. - 11:30 p.m., **What Every Mobile Device Owner Should Know** - The George Washington University acknowledges National Cyber Security Awareness Month with this seminar focused on mobile security. Please bring a functional smartphone and a pen or pencil in order to derive maximum benefit from the hands-on segment. Marvin Center Grand Ballroom, 3rd Floor, H St. NW.

-Oct. 3-5, **8th Annual IT Security Automation Conference** - This conference includes talks on implementing continuous monitoring; using security automation tools and technologies to ease the technical burdens of policy compliance; and innovative uses of automation across the enterprise in both federal government and industry applications. Baltimore Convention Center, Baltimore Inner Harbor, MD. More information.

-Oct. 4, 7:30 a.m. - 11:45 a.m., **Cybersecurity 2013** - Federal Computer Week hosts a seminar on how to extend the principles of FISMA to devices and processes beyond traditional network

perimeters, and methods to mitigate and manage malware. Speakers include Parmy Olson, London bureau chief, Forbes; and Ron Ross, computer scientist and NIST fellow, computer security division, National Institute of Standards and Technology. The Willard InterContinental Hotel, 1401 Pennsylvania Avenue NW. More information.

-Oct. 4, 6:30 p.m. - 9:00 p.m., **OWASP NoVA Meetup** - The monthly meeting of the OWASP Northern Virginia local chapter features vendor-agnostic presentations on a range of security topics. This month includes a talk called Benchmarking Web Application Scanners for Your Organization. Living Social, 11600 Sunrise Valley Drive, VA. More information.

-Oct. 10, 10:00 a.m. - 11:00 a.m., **Creating Strong Passwords That You Don't Have to Memorize** - The George Washington University will observe National Cyber Security Awareness Month with a primer on password security. Attendees are asked to please bring a laptop connected to GWIX and a pen or pencil in order to derive maximum benefit from the hands-on segment. Marvin Center 413/414.

-Oct. 15-16, **2nd Annual Cyber Security Finance Forum** - CSFF features combination of expert panels, individual company presentations and networking breaks that focus on the opportunities, challenges and issues that need to be understood to succeed in the cyber security sector. 1777 F St. NW. More information.

-Oct. 16, **Nuclear Regulatory Commission Cyber Security Conference** - The Nuclear Regulatory Commission is hosting a Cyber Security Conference on October 16, 2012 in Rockville Maryland. This one-day conference will consist of Cyber Sessions in the NRC Auditorium given by government and industry speakers. NRC Auditorium 11545 Rockville Pike, Rockville, MD 20852. More information.

-Oct. 16-17, The Cyber Maryland Conference - A two-day conference that includes 28 sessions in three tracks, a cybersecurity showcase and expo, and the national cybersecurity hall of fame inaugural induction ceremony and awards banquet. Baltimore Convention Center, One West Pratt Street, Baltimore, MD 21201. More information.

# Legislative Lowdown

-Rep. Zoe Lofgren (D-Calif.) last week unveiled a pair of bills aimed at protecting innovation, digital privacy and freedom of expression online, The Hill writes. Lofgren said she aims to get feedback on the two bills in the coming weeks and plans on introducing them during the next session of Congress. With several tech companies headquartered in her district, Lofgren has long advocated for policies that would bolster the tech industry. She hopes her most recent legislation will prevent a sequel to the controversial Stop Online Piracy Act (SOPA).

# Cyber Security Policy News

-A company whose software and services are used to remotely administer and monitor large sections of the energy industry began warning customers last week that it is investigating a sophisticated hacker attack spanning its operations in the United States, Canada and Spain, according to a story first reported by KrebOnSecurity.com. The attack comes as U.S. policymakers remain gridlocked over legislation designed to beef up the cybersecurity posture of energy companies and other industries that maintain some of the world's most vital information networks. Experts say digital fingerprints left behind by attackers point to a Chinese hacking group tied to repeated cyber-espionage campaigns against key Western interests.

Meanwhile, a group of electric companies says it is not opposed to working with the federal government to secure power-grid computer networks, as long as regulators don't proscribe new burdensome and inflexible rules. Senate Commerce Committee Chairman Jay Rockefeller, D-W.Va., helped sponsor legislation that would have created more government oversight of certain critical networks, including those that control electric grids. After that bill floundered in the Senate partly because of industry opposition to new rules, he wrote a letter to top leaders of Fortune 500 companies asking them about their views on cybersecurity. A copy of that letter, obtained by a reporter with the National Journal, says the utilities are open to voluntarily collaborating with government officials.

-The world's largest professional organization for computer engineers exposed user names, plaintext passwords, and website activity for almost 100,000 of its members, some of whom are employees of Apple, Google, IBM, and other large companies. The sensitive information was contained in 100 gigabytes worth of website logs that were publicly available for at least a month on servers maintained by the Institute of Electrical and Electronics Engineers, according to a blog post published by a recent graduate and current teaching assistant at the University of Copenhagen. The 99,979 unique user names Radu Dragusin said he found in the cache comprises about 24 percent of 411,000 members counted in the 2011 IEEE Annual Report.

-Rented computers from seven different companies secretly took photographs of their users, US authorities have said. The BBC reports that the companies used software made by US company Designerware which could track key strokes and other personal data. The software, called PC Rental Agent, captured people engaging in "intimate acts", including sex. The FTC named DesignerWare, LLC, a company that licensed software to rent-to-own stores to help them track and recover rented computers. According to the FTC, DesignerWare's software contained a "kill switch" the rent-to-own stores could use to disable a computer if it was stolen, or if the renter failed to make timely payments. DesignerWare also had an add-on program known as "Detective Mode" that purportedly helped rent-to-own stores locate rented computers and collect late payments. The FTC said DesignerWare's software also collected data that allowed the rent-to-own operators to secretly track the location of rented computers, and thus the computers' users.

-The Defense Information Systems Agency has been tapped to tighten up network security of all branches of the federal government except the State Department and the FBI, which have their own systems. According to NextGov, the move is in response to the unauthorized release of hundreds of thousands of pages of Pentagon and State classified documents in 2010 and 2011 by the website WikiLeaks, the agency said. Defense Secretary Leon Panetta on July 20 hinted at Pentagon assistance to other federal agencies to beef up security for their networks. DISA obliquely disclosed Monday in contract documents that it will function as the common service provider for the new public key infrastructure hardware tokens, certificates and services for federal classified and secret networks except those belonging to State and the FBI.

-The Defense Department's top industrial policy official said last week that when it comes to securing the technology supply chain, the agency needs to accept the fact that it no longer dominates the market for most of the products it buys, Federal News Radio reports. The phrase "Defense Industrial Base" is one too-often thrown around without much consideration for what actually makes up the marketplace for goods and services the military buys each day, said Brett Lambert, DoD's deputy assistant secretary for manufacturing and industrial base policy. To make progress on securing the modern supply chain, the Pentagon needs to rid itself of the outdated notion that there's a monolithic bloc of defense companies that supply products to warfighters.

*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.*