# GW CSPRI Newsletter

August 25, 2014

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



# Announcements

The National Science Foundation has awarded GW's Cyber Security Research and Policy Institute (CSPRI) a five-year, $4.14 million renewal grant for the project "PISCES 2019: Partnership in Securing Cyberspace through Education and Service: Renewal." Prof. Lance Hoffman (CSPRI director) is the PI on the grant, and Profs. Rachelle Heller (CS) and Costis Toregas (CSPRI lead research scientist) are the co-PIs. The renewal is a testament to the quality of the program and its success in placing graduates in the workplace. Since 2004, more than 70 GW graduates have benefited from PISCES' CyberCorps (and related) scholarships awarded through CSPRI; and these graduates have been placed in more than 35 government agencies, national labs, and federally funded research and development corporations. More information about the CyberCorps program and scholarships is available on theGW CyberCorps website.

# Events

-Aug. 26, 1:00 p.m. – 1:30 p.m., **Ask the Dept. of Labor CIO** – Dawn Leaf, the Labor Department's deputy chief information officer, will join Federal News Radio for a free online chat. Leaf will discuss Labor's priorities around IT modernization, data center consolidation, and cybersecurity. More information.

-Aug. 28, 7:00 p.m., **Build It, Break It, Fix It** - security contest aims to teach students to write more secure programs. The contest evaluates participants' abilities to develop secure and efficient programs. The contest is broken up into three rounds that take place over consecutive weekends. During the Build It round, builders write software that implements the system prescribed by the contest. In the Break It round, breakers find as many flaws as possible in the Build It implementations submitted by other teams. During the Fix It round, builders attempt to fix any problems in their Build It submissions that were identified by other breaker teams. Each round will respectively start on August 28th**,** September 4th, and September 12th**.** More information.

-Aug. 28, 7:00 p.m. – 10:00 p.m., **CharmSec Meetup** – An informal, all-ages, citysec-style meetup of information security professionals in Baltimore. Heavy Seas Alehouse, 1300 Bank Street, Baltimore, MD, 21231. More information.

-Sept. 3, 6:30 p.m. – 8:30 p.m., **OWASP DC Meetup: The World of Ruby on Rails Security** – Take a quick trip through the world of Ruby on Rails security! The journey will start with an overview of security features offered by the popular web framework, then detour through dangerous pitfalls and unsafe defaults, and finally end with suggestions for improving security in Rails apps and integrating improvements into the development process. Uber, 1200 18th Street NW, Suite 700. More information.

# Legislative Lowdown

-Some in the business community are asking how many data breaches need to happen before Congress sees fit to pass a national data breach disclosure law. As The Hill reports, a credit union trade group is calling on Congress to get it done when lawmakers return from their August recess. “Despite an initial flurry of talk and activity on Capitol Hill after Target suffered a massive breach affecting up to 110 million shoppers last year, there has so far been little movement for some type of data security bill in Congress,” Julian Hattem writes. “Squabbling between congressional committees and disagreement over how far a bill should go have sidelined the issue for the time being, and it’s not likely to come back in the short period lawmakers have left before the midterm elections in November.”

# Cyber Security Policy News

-Data breaches took center stage last week, with several high-profile attacks jeopardizing personal information on millions of U.S. consumers. Reuters was the first to report that Community Health Systems Inc., one of the biggest U.S. hospital groups including some 200 hospitals, was the victim of a cyber attack from China, resulting in the theft of Social Security numbers and other personal data belonging to 4.5 million patients. “The information stolen from Community Health included patient names, addresses, birth

dates, telephone numbers and Social Security numbers of people who were referred or received services from doctors affiliated with the hospital group in the last five years, the company said in a regulatory filing," the publication reported.

Also disclosing a breach last week was the shipping giant UPS. First acknowledged in a state data breach disclosure law filing, the breach involved the malware compromise of credit card payment terminals at some 51 locations in 24 states.

News of the UPS breach surfaced as the U.S. Department of Homeland Security issued an updated advisory about the breadth of payment terminal compromises that the agency is seeing across hundreds of organizations. As the New York Times reports, the advisory stated that more than 1,000 American businesses have been affected by the cyberattack that hit the in-store cash register systems at Target, Supervalu and UPS. "On July 31, Homeland Security, along with the Secret Service, the National Cybersecurity and Communications Integration Center and their partners in the security industry, warned companies to check their in-store cash register systems for a malware package that security experts called Backoff after a word that appeared in its code," Nicole Perlroth wrote. "Until that point, Backoff malware and variations of it were undetectable by antivirus products. Since then, seven companies that sell and manage in-store cash register systems have confirmed to government officials that they each had multiple clients affected, the government said Friday. Some of those clients, like UPS and Supervalu, have stepped forward, but most have not."

Uncle Sam even got in on the data breach news. Computers at the Nuclear Regulatory Commission were successfully hacked by foreigners twice over the past three years, according to an internal investigation. As NextGov reports, "one incident involved emails sent to about 215 NRC employees in 'a logon-credential harvesting attempt. In another case, intruders broke into the personal email account of an NRC employee and sent malware to 16 other personnel in the employee's contact list. A PDF attachment in the email contained a JavaScript security vulnerability'."

-BBC carried a story last week that is sure to cheer those weary of news about governments spying on their own citizens. The publication wrote that British and American intelligence agents attempting to hack the 'dark web' are being deliberately undermined by colleagues. "Spies from both countries have been working on finding flaws in Tor, a popular way of anonymously accessing 'hidden' sites," writes Leo Kelion. "But the team behind Tor says other spies are tipping them off, allowing them to quickly fix any vulnerabilities."

-The White House's new cybersecurity coordinator last week deflected questions about his lack of experience in IT security, saying his expertise in the field was more likely to be an asset rather than a liability. "Being too down in the weeds at the technical level could actually be a little bit of a distraction," Daniel, a special assistant to the president, says in an interview with Information Security Media Group. "You can get enamored with the very detailed aspects of some of the technical solutions," he says. "And,

particularly here at the White House ... the real issue is to look at the broad, strategic picture and the impact that technology will have." Read more at GovInfoSecurity.com.

*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.*