GW CSPRI Newsletter

September 2, 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

Events

-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.

Sept. 4, 6:30 p.m. – 8:00 p.m., **OWASP NoVA Meetup** – Living Social, 11600 Sunrise Valley Dr., Reston, VA 20136. More information. 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. More information.

-Sept. 4, **Build It, Break It, Fix It** – This is a new security-oriented programming contest held by the Maryland Cybersecurity Center, Cyberpoint, and Trail of Bits. The contest aims to teach students to write more secure programs, and evaluates participants' abilities to develop secure and efficient programs. The event 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.

-Sept. 5, 7:00 p.m. – 10:00 p.m., **2600 Arlington Meetup** –The goal of the meetings is to discuss technology, hacking, computers, and anything of general interest. The meetings are open to anyone who has a general interest in technology, though the discussion can be technical / dive into geekery at times. Rock Bottom, 4238 Wilson Blvd., Arlington, VA 22203.

-Sept. 9-10, **Cybersecurity Simulation and Exercise for Banks and Credit Unions** – Over a two day period this fall, hundreds of security risk and IT professionals will experience a highly realistic set of scenarios in a safe environment in order to practice and improve their response to cyber incidents. The teams are encouraged to involve multiple parts of their organizations, from IT and security to payments experts to communications teams to line of business leaders and executive teams. Registration and more information (PDF).

-Sept. 10, 2:00 p.m., **Operationalizing Cyber for the Military Services** – The House Committee on Armed Services' Subcommittee on Intelligence, Emerging Threats and Capabilities will hold a hearing. Rayburn House Office Bldg., Room 2212. More information.

-Sept. 10, 3:00 p.m. – 4:30 p.m., **Data Breach Prevention, Response and Management: The Road to Reasonable Security** – Panelists on this Webinar will offer an overview of "reasonable security" with an emphasis on consumer protection, business continuity and litigation considerations. More information.

-Sept. 10, 3:00 p.m. – 8:00 p.m., **ISACA CM Meetup: Building an Effective Periodic User Access Review Process** – During this session, the speaker will discuss Identity Access Governance Theory, common pitfalls the access review process will face, what an actual review process looks like, and then conduct a real world walk through. Chiapparelli's Restaurant, 237 S. High St., Baltimore, MD 21202. More information.

-Sept. 16, 8:00 a.m. – 5:30 p.m., **5th Annual Billington Cybersecurity Summit** – This conference will feature talks from well-known cybersecurity speakers including Admiral Michael Rogers, Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service. This leading summit also will feature Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator, The White House; David DeWalt, Chairman and Chief Executive Officer, FireEye; Dr. Phyllis Schneck, Deputy Under Secretary for Cybersecurity, NPPD. Capital Hilton, 1001 16th St. NW. More information.

Legislative Lowdown

-The Federal Trade Commission (FTC) is considering new ways in which parents can verify their kids' identities online, writes The Hill. The proposed changes are to The Children's Online Privacy Protection Act, last updated in July 2013, which requires websites to obtain consent from the parents of children who are under the age of 13 before sharing their personal information.

Cyber Security Policy News

-The FBI is investigating claims that a hacker stole nude photos of actress Jennifer Lawrence and a host of other celebrities and posted them online. Apple says it's investigating whether any iCloud accounts had been hacked, and it remains unclear how the attackers obtained the images. "Some cybersecurity experts speculated that hackers may have obtained a cache of private celebrity images by exploiting weaknesses in an online image-storing platform," reports The Associated Press.

-Contractors that work with the U.S. Defense Department are expecting new rules that will require them to report computer breaches to the Pentagon and give the government access to their networks to analyze the attacks, according to Bloomberg. "Groups representing the contractors are raising concern about the Pentagon rooting around their data, and say smaller companies may not even have the cybersecurity protections needed to comply," writes Chris Strohm. "The pending rule change marks an escalation of efforts to understand the scale of hacking as the Defense Department plans to spend $23 billion through fiscal year 2018 on cybersecurity. The crux of the rule is designed to ensure companies handling classified data quickly inform the Pentagon of hacking attacks."

Information sharing about breaches works both ways, of course. Toward that end, the FBI and DHS say they will work to release cyberthreat information more rapidly to the healthcare industry, following a massive breach at hospital vendor Community Health Systems that jeopardized more than 4 million patient records. According to Computerworld, part of the problem is that much information gathered by federal investigators is classified, and needs to be de-classified or vetted before being shared with private industry.

The federal government also has much work to do in sharing threat information with its state partners. Government Technology carries a story which notes that despite a 2013 executive order calling on DHS to share classified and unclassified cybersecurity information to 16 "critical infrastructure" sectors, most state officials remain unaware of the program. "Three state chief information security officers (CISOs) were contacted by *Government Technology* and none of them were familiar with the DHS Enhanced Cybersecurity Services program," reports Brian Heaton. "Designed to pass along "indicators" of hacker threats, the program was expanded by executive order in early 2013. It previously was restricted to federal defense contractors."

-The White House last week announced that it had appointed Mikey Dickerson, a former Google engineer, to head up the new U.S. Digital Service, a tech corps tasked with helping Uncle Sam redeem its tech projects in much the way that Dickerson aided the government in its efforts to shore up Healthcare.gov last year, The Washington Post reports. "The White House today posted a video of Dickerson's employee on-boarding process and in the nearly 5 minute clip the White House makes much of Dickerson's appearance," writes Nancy Scola. "And with the video, the White House is attempting to signal that government will change -- not the technologists it hires."

The new hire comes as the government is preparing for a significant restructuring of the Defense Information Systems Agency (DISA), an organization that has long held the mantle of providing information technology and communications support to the president, vice president, secretary of defense, the military services and the combat commands. "Officials, for now, are keeping quiet about most of the details of the reorganization, but many of the adaptations that do take place will begin to appear around Oct. 1, when DISA expects to declare 'initial operational capability' for the restructured organization," writes Jared Serbu for Federal News Radio.

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.