GW CSPRI Newsletter

February 24, 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

It's the Economics, Stupid.
Everyone from the President on down has acknowledged that Cyber Security often comes down to incentives. Have an idea about the market side of cyber security? Submit to the annual Workshop on the Economics of Information Security, held this year at Penn State University in June. Papers due February 28. More info here: http://weis2014.econinfosec.org/cfpart.html

Events

-Feb. 24-26, **Big Data for Federal Government and Defense** - The amount of data the government faces is at its highest ever and less than one-third of federal IT executives believe they have a sufficient Big Data strategy. Big Data for Government & Defense will be an opportunity for CIOs, IT directors, program managers and more to express the latest government challenges, strategies and initiatives relating to federal Big Data. Hear from those closest to these developments as they speak on topics including advancing data mining processes; increasing server storage capacity; Big Data security; Cloud-like infrastructure to support big data. Walter E. Washington Convention Center. 801 Mt. Vernon Place NW., Washington, DC. More information.

-Feb. 26, 5:00 p.m. - 7:00 p.m., **ISSA Baltimore Meetup** - The topic will be "EMET, Windows XP End of Life." CyberCore Technologies, 6605 Business Parkway, Elkridge, MD, 21075. More information.

-Feb. 26, 6:30 p.m. - 9:00 p.m, **CapSec DC Meetup** - This group is a social gathering group for people interested in all facets of information security. We meet about once a month to socialize and network. No agenda, no sponsors, just food, drink, and conversations with folks interested in security in the DC Metro area. Fado Irish Pub & Restaurant, 808 7th Street NW.

-Feb. 27, 9:30 a.m., **U.S. Strategic Command and U.S. Cyber Command** - The Senate Armed Services Committee will hold a hearing to receive testimony on U.S. Strategic Command and U.S. Cyber Command in review of the Defense Authorization Request for Fiscal Year 2015 and the Future Years Defense Program. Witnesses will include Admiral Cecil D. Haney, USN, commander, U.S. Strategic Command; and General Keith B. Alexander, USA, commander, U.S. Cyber Command. Senate Dirksen Office Bldg., Room SD-G50. More information.

-Feb. 27, 6:30 - 8:30 p.m., **OWASP DC Meetup**: An introduction to Bitcoin Security with Applications - Bojan Simic will provide a short background into Bitcoin and how it works. He will then provide some of his firsthand experiences with the state of Bitcoin businesses with regard to security and how many individuals are (insecurely) handling their Bitcoins. These experiences will demonstrate some "hacks" that pertain to the OWASP Top 10 as well as other types of vulnerabilities. The talk will include an overview of simple security steps that individuals and businesses who are working with Bitcoin should take to in order to mitigate the chance of hackers stealing Bitcoin and Personally Identifiable Information (PII) from them and their customers. Uber, 1200 18th Street NW, Suite 700. More information.

-Feb. 28, 9 a.m. – 10 a.m., **Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat** - The Bipartisan Policy Center's (BPC) **Electric Grid Cybersecurity Initiative** will release its recommendations for how government and industry can protect the North American electric grid from cyber attacks at an event at BPC. More information.

-Mar. 4, AFCEA DC **Cybersecurity Summit 2014** - Attendees will have an opportunity to see what challenges key DoD and federal cyber leaders are facing today; engage in breakout sessions on critical topics; network with cyber professionals and discuss new ideas and solutions; and hear where agencies are headed and where the budgets are in 2014. Capital Hilton, 1001 16th St. NW. More information.

-Mar. 5-7, **IAPP Global Privacy Summit 2014** - Washington Marriott Wardman Park, 2660 Woodley Rd. NW More information.

-Mar. 5, 10:30 a.m., **Information Technology and the Future of Defense** - Speakers will include David Zolet, executive vice president and general manager, CSC North

America Public Sector; and Jason Healey, director, Cyber Statecraft Initiative, Brent Scowcroft Center on International Security, Atlantic Council 1030 15th Street, NW, 12th Floor. More information.

Cyber Security Policy News

Edward Snowden warns in a new TV interview that the National Security Agency can track people no matter how well they hide their online presence. "The public has a right to know that, which the government is doing in its name," Snowden said. "Anywhere you try and hide your online presence, the NSA can find you." The Hill writes of Snowden's last revelations.

With so many leaks about the extent of U.S. government domestic surveillance programs, it is increasingly difficult to separate fact from fiction regarding a number of the NSA's most epic hacks. But as Reuters reports, a major flaw in Apple Inc software for mobile devices could allow hackers to intercept email and other communications that are meant to be encrypted. "Because spies and hackers will also be studying the patch, they could develop programs to take advantage of the flaw within days or even hours," Reuters writes. "The issue is a 'fundamental bug in Apple's SSL implementation.' "If attackers have access to a mobile user's network, such as by sharing the same unsecured wireless service offered by a restaurant, they could see or alter exchanges between the user and protected sites such as Gmail and Facebook. Governments with access to telecom carrier data could do the same." (GW has advice to users of Apple products on how to protect themselves from this threat.)

The virtual currency Bitcoin may be emerging from a few weeks of negative headlines, but one of the most outspoken regulators on the issue says he still sees promise in the virtual currency. Benjamin Lawsky, New York Superintendent of Financial Services, gave the comments last Thursday in a two-hour question-and-answer session on social news site Reddit. "Lawsky has spoken publicly about the future of bitcoin, a decentralized currency created in 2008 by a person or people under the pseudonym Satoshi Nakamoto, and its peers before," the National Journal writes. "Earlier this month, he said there could be a 'kernel of something here that will have a profound impact on the future of payments technology and our financial system,' even as he cited recent problems with the Bitcoin exchange Mt. Gox and acknowledged regulators are not the experts, necessarily, on cryptocurrency.

-The Obama administration recommends a uniform federal standard requiring businesses to quickly report thefts of electronic personal information, according to USA Today's description of the testimony of Acting Assistant Attorney General Mythili Raman before the Senate Judiciary Committee."The hearing explored ways to combat cyber-crime after massive data breaches at major retailers, including Target, which announced it is spending $100 million to expedite transition to 'smart' cards with computer chips from the standard magnetic strip credit and debit cards."

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.