GW CSPRI Newsletter

October 15, 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. 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 1-Day Conference will consist of Cyber Sessions in the NRC Auditorium given by government and industry speakers. NRC Auditorium 11545 Rockville Pike, Rockville, MD. 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.

-Oct. 17, 10:00 a.m. - 11:30 a.m., **Why Should You Care About Protecting Your Privacy and Identity in Cyberspace?** - This panel discussion, hosted by GWU, will include: Dr. Daniel J. Solove, John Marshall Harlan research professor of law, GW Law School; Darrell Darnell, GW senior associate vice president for safety and security; Danielle Lico, GW associate dean of students for student administrative services and senior advisor to the dean; Ashwin Narla, president, GW Student Association; Benjamin Fielden, manager of student technology services, Division of IT. The discussion will be moderated by Dennis Devlin, assistant vice president of information security & compliance services, Division of IT. Jacob Burns Moot Court Room (2000 H Street, NW).

-Oct. 19, 10:00 a.m., The Commission on Security and Cooperation in Europe will receive a briefing on online safety under repressive regimes, focusing on responsibility of technology

companies. Rayburn House Office Bldg., Room 2203.

-Oct. 19-20, **Hacking Across the Commonwealth for EDUcation** - Apps4VA, a collaborative effort between the Center for Innovative Technology and the Virginia Department of Education to encourage the development of new and innovative ways to use and analyze education data, is hosting a series of hackathons that will occur simultaneously in five separate locations in Virginia and linked via webcast. Participants will have 24 hours to create software applications using education data and winners will earn cash and other prizes. Meals and snacks will be provided. There is no fee to register. More information.

-Oct. 24, 10:00 a.m. -11:30 a.m., **Protecting Your Data in the Cloud** - This seminar is offered as part of GWU's observation of Cybersecurity Awareness Month. Marvin Center 413/414.

-Oct 24, 11:00 a.m., **The Battle for Control of Online Communication** - The George Washington University Department of Computer Science is hosting a Colloquium on Wednesday by Nick Feamster of University of Maryland and Georgia Tech. Dr. Feamster will discuss a study of the network-level behavior of spammers, present a spam filtering system that classifies e-mail message based on the network-level traffic characteristics rather than the contents of the message. He will also describe emerging threats concerning domain name registration and methods to ascertain the legitimate reputation of domain names. Approaches to monitor and circumvent attempts to restrict and manipulate access to online information will also be discussed. Refreshments will be provided. Academic Center, 801 22nd St. NW, Computer Science Conference Room 736.

-Oct 24, 6:30 p.m. - 8:00 p.m., **Journalists' Digital Security** - What would you do if you found your computer had been hacked and sensitive emails with sources, story research and interview notes were now exposed? Or what if you learned someone had intercepted your cell phone conversations and used them to learn the identity your would-be 'Deep Throat?' To raise awareness about just how serious the digital security problem is, the National Press Club's Press Freedom Committee will hold a panel discussion. This event is free and open to the public. National Press Club. 529 14th St. NW,, 13th Fl. More information.

-Oct. 24-25, **SINET D.C. Showcase & Workshops** - A chance to meet and listen to some of the nation's top cybersecurity leaders. The theme of the conference is finding ways to advance cybersecurity innovation through public-private partnerships. Keynotes include talks from U.S. Director of National Intelligence Stephanie O'Sullivan, White House Cybersecurity Coordinator Michael Daniels, and AT&T CSO Dr. Edward Amoroso. National Press Club, 529 14th Street, N.W., 13th Floor. More information.

Legislative Lowdown

-Senate Majority Leader Harry Reid (D-Nev.) said he will try and revive stalled cybersecurity legislation on the heels of Defense Secretary Leon Panetta's warning that the U.S. is at risk of a devastating cyber-attack, The Hill reports. Reid, in a statement Saturday, said that when Congress returns in November he will bring back legislation that stalled in August. "My colleagues who profess to understand the urgency of the threat will have one more chance to

back their words with action, and work with us to pass this bill," Reid said. A bipartisan cybersecurity bill failed to secure the needed 60 votes to advance in early August, an impasse fueled by GOP concerns that the bill would require too much from businesses.

Meanwhile, a group of House and Senate GOP lawmakers on Thursday urged President Obama to not issue an executive order on cybersecurity because they argue it would give countries like Russia and China more ammunition in their push to give the United Nations more regulatory control over the Internet.

Cyber Security Policy News

-Defense Secretary Leon Panetta said late last week that a series of recent electronic attacks that have been tied to Iran, both in the U.S. and abroad, herald a "significant escalation in the cyberthreat," and warned the U.S. would aggressively pursue the perpetrators, in what cybersecurity experts called a veiled warning to Tehran. U.S. officials believe hackers supported by the Iranian government staged a set of cyberattacks against oil and gas companies to retaliate against tightened sanctions, the Wall Street Journal reported.

In its analysis, The New York Times said defense officials insisted that Mr. Panetta's words were not hyperbole, and that he was responding to a recent wave of cyberattacks on large American financial institutions. He also cited an attack in August on the state oil company Saudi Aramco, which infected and made useless more than 30,000 computers. "But Pentagon officials acknowledged that Mr. Panetta was also pushing for legislation on Capitol Hill," The Times wrote. "It would require new standards at critical private-sector infrastructure facilities — like power plants, water treatment facilities and gas pipelines — where a computer breach could cause significant casualties or economic damage."

-The Supreme Court declined to review a lower court ruling in a case that challenged a Bush-era law (the FISA Amendments Act), retroactively giving telecommunications firms—including Verizon, Sprint, and AT&T—legal immunity after performing warrantless wiretapping at the government's request, Ars Technica reports. The case, Hepting v. AT&T, was a class-action suit filed in 2006 by the American Civil Liberties Union and Electronic Frontier Foundation on behalf of customers. They originally sought billions of dollars in damages by arguing the telecom firms violated both users' privacy and federal law. However, in the wake of this lawsuit and others like it, Congress passed the retroactive immunity law (FISA AA). The central question in the Hepting case was whether these immunity provisions were constitutional.

-By the end of 2012, major Internet service providers (ISPs) in the US will have in place monitoring systems that will help implement a six-strikes plan to discourage illegal filesharing, according to Wired.com. Being dubbed the "Copyright Alert System," the plan will result in increasingly severe responses for each successive strike, although "each strike is dozens or scores or hundreds of infringements." The first several strikes will result in warnings; subsequent strikes could result in users being redirected to a certain page until they contact the ISP to discuss the matter or having their Internet speeds throttled. The plan involves monitoring peer-to-peer filesharing services. Much of the response is aimed at being educational rather than punitive.

-A single mysterious computer program that placed orders — and then subsequently canceled

them — made up 4 percent of all quote traffic in the U.S. stock market last week, CNBC wrote last week. The motive of the algorithm is still unclear. The program placed orders in 25-millisecond bursts involving about 500 stocks, according to Nanex, a market data firm. The algorithm never executed a single trade, and it abruptly ended at about 10:30 a.m. ET Oct. 5. Experts believe the ultimate goal of many of these programs is to gum up the system so it slows down the quote feed to others and allows the computer traders (with their co-located servers at the exchanges) to gain a money-making arbitrage opportunity. The scariest part of this single program was that its millions of quotes accounted for 10 percent of the bandwidth that is allowed for trading on any given day, according to Nanex.

-An information breach at a Florida college has compromised information of about 279,000 students and employees, the Florida Department of Education said on Wednesday. Computerworld reports that the breach in computer systems at Northwest Florida State College in Niceville also compromised the personal information of some 3,200 current and retired college employees. The school was still investigating the cause of the breach, which lasted between May 21 to Sept. 24 and included name, birth date, employee direct deposit bank routing and account number information, and Social Security numbers. At least 50 employees were hit by identity thefts as a result of the breach, the school's president was quoted as saying.

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.