# GW CSPRI Newsletter

July 30, 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.*

## Contents

# Events

-July 31, 10:00 a.m., **State of Federal Privacy and Data Security Law: Lagging Behind the Times?** - The Senate Homeland Security and Governmental Affairs Committee's Subcommittee on Oversight of Government Management will hold a hearing. The witnesses will include Mary Ellen Callahan, chief privacy officer, Department of Homeland Security; Greg Long, executive director, Federal Retirement Thrift Investment Board; Greg Wilshusen, director of information security, Government Accountability Office; Peter Swire, professor of law, Ohio State University law school; Chris Calabrese, legislative counsel, ACLU; and Paul Rosenzweig, visiting fellow, Heritage Foundation. Dirksen Senate Office Bldg., Room 628. More information.

-Aug. 2, 9:30 a.m. - 10:30 a.m., **Will the Real Internet Freedom Please Stand Up?** - A broadly worded Declaration of Internet Freedom was recently issued by a broad coalition, some of which are already using the document to push for increased regulation, such as net neutrality mandates. Meanwhile, a coalition of free market groups has offered a counter-declaration that shares much common ground, but emphasizes restraint, respect for the rule of law, and humility as guiding principles for policymakers approaching the Internet and digital markets. Can these two visions be reconciled or are they fighting for very different goals? What is real Internet Freedom? Sen. Rand Paul (R-KY) will address these issues in a speech at the Heritage Foundation, 214 Massachusetts Ave., NEMore information.

-August 6-8, **Digital Forensic Research Workshop** - The annual Digital Forensic Research Workshop conference allows digital forensics researchers from government, industry, and academia to present their work and results to fellow researchers and practitioners. Many of the most cited digital forensics papers have been presented at DFRWS and the annual challenge has spawned research in important areas. Initial results and tool prototypes are also presented during the Works in Progress and demo sessions. Embassy Suites, 1250 22nd Street, NW. More information.

# Legislative Lowdown

-The Senate voted on Thursday to move ahead on a bill designed to boost cybersecurity, setting the stage for debate next week, NextGov reports. Senate leaders spent Thursday gathering support for the motion to proceed on the Cybersecurity Act of 2012. Some Republicans, like Sen. John McCain, R-Ariz., had said the Senate should not consider the cybersecurity legislation until more disagreements were worked out. In the end, however, compromise language introduced by the bill's sponsors last week appears to have won over enough support to for an 84-11 vote to move forward with debate next week.
An open amendment policy was agreed to in approaching the bill next week, and several lawmakers are proposing add-ons. Sen. Patrick Leahy (D-Vt.) is pushing for an amendment to a cybersecurity bill that would make it a crime for a company to hide a data breach from its customers, The Hill writes. Under the legislation, anyone who purposefully conceals a data breach that causes financial damage could face up to five years in prison.
Meanwhile, Sen. Ron Wyden (D-Ore.) plans to offer an amendment to cybersecurity legislation that would require law enforcement officials to procure a warrant before obtaining location data from a person's cell phone, laptop or other gadgets.

-On July 31, the House of Representatives will meet to consider several technology and security related bills, including the "Foreign and Economic Espionage Penalty Enhancement Act of 2012", the "Child Protection Act of 2012", and the "STOP Identity Theft Act of 2012". More information on the votes is available via Rep. Cantor's schedule for the week.

# Cyber Security Policy News

-The top American military official responsible for defending the United States against cyberattacks said Thursday that there had been a 17-fold increase in computer attacks on American infrastructure between 2009 and 2011, initiated by criminal gangs, hackers and other nations. The New York Timescites an assessment by Gen. Keith Alexander, who heads the National Security Agency and was also recently tapped to lead the U.S. Cyber Command.

-More than 20,000 hackers and security professionals descended on Las Vegas this week to attend the back-to-back conferences BlackHat and DefCon last week. A major theme of this year's conference was mobile security, and a number of researchers presented new methods for breaking the security of mobile platforms like Google's Android operating system. NPR's Steven Henn reports on a couple of hacks that were displayed. Some mobile phones can connect with other networks in all kinds of ways and some have payment systems that use near-field communication, or NFC, chips. These chips let you wave you phone near an NFC reader, your phone connects and you can pay. Charlie Miller, a researcher at Accuvant, realized he could use those chips to break a phone wide open. For this hack to work, Miller just has to be standing next to you. Ethical hacker and researcher Nicholas Percoco figured out how to slip past Google's bouncer, the system that polices Android's app store. Ridley and his partner figured out how to attack the computer chips that run pretty much every mobile phone.

At DefCon, National Security Agency Director General Keith B. Alexander asked attendees for help. NSA's and U.S. Cyber Command's roles are to protect the nation from cyberattacks and foreign intelligence, Gen. Alexander said. The issue is that if you don't see a cyberattack you can't defend against it and at the moment, the NSA has no insight if Wall Street is going to be attacked, for example, he said. Gen. Alexander pointed out that if the industry could share some limited pieces of information from their intrusion detection systems in real time, the NSA could take it from there. The next step from information sharing is jointly developing standards that would help secure critical infrastructure and other sensitive networks, he said. He encouraged hackers to get involved in the process.

-Alexander used the speech to deny claims by a former NSA chief that the agency is creating digital dossiers on tens of millions of Americans, in violation of federal laws that bar the agency from spying on American citizens. Wired.com writes that A former NSA official has accused the NSA's director of deception during a speech he gave at the DefCon hacker conference on Friday when he asserted that the agency does not collect files on Americans. William Binney, a former technical director at the NSA, said during a panel discussion that NSA Director Gen. Keith Alexander was playing a "word game" and that the NSA was indeed collecting e-mails, Twitter writings, internet searches and other data belonging to Americans and indexing it. Alexander also told the audience that the NSA targets only foreign entities and that if it "incidentally" picked up the data of Americans in the process, the agency was required to "minimize" the data, "which means nobody else can see it unless there's a crime that's been committed." Minimization refers to legal restrictions under the United states Signals Intelligence Directive 18 on how data pertaining to U.S. citizens can be handled, distributed or retained.

(Three of GW's CyberCorps students were attending BlackHat or DefCon or both, supported by their GW scholarships provided by the National Science Foundation and the Department of Homeland Security.  They will report back on what they learned to their classmates when classes resume at the end of this month.)

At the same time, the Pentagon is still trying to figure out how to write the rules of cyberwarfare, wrestling with such weighty questions as how to fire back against a computer-based attack that has physical consequences. The Associated Press writes that four months ago the military's top cyberwarrior predicted the rules would be ironed out in a "month or two" and sent to other federal agencies for discussion. But the complex world of cyberspace, which has no real boundaries and operates at the speed of light, has proven to be a difficult battlefield for the military to map out, senior military leaders told lawmakers last week. House members said that working out the rules of cyberwar is critical so that the military will be able to respond quickly when U.S. networks are attacked or threatened. Rep. Mac Thornberry, R-Texas, told military leaders that there likely won't be time for Congress to pass a declaration of war if or when a computer-based attack.

*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.*