GW CSPRI Newsletter

July 16, 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 16-20, **Open Group Conference** - Cybersecurity will be a major theme at this year's conference, which will focus on identifying risks and eliminating vulnerabilities that could undermine integrity and supply chain security. Hyatt Regency, Capitol Hill, 400 New Jersey Avenue, NW. More information.

-July 17-18, **United States Department of Agriculture Cyber Security Summit & Expo** - This USDA conference will provide participants with information and resources on today's vulnerabilities, incidents, security lifecycle, risks and mitigations; it will also identify ways build a solid security foundation program to meet future challenges and trends in cyber security. The Cybersecurity Expo, running in conjunction to the Summit, will provide live demos and informational booths focused around the summit topics. USDA Headquarters, 14th & Independence Ave, S.W. More information.

-July 18, 2:30 p.m., **What Facial Recognition Technology Means for Privacy and Civil Liberties** - The Senate Committee on the Judiciary has scheduled a hearing of the Subcommittee on Privacy, Technology and the Law. Witnesses to include Jerome Pender, deputy assistant director, Information Services Branch, Criminal Justice Information Services Division, FBI; Maneesha Mithal, associate director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission; Rob Sherman, manager of privacy and public policy, Facebook; Jennifer Lynch, staff attorney, Electronic Frontier Foundation. Dirksen Senate Office Bldg., Room 226. More information.

Legislative Lowdown

-The pressure is on lawmakers in the Senate to proceed with comprehensive cybersecurity legislation, but with the August recess nearly three weeks away, it will be difficult for lawmakers move forward on a cybersecurity bill. Yet, writing for The Hill, Jennifer Martinez says it may be too early to dismiss the possibility. Some are holding out for progress to be made on a compromise framework drafted by Sens. Jon Kyl (R-Ariz.) and Sheldon Whitehouse (D-RI) on provisions dealing with critical infrastructure, such as water systems and telecommunications networks. The U.S. Chamber of Commerce met with Kyl and his staff this past week to discuss the latest version of the framework. A spokesman for the Chamber said the business lobby had a “constructive dialogue” with Kyl at the meeting and declined to comment further.

Cyber Security Policy News

-The head of the Pentagon’s Cyber Command on Monday called for swift action in Congress to sort out roles, standards and authorities for government agencies charged with defending against destructive computer attacks. Speaking at a think tank gathering in Washington, Army Gen. Keith Alexander said the time for legislative action is now, before the nation is hit with a major cyberattack — an event he called increasingly likely.

Critics have raised privacy concerns about a bill passed in the House of Representatives earlier this year that would allow the government and companies to share information about cybersecurity threats and hacking, saying it would allow the agency that Alexander heads -- the National Security Agency -- to collect data on American communications, which is generally prohibited by law. Reuters writes that Alexander used the speech at the American Enterprise Institute to reassure Americans that the NSA would not read their personal email if a new cybersecurity law was enacted to allow more sharing between private companies and the government. He said the information the government was seeking was the Internet address where an email containing malicious software originated and where it traveled to, not the content of the email. "It doesn't require the government to read their mail or your mail to do that. It requires them, the Internet service provider or that company, to tell us that that type of event is going on at this time. And it has to be at network speed if you're going to stop it," Alexander said.

Mobile carriers responded to a staggering 1.3 million law enforcement requests last year for subscriber information, including text messages and phone location data, according to data provided to Congress, Wired.com reports. The revelation marks the first time figures have been made available showing just how pervasive mobile snooping by the government has become in the United States. Nine mobile phone companies forwarded the data as part of a Congressional privacy probe brought by Rep. Edward Markey, (D-Massachusetts), who co-chairs the Congressional Bi-partisan Privacy Caucus.

-The Department of Defense does not have a department-wide framework for planning, directing and controlling electronic warfare activities, according to a report (PDF) released last week by the Government Accountability Office. The GAO believes the DoD "may face challenges in its oversight of electronic warfare as a result of the evolving relationship between electronic warfare and cyberspace operations." It also found that "U.S. military's access to and use of the electromagnetic spectrum is facing rapidly evolving challenges and increased vulnerabilities due to the increasing quality and availability of electronic warfare capabilities to both state and non-state actors", and particularly, the People's Republic of China.

-The FBI plans to tap George Mason University scientists to perform tests on the law enforcement agency's Android mobile applications to see if they are hacker-proof, a notice of intent reveals. NextGov carries a story about efforts to "fuzz" FBI mobile applications -- essentially attacking them in automated ways to find security flaws. The scientists have been seeking to develop a “scalable approach for intelligent fuzz testing of Android applications” with the help of cloud computing. “The framework uses numerous heuristics and software analysis techniques to intelligently guide the generation of test cases aiming to boost the likelihood of discovering vulnerabilities,” the paper adds.

-A long-awaited U.S. Food and Drug Administration proposed rule requiring unique identifiers on medical devices was published last week, according to GovInfoSecurity. While the rule aims to ease the collection and analysis of data about adverse health events and help detect counterfeit products, no patient information would be collected in a proposed new FDA database to help track the safety of these devices, the agency notes.

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.