GW CSPRI Newsletter

June 10, 2013

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

-June 17, 3:00 p.m. - 5:00 p.m., **Taking Cyber to the Hill: The Future of Internet Governance** - This is the third discussion in a series exploring the intersection of responsible Internet governance and improved international cybersecurity. The panel will feature three cyber policy experts, each with knowledge and experience in Internet governance and cybersecurity: Jason Healey, director of the Atlantic Council's Cyber Statecraft Initiative; Greg Rattray, former Chief Security Officer of ICANN, principal at Delta Risk LLC, and Atlantic Council Senior Fellow; and Paul Twomey, former President and CEO of ICANN; founder of Argo Pacific; and Atlantic Council board member. US Capitol Visitor Center, Congressional Meeting Room – North, 1 1st Street, SE. More information.

-June 19, 9:30 a.m., **Federal Government Approaches to Issuing Biometrics IDs: Part II** - The House Oversight and Government Reform Committee's Subcommittee on Government Operations will hold a hearing. Rayburn House Office Bldg., Room 2154. More information.

-June 20, 3:15 p.m. - 4:15 p.m., **8th Annual Homeland Security Law Institute** - The American Bar Association is hosting a three-day conference, and one session on the second day is titled "Cyber Security for the Private Sector: What Companies and Their

Lawyers Need to Know." From 9:30 a.m. to 10:30 a.m. on June 21, the ABA will host a panel discussion entitled "Protecting Our Nation's Cyber Critical Infrastructure." Capital Hilton Hotel, 1001 16th St., NW. More information.

-June 21, 12 noon - 1 p.m., **Privacy, the NSA, and Your Constituents' Phone and Internet Records: An Experts' Primer on the Law, the Technology and the History** - A short, 60-minute flash briefing on their legal, legislative, and technical background for Congressional staff. The discussion will include experts on surveillance programs and the Congressional acts that may or may not have authorized them -- from the PATRIOT Act to the Foreign Intelligence Surveillance Act. The panel will also discuss some technical aspects related to accessing and analyzing phone records and Internet website data. Rayburn House Office Bldg., Room 2237. More information.

-June 24, 10:00 a.m. - 12:00 noon, **Black Code: Inside the Battle for Cyberspace** - The National Endowment for Democracy will host a panel discussion regarding the book by the same title. The speakers will be the author Ronald Deibert; Leslie Harris, president and CEO, Center for Democracy and Technology; and Harvey Rishikof, chair of the advisory committee, American Bar Association Standing Committee on Law and National Security, New America Foundation. NED, 8th Floor, 1025 F St., NW. More information.

-June 24, 2:00 p.m. - 3:30 p.m., **The Chinese Cyber Challenge: How to Address the Growing Threat** - The Brent Scowcroft Center of the Atlantic Council will host a panel discussion on the most recent claims of Chinese cyber espionage and the implications of this threat for the US-China relationship and China's ties with its neighbors in Asia. Speakers will include Dmitri Alperovitch, co-founder and CTO, CrowdStrike, Inc.; James Mulvenon, vice president, intelligence division Director, Center for Intelligence Research and Analysis, Defense Group, Inc; Gregory J. Rattray, CEO and Founding Partner, Delta Risk LLC. The Army and Navy Club Ballroom, 901 17th St NW, 2nd floor. More information.

-June 25-26, 8:00 a.m. - 5:00 p.m., **CyberSci Summit 2013** - The goal of this technical gathering is to provide a venue for government, industry, and academia to discuss state-of-the-art and visionary developments spanning emerging technologies to meet the evolving requirements of security in cyberspace. Arlington Hilton Hotel, 950 North Stafford Street, Arlington, Va. More information.

-June 25-26, **Open Source Security Summit** - This year's Open Source Summit will explain how to build, engage with, and maintain open source communities. NYU, 1307 L St NW. More information.

-June 25-27, **Software Assurance Working Group Sessions, Summer 2013** - Co-sponsored by organizations in the U.S. Department of Homeland Security (DHS), U.S. Department of Defense (DoD), and U.S. National Institute for Standards and Technology (NIST), the DHS/DoD Software and Supply Chain Assurance Working Group Sessions provide venues for public-private interaction and collaboration on enhancing software security and focus on software security-related advances in practices, products, and standards for software development, acquisition, supply chain management, education and training, tools, and measurement in order to reduce risk. MITRE, 7525 Colshire Drive, McLean, VA, 22102. More information.

Legislative Lowdown

-With last week's revelations that the National Security Agency was collecting data on millions of phone calls made through Verizon and also running an Internet surveillance program that targets foreign nationals via major online corporations, it appears inevitable that the issue of electronic privacy -- already a hot topic in 2012 -- will vault to near the top of the lobbying charts in 2013, according to a blog post by the Center for Responsive Politics.

-A bi-partisan group of senators proposed legislation last week that seeks to declassify certain rulings from the Foreign Intelligence Surveillance Court, after a leak revealed that the secretive court has been ordering phone companies to turn over calling records on millions of customers, Wired.com writes. The FISC came to life in the wake of the Watergate scandal under the President Richard M. Nixon administration. It approved all of the 1,856 government surveillance requests last year. The legislation would require the Justice Department to declassify the court's interpretations of the law, specifically the Foreign Intelligence Surveillance Act and the Patriot Act. The lawmakers, however, say the sources and methods of data-collection could remain secret.

Cyber Security Policy News

-As Google and other large tech companies cope with the aftermath of recent reports that the National Security Agency has had broad access to their users' data, the search giant is asking the U.S. government for permission to publish the number of national security requests it receives, including those made under the Foreign Intelligence Surveillance Act, NPR reports. In a letter to the head of the Justice Department and the FBI, Google's chief legal officer, David Drummond, said that government nondisclosure obligations are keeping the company from being able to ease public concerns about the privacy and security of users' data.

Brought before lawmakers to explain the NSA's domestic surveillance program, NSA chief Keith Alexander testified before the Senate appropriations committee that maintaining a database of millions of Americans' phone records was critical to thwarting "dozens" of plots, writes The Guardian. One of the examples Alexander mentioned, the case of would-be New York subway bomber Najibullah Zazi, appears to have been prevented by conventional police surveillance, including efforts by UK investigators. For their part, Sens. Ron Wyden (D-Ore.) and Mark Udall (D-Colo.) said they were not convinced. "Gen Alexander's testimony yesterday suggested that the NSA's bulk phone records collection program helped thwart 'dozens' of terrorist attacks, but all of the plots that he mentioned appear to have been identified using other collection methods," Wyden and Udall said in a statement. "The public deserves a clear explanation." Alexander testified that the efficacy of the phone-records program could not be independently analyzed from that of another NSA program disclosed by the Guardian, an effort called Prism that monitors the internet communications of people believed to be outside the US. In an interview with the Guardian, Wyden challenged that assertion as well.

The EU's Justice Commissioner has written to the US attorney general, questioning him about America's data surveillance program, Prism. The BBC reports that Viviane Reding wrote that she was concerned America's efforts "could have grave adverse consequences for the fundamental rights of EU citizens". The story notes that European data protection laws put restrictions on how data gathered about people, including social networking data, can be used, and that companies which helped the government gather this data will now face serious questions from national data commissioners and even potentially from individual users in Europe over whether they followed all the European data protection laws that are supposed to stop things like this happening."

-Security researchers Billy Rios and Terry McCorkle of Cylance have reported a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors, warns the U.S. Department of Homeland Security's US-CERT. According to their report, the vulnerability could be exploited to potentially change critical settings and/or modify device firmware. "Because of the critical and unique status that medical devices occupy, ICS-CERT has been working in close cooperation with the Food and Drug Administration (FDA) in addressing these issues," DHS warned last week. "ICS-CERT and the FDA have notified the affected vendors of the report and have asked the vendors to confirm the vulnerability and identify specific mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks. ICS-CERT and the FDA will follow up with specific advisories and information as appropriate."

The warning comes as the FDA is calling on medical device makers to take new steps to protect their products from malware and cyber attacks or face the possibility that it won't approve their devices for use. Computerworld writes that The FDA issued new cybersecurity recommendations for medical devices on Thursday, following reports that some devices have been compromised. Recent vulnerabilities involving Philips fetal monitors and in Oracle software used in body fluid analysis machines are among the incidents that prompted the FDA to issue the recommendations, an FDA spokeswoman said. In one case reported in October, malware slowed down fetal monitors used on women with high-risk pregnancies at a Boston hospital. In another case, the FDA in January issued a warning about Oracle software that could allow remote access to the databases of Roche Cobra analysis devices, she said.

-The first cyber protection platoon was assigned at the Defense Information Systems Agency (DISA) last week. According to DISA, the mission of the platoon is to provide enhanced defensive cyber capabilities to enable the agency to operate and maneuver more securely through the cyber domain in support of our mission partners. This platoon, which will reach operational capability in the October-December timeframe, is the first of six platoons to be created at DISA from now through fiscal year 2016.

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.