GW CSPRI Newsletter

April 1, 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. To change your subscription settings, please email cspriaa@gwu.edu with your request.

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

-Apr. 2, 12 noon, **Travel Surveillance, Traveler Intrusion** - The United States government practices surprisingly comprehensive surveillance of air travel, amassing data about the comings and goings of all Americans who fly. The Court of Appeals for the D.C. Circuit has ordered the Transportation Security Administration to begin a public comment process on its imaging machines by April 2. Speakers will include Edward Hasbrouck, journalist, consultant, The Identity Project (PapersPlease.org) and author of the book and blog, The Practical Nomad; and Ginger McCall, director, Open Government Program, Electronic Privacy Information Center. This event includes a luncheon to follow, and will be Webcast. Cato Institute, 1000 Massachusetts Ave, NW. More information.

-Apr. 2, 6:00 p.m. - 9:00 p.m., **Defending Against Cyber-Intrusions from Both State-Sponsored and Civilian Hackers** - The DC Bar Association will host a reception and panel discussion. The speakers will include Michael Hayden, former NSA and CIA director, currently with the Chertoff Group; Ronald Lee, partner, Arnold & Porter, and former general counsel, National Security Agency; Suzanne Spaulding, deputy under secretary, DHS National Protection and Programs Directorate; and Steven Cash, founder of Deck Prism, and former chief counsel and staff director to the U.S. Senate's Subcommittee on Terrorism, Technology, and Homeland Security. Arnold & Porter, 555 12th St., NW. More information.

-Apr. 3, 12 noon - 1:30 p.m., **Is Privacy a Thing of the Past?** - The Constitution Project will host a panel discussion of the current debate surrounding efforts to reform the Electronic Communications Privacy Act (ECPA), the law that regulates government access to electronic communications. This panel discussion will provide a variety of perspectives on the issues before this Congress as it considers legislation designed to bring ECPA into the 21st century. Lunch will be served. Google Washington D.C., 1101 New York Avenue, NW, Second Floor. More information.

-Apr. 4, 1:00 p.m. - 5:00 p.m., **Mobile Application and Transparency** - The National Telecommunications and Information Administration will hold another in its series on mobile application transparency. The goal of this process is to develop a code of conduct to provide transparency in how companies providing applications and interactive services for mobile devices handle personal data. This event will also be teleconferenced. American Institute of Architects, 1735 New York Ave., NW. More information.

-Apr. 4, 4:30 p.m. - 6:30 p.m., **The Challenges in Global Cyber Strategy** - The George Washington University Law School presents a talk by Vice Chairman of Booz Allen Hamilton, Admiral J. Michael "Mike" McConnell, former director of the National Security Agency under Presidents George H.W. Bush and Bill Clinton. George Washington University, Jacob Burns Moot Court Room, Lerner Hall, 1st Floor, 2000 H Street, NW. More information.

-Apr. 8, 5:30 p.m. - 8:30 p.m., **NoVA Hackers Association Meetup** - This informal group of security professionals from around the NoVA/DC area coordinates one or two monthly events – an evening meetup with presentations on the second Monday of the month and various lunch or bar meetups. QinetiQ, 11091 Sunset Hills Road, Reston, VA, 20190. More information.

-Apr. 10, 8:00 a.m. - 6:00 p.m., **Developing International Norms for a Safe, Stable & Predictable Cyber Environment** - The Atlantic Council and Georgetown University's Institute for Law, Science and Global Security are hosting the third annual International Engagement on Cyber conference. This gathering aims to promote dialogue among policymakers, academics, and key industry stakeholders from across the globe, and explores the worldwide community's increasing interconnectivity in this domain. The 2013 keynote speakers will be Ronald K. Noble, Secretary General of INTERPOL, Terry D. Kramer, Ambassador, Head of the US Delegation for the World Conference on International Telecommunications, Dubai, Michael Daniel, Cybersecurity Coordinator, The White House, Eugene Kaspersky, CEO and Co-founder, Kaspersky Lab, and Teresa M. Takai, Chief Information Officer, U.S. Department of Defense. Georgetown University, Healy Building (Gaston Hall), 3700 O Street NW. Registration. More information.

-Apr. 10, 1:00 p.m., **Lessons Learned from Recent Cyber Breach Investigations** - The FS-ISAC and PwC will host a complimentary Webcast to discuss the newest and most common threat vectors from recent breach investigations. The speakers will highlight how the attacks are carried out, and focus on techniques to implement countermeasures for the current threat landscape. More information.

-Apr. 10-11, **NIST Improving Trust in Online Marketplace Workshop** - This workshop provides an opportunity for industry, research and academia communities, and government sectors, to review, promote and move toward consensus on emerging industry standards and guidelines and to learn about NIST's current cryptographic research, activities, programs and standards development. 100 Bureau Drive, Gaithersburg, MD, 20899. More information.

-Apr. 12, 8:00 a.m. - 1:00 p.m., **The Cyber 9/12 Project: Cyber Statecraft After Catastrophes** - The Atlantic Council and Science Applications International Corporation (SAIC) for the second scenario-driven, interactive conference to discuss the day-after response to a cyber incident. The goal of the conference is to encourage greater dialogue about the intricate decision-making process various sectors must face during a serious cyber conflict, and shine light on the need for greater conversation on how to respond to cyber security issues. The Knight Studio at the Newseum, 555 Pennsylvania Ave., NW. More information.

Legislative Lowdown

-Congress has taken the first step toward requiring companies to admit when their networks have been hacked, National Journal reports. The proposed rule on data breaches appears as part of a larger draft bill being circulated in the House Judiciary Committee. On top of raising the maximum penalty for computer crimes, the unnamed legislation gives businesses 14 days to disclose a security breach after they find out about it. In the case of a "major" breach, that window shrinks to a mere 72 hours, and involves the FBI or the Secret Service. Any firm that handles personal information will be subject to the rule, except those that work under HIPAA--the federal health privacy law--and some financial institutions.

-A proposed update to 1986 Computer Fraud and Abuse Act would, instead of fixing the current law's flaws, would enable prosecutors to threaten alleged violators with dramatically bigger penalties, argues an editorial in last week's The Los Angeles Times. The 27-year-old law makes it a crime to gain access to information on a computer in an unauthorized way — for example, by hacking through the passwords protecting a shopping website's server and copying the credit card numbers stored there. That prohibition applies to both people who aren't authorized to use the computer and to people who exceed the authority they were granted. The problem is that the act doesn't clearly define what it means by exceeding one's authorization. As a result, some prosecutors have argued — and some judges have agreed — that simply violating a site's terms of service is equivalent to gaining unauthorized access. The draft circulated by the Judiciary Committee's staff maintains the sorry status quo, affirming that those who violate terms of service to obtain information from a government website or "sensitive or nonpublic information" from any other site could be prosecuted. As CSPRI researcher and George Washington University Law Professor Orin Kerr has observed, “the language would make it a felony to lie about your age on an online dating profile if you intended to contact someone online and ask them personal questions.” Professor Kerr describes the proposed legislation here as “a step backward, not a step forward.”

Cyber Security Policy News

- A squabble between a group fighting spam and a Dutch company that hosts Web sites said to be sending spam has escalated into one of the largest computer attacks on the Internet, causing widespread congestion and jamming crucial infrastructure around the world. The New York Times wrote that millions of ordinary Internet users have experienced delays in services or could not reach a particular Web site for a short time as a result of the attack, although few outside Internet measurement firms could independently confirm that claim. The attack was reportedly launched against anti-spam provider Spamhaus.org by activists upset over Spamhaus's recommendation to block Cyberbunker, a hosting company associated with anti-government groups and located in a former NATO bunker.

-Citing cyber-security concerns, Japan-based corporation Softbank has agreed with US officials to phase out and replace telecommunications equipment manufactured by Chinese companies with close ties to Beijing. The agreement would allow national security officials to monitor changes to the company's system of routers, servers and switches, among other equipment and processes, the officials said. It would also let them keep a close watch on the extent to which Sprint and SoftBank use equipment from Chinese manufacturers, particularly Huawei Technologies.

The move came the same week revelations that a funding bill signed by President Barack Obama included provisions requiring that U.S. government technology purchases first go through a cyber-espionage review process. Experts say the could potentially impact the sales of Chinese tech companies like Lenovo, which relies on sales to U.S. government agencies and schools as an important part of its North American growth strategy. As TechCrunch reports, the provision came to attention via a blog post by lawyer Stewart A. Baker, a former Assistant Secretary in the U.S. Department of Homeland Security under George W. Bush. Baker wrote that the sanctions "[demonstrate] remarkable bipartisan angst about Chinese hacking and the risks in Chinese high tech equipment." The law means that NASA, the National Science Federation, and the Justice and Commerce Departments, need to get approval from federal law enforcement officials before buying information technology systems in order to assess "cyber-espionage or sabotage" risk. In particular, federal law officials must first assess "any risk associated with such system being produced, manufactured or assembled by one or more entities that are owned, directed or subsidized" by China.

Meanwhile, two top Democrats urged the Obama administration on Thursday to take action against China for allegedly engaging in the cybertheft of U.S. intellectual property and other trade secrets. The Hill reports that the House Ways and Means Committee ranking member Sander Levin (D-Mich.) and Trade Subcommittee ranking member Charles Rangel (D-N.Y.) are pressing for U.S. Trade Representative (USTR) Demetrios Marantis to consider designating China as a "priority foreign country" as evidence mounts that Beijing is involved in "egregious conduct" that is hurting U.S business and likely violates World Trade Organization (WTO) rules, in a letter sent on Thursday.

-The much-derided decision by Google to kill off its popular Google Reader Web app for perusing RSS feeds was in part motivated by Google's desire to save itself from additional consumer privacy hurdles associated with the app and its new privacy policies, according to The Wall Street Journal's All Things D blog. "Google is also trying to better orient itself so that it stops getting into trouble with repeated missteps around compliance issues, particularly privacy," AllThings's Liz Gannes wrote. "That means every team needs to have people dedicated to dealing with these compliance and privacy issues — lawyers, policy experts, etc. Google didn't even have a product manager or full-time engineer responsible for Reader when it was killed, so the company didn't want to add in the additional infrastructure and staff, the sources said."

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.