GW CSPRI Newsletter

July 15, 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

-July 15, 6:00 p.m. - 8:00 p.m., **Techno-Activism Third Mondays** - The New America Foundation will host an event. The speakers will be Sacha Meinrath, vice president and director, Open Technology Institute, New America Foundation; and Thomas Gideon, technology director, Open Technology Institute, New America Foundation. The event is designed to connect software creators and activists who are interested in censorship, surveillance, and open technology. NAF, Suite 400, 1899 L St., NW. More information.

-July 16, 12 noon - 1:00 p.m., **The Growing Importance of Trade Secrets** - The D.C. Bar Intellectual Property Law Section will present a luncheon program which will explore the policies in place for using trade secrets to protect intellectual property values. Faculty experts Walter D. Davis Jr. of Axinn, Veltrop & Harkrider LLP and Jia Lu of Finnegan, Henderson, Farabow, Garrett & Dunner, LLP will highlight some of the most relevant policy changes and recent court decisions and provide participants with vital information to make better decisions about using trade secrets to protect intellectual property. D.C. Bar Conference Center, 1101 K Street NW, first floor. More information.

-July 16, 2:00 p.m. - 3:30 p.m., **Safeguarding Human Rights in Times of Surveillance** - U.N. Special Rapporteur Frank la Rue offers a view on privacy and freedom of expression, setting global standards for international behavior. Speakers include Frank La Rue, special rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations' Sascha Meinrath, director, Open Technology Institute and vice president, New America Foundation; and Gene Kimmelman, internet freedom and human rights program, New America Foundation. 1899 L St. NW Suite 400. More information.

-July 16, 6:30 p.m. - 8:00 p.m., **ISSA DC Meetup** - Through its meetings and other events, the chapter fosters professional development and support for computer and information security professionals. Membership is open to practicing security professionals or to those with an interest in the profession. New members are always welcome — please feel free to attend one of our open meetings or to contact the chapter for more information. Center for American Progress, 1333 H Street, NW. More information.

-July 16, 7:00 p.m., **Achieving Success as a Woman in Cybersecurity** - A panel discussion of successful women in cybersecurity, covering topics that women looking to enter or advance in their career would benefit from. Will have time for Q&A, networking, and resume reviews. Teqcorner, 1616 Anderson Rd, 3rd Fl, McLean, VA 22102. More information.

-July 17, 9:30 a.m., **Evaluating Privacy, Security, and Fraud Concerns with ObamaCare's Information Sharing Apparatus** - The House Homeland Security Committee's Subcommittee on Cybersecurity and the House Oversight and Government Reform Committee's Subcommittee on Energy Policy, Health Care and Entitlements will hold a joint hearing. Cannon House Office Bldg., Room 211. http://judiciary.house.gov/hearings/113th/hear_07172013.html">More information.

-July 17 10:00 a.m., **Oversight of the Administration's use of FISA Authorities** - The House Judiciary Committee (HJC) will hold a hearing. Rayburn House Office Bldg., Room 2141. More information.

-July 17, 1:00 p.m., **Communicating Cyber Risks to Business Leaders** - In this Webcast, the Financial Services Information Sharing and Analysis Center (FS-ISAC) and Booz Allen Hamilton executive vice president Thomas Sanzone and principal Sedar Labarre will discuss how CISOs can communicate with their business leaders when it comes to investing in cyber risk solutions. More information.

-July 18, 10:00 a.m., **Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?** - The House Commerce Committee's Subcommittee on Commerce, Manufacturing and Trade will hold a hearing. Rayburn House Office Bldg., Room 2123. More information.

-July 18, 10:00 a.m., **Oversight of Executive Order 13636 and Development of the Cybersecurity Framework** - The House Homeland Security Committee's Subcommittee on Cybersecurity will hold a hearing. Cannon House Office Bldg., Room 311. More information.

- July 18, 12 noon to 1 p.m., **Cyberwar, Without the Magical Thinking** - In this free Webcast event, attorney Stewart Baker from Steptoe & Johnson will discuss ongoing improvements in attribution and that "we have a growing ability to identify and eventually to deter attackers by exploiting their inevitable security errors." Stewart maintains that identifying and punishing intruders must be a major part of any cyberwar or cyberespionage technological strategy. Secure systems, he argues, should seek not so much to lock out attackers as to force them to make such heavy investments that they put at risk their own anonymity and their own networks: That means more digital dyepacks and network mantraps, he asserts, not stronger network walls. National Science Foundation, Stafford I Room 110, 4201 Wilson Boulevard, Arlington, VA. More information.

-July 18, 3:30 p.m. - 5:00 p.m., **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012** - Frank Cilluffo, director of The George Washington University's Homeland Security Policy Institute, will moderate a discussion with Jason Healey, director of the Cyber Statecraft Initiative at the Atlantic Council, to explore the findings in this first book on the history of cyber conflict. The George Washington University, The Alumni House, 1918 F St., NW. More information.

-July 24 2:00 – 6:00 p.m., **INET Washington D.C.** The INET Washington is organizing a discussion on "Surveillance, Cybersecurity, and the Future of the Internet" with leading experts as they tackle the complex implications of the US Government surveillance programs. This half-day event will feature experts on Internet privacy, security, and governance. Panelists include: Leslie Harris, CEO, Center for Democracy and Technology, Laura DeNardis, American University School of Communications , John Curran, CEO, ARIN , Melissa Hathaway, Hathaway Global Strategies, Randy Marchany, IT Security Officer, Virginia Tech, Lynn St. Amour, CEO, Internet Society and Danny Weitzner, MIT Computer Science and Artificial Intelligence Lab The moderator will be: Steve Roberts, Shapiro Professor of Media & Public Affiars – GWU; columnist; TV and radio analyst. More information.

Legislative Lowdown

-While President Obama was busy shooting down the House Intelligence Committee's cybersecurity bill for the second year in a row, the Senate was quietly working on a bill of its own. After months of talks, a draft of the legislation has finally come out—and it looks nothing like the much-reviled House version, The National Journal's Brian Fung reports. The 25-page document circulated by Senate Commerce Committee Chairman Jay Rockefeller, D-W.Va., details a handful of things, but overall the measure is uncontroversial and unambitious, Fung says. It formally codifies a project by the National Institute of Standards and Technology to draw up voluntary guidelines for businesses. It calls for a national research program to study the country's electronic vulnerabilities, and for the development of secure ways of dealing with them, and it proposes a nationwide public-awareness campaign to teach Americans about cybersecurity.

Cyber Security Policy News

-The Guardian has published part 2 of its June 6 interview with NSA whistleblower/leaker Edward Snowden, during which he matter-of-factly states that U.S. tech giants provide the National Security Agency (NSA) with "direct access" to their servers for purposes of bulk collection of data, Business Insider writes. The Guardian and Washington Post, to whom Snowden gave 41 NSA PRISM slides, both published articles and several slides which quote the presentation's statement regarding "collection directly from the servers" of nine Internet companies including Google, Facebook, Apple, and Microsoft." The companies vociferously denied the claims, and the Washington Post subsequently qualified its story by adding "according to a top-secret document obtained by The Washington Post" to the first sentence.

As Reuters notes, the latest bombshells focused in part on the alleged role of Microsoft in helping the NSA intercept users' communications. Citing top-secret documents provided by former U.S. spy contractor Edward Snowden, the UK newspaper said Microsoft worked with the Federal Bureau of Investigations and the NSA to ease access via Prism - an intelligence-gathering program uncovered by the Guardian last month - to cloud storage service SkyDrive. Microsoft also helped the Prism program collect video and audio of conversations conducted via Skype, Microsoft's online chat service, the newspaper added. Microsoft had previously said it did not provide the NSA direct access to users' information. On Thursday, it repeated that it provides customer data only in response to lawful government requests.

Meanwhile, Yahoo is continuing its fight to show that it was not involved in handing over consumer information to the National Security Agency's PRISM surveillance program. CBSNews reports that the company has petitioned a court to unseal documents from a classified 2008 case, which apparently shows that Yahoo "objected strenuously" to providing the government with customer data, reports the Mercury News.

Snowden emerged from seclusion Friday to say he wants political asylum in Russia until he can find a safe way to reach the Latin American countries offering to harbor him. According to The Wall Street Journal Snowden's plea to enter Russia after nearly three weeks in the Moscow airport's transit zone reflects his narrowing options after the U.S. withdrew his passport, pressured countries to reject his asylum requests and made efforts to prevent him from reaching those nations willing to take him.

The European Parliament Civil Liberties Commission voted overwhelmingly to investigate the privacy and civil rights implications of the NSA's PRISM and other spy programs on European citizens, and demanded more information on the programs from U.S. authorities, ComputerWorld writes. In a resolution, the Parliament called on member nations to also consider suspending any counter-terrorism related data transfer arrangements -- such as airline passenger records -- they might have with the U.S. until better protections become available for the data. Meanwhile, in a separate development, the Washington-based rights group Electronic Privacy Information Center (EPIC) filed a petition with the U.S. Supreme Court challenging the legal basis that the NSA is using to collect the phone records of tens of millions of Americans.

-Several models of Emergency Alert System decoders, used to break into TV and radio broadcasts to announce public safety warnings, have vulnerabilities that would allow hackers to hijack them and deliver fake messages to the public, Wired.com reports. The vulnerabilities

included a private root SSH key that was distributed in publicly available firmware images that would have allowed an attacker with SSH access to a device to log in with root privileges and issue fake alerts or disable the system. The researchers indicated that to resolve the issue would require “re-engineering” of the digital alerting system side as well as firmware updates pushed out to appliances in the field. But a spokesman for Monroe Electronics, owner of the company that makes the DASDEC devices, says that the company stopped shipping the vulnerable systems in February and began issuing a firmware patch in April that eliminates the SSH key issue. Earlier this year hackers used default credentials to break into the Emergency Alert System at local TV station KRTV in Montana to interrupt programming with an alert about a zombie apocalypse. Similar attacks also reportedly hit stations in Michigan, New Mexico, Utah and California. The hackers targeted local systems, however, not the national EAS network.

-The IRS mistakenly posted the Social Security numbers of tens of thousands of Americans on a government website, the agency confirmed last week. The numbers were posted to an IRS database for tax-exempt political groups known as 527s and first discovered by the group Public.Resource.org. The California-based group said it learned of the "privacy breach" while working on an unrelated audit of an “improperly vetted shipment” of IRS data on DVDs and promptly informed the agency, which shut down the site the next day. The group said the Social Security numbers were largely those of donors, though some were also from people who prepared tax returns to furnish to the IRS.

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.