GW CSPRI Newsletter

June 4, 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

-June 5-8, **Cloud Computing Forum & Workshop** - The National Institute of Standards and Technology (NIST) will host a three-day workshop. Department of Commerce, Hoover Bldg., 401 Constitution Ave., NW. More information.

-June 5, 7:00 a.m. - 10:30 a.m., **Biznow Cybersecurity Summit** - Speakers include Congressman Dan Lungren (R-Calif.); Greg Garcia, former assistant secretary for cybersecurity and communications, Department of Homeland Security; and Jody Westby founder & CEO, Global Cyber Risk. The Liaison Capitol Hill, 415 New Jersey Avenue, NW. More information.

-June 5, 1:00 p.m. - 2:00 p.m., **Privacy and Information Security Update** - The American Bar Association will host a webcast and teleconferenced panel discussion. The speakers will include Aryeh Friedman, chief privacy officer and compliance counsel, Dun & Bradstreet; Lisa Sotto, managing partner, Hunton & Williams; and Aaron Simpson, partner and privacy counsel, Hunton & Williams. More information (PDF).

June 5, 12:00 noon - 2:00 p.m. **What Role Should the UN Have in Governing the Internet? A Briefing on the UN's Internet Governance Initiative** - The Internet Caucus will host an event. The speakers will include Fiona Alexander, associate administrator, National Telecommunications and Information Administration NTIA); Richard Beaird, senior deputy U.S. coordinator, international communications and information policy, Department of State; David Gross, chair, international telecommunications group, Wiley Rein; Robert McDowell, commissioner, Federal Communications Commission; and Sally Wentworth, senior manager of public policy, Internet Society. This event is free and open to the public. Register by contacting rsvp@netcaucus.org, or calling 202-407-8829. Lunch will be served. Rayburn House Office Bldg., Room B-369.

-June 6, 8:00 a.m. - 2:30 p.m., **2012 Health Privacy Summit** - Over 40 leading health-privacy experts from around the globe will gather in Washington for the 2nd International Summit on the Future of Health Privacy to discuss the urgent privacy issues raised by emerging health technologies. Experts from the U.S. government, the private sector and academia will explore the new laws and regulations, data exchanges, secondary uses of health data and social media platforms that threaten the privacy of patients here and abroad. The summit also will examine new policies including the Consumer Bill of Privacy Rights and the EU Draft Regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Georgetown Law Center 600 New Jersey Ave NW. More information.

-June 6, 9:30 a.m. - 5:30 p.m., **AT&T Cyber Security Conference** - Although this event is being held at the New York Hilton, many of the sessions will be available via online webcast. Talks include discussions on DNSSEC, mobile security and advanced persistent threat (APT) attacks. More information.

-June 6-7, **Safeguarding Health Information: Building Assurance through HIPAA Security** - The National Institute of Standards and Technology (NIST) and the Department of Health and Human Services (HHS), Office for Civil Rights (OCR) are co-hosting the 5th annual conference. The conference will explore the current health information technology security landscape and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. This event will highlight the present state of health information security, and practical strategies, tips and techniques for implementing the HIPAA Security Rule. The Security Rule sets federal standards to protect the confidentiality, integrity and availability of electronic protected health information by requiring HIPAA covered entities and their business associates to implement and maintain administrative, physical and technical safeguards. Ronald Reagan Building and International Trade Center, 1300 Pennsylvania Avenue, NW. More information.

-June 7, 12 noon - 1:30 p.m., **HIPAA and HITECH Act Fundamentals: What You Need to Know Now About the Privacy and Security Rules** - The American Bar Association will host the meeting, which will be webcast. More information.

Legislative Lowdown

-A bipartisan group of lawmakers on the House Energy and Commerce Committee introduced a resolution on Wednesday urging the Obama administration to oppose efforts to give the United Nations more control over the Internet, The Hill reports. Proposals to give the UN's International Telecommunication Union (ITU) more control over the governance of the Internet could come up at a conference in Dubai in December. The move is backed by China, Russia, Brazil, India and other UN members, but is opposed by lawmakers on both sides of the aisle, as well as the Obama administration.

Cyber Security Policy News

-Most of the tech and security community last week was consumed with discussion of "Flame," one of the nicknames assigned to an extremely large and sophisticated piece of malware that appears to have been deployed as another cyber weapon against Iran. Wired's Kim Zetter writes that the malware Stuxnet in size — the groundbreaking infrastructure-sabotaging malware that is believed to have wreaked havoc on Iran's nuclear program in 2009 and 2010. Although Flame has both a different purpose and composition than Stuxnet, and appears to have been written by different programmers, its complexity, the geographic scope of its infections and its behavior indicate strongly that a nation-state is behind Flame, rather than common cyber-criminals — marking it as yet another tool in the growing arsenal of cyberweaponry.

Flame surfaced as the New York Times was getting ready to run an explosive story claiming that the Obama administration authorized the development and use of Stuxnet as a means of delaying Iran's nuclear ambitions. According to The Times's David E. Sanger, whose reporting relied entirely on anonymous sources, "Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet."

Meanwhile, Politico asks the question, can the president declare cyberwar without the authorization of Congress? Politico quotes Rep. Jim McDermott (D-Wash.) expressing strong misgivings about the president acting unilaterally. "When we see the results it's pretty clear they're doing it without anybody except a very few people knowing about it, much less having any impact on whether it's happening or not," McDermott said. The lawmaker said he was trouble because "we have given more and more power to the president, through the CIA, to carry out operations, and, frankly, if you go back in history, the reason we have problems with Iran is because the CIA brought about a coup."

-NextGov writes that U.K.-based security researchers have found a backdoor that was "deliberately" inserted into an American military chip to help attackers gain unauthorized access and reprogram its memory, according to a draft research paper. Sergei

Skorobogatov, a researcher at Cambridge University, discovered that a military-grade silicon device made by California-based Microsemi Corp., the ProASIC3 A3P250, contained a glitch that would allow individuals to remotely tweak its functions. The backdoor is said to be "close to impossible to fix on chips already deployed" because software patches can't fix the bugs. The security holes can only be removed by replacing all such chips installed in systems, the researchers said.

-A New Jersey mayor and his son were arrested last week by the FBI for allegedly hacking into an email account and website tied to a recall effort — and then intimidating those associated with the site. Politico reports that Felix Roque, 55, the Democratic mayor of West New York, N.J., and his son Joseph, 22, allegedly accessed and cancelled the domain registration for Recallroque.com, a website that was critical of the mayor and associated with a movement to recall him in early February. Joseph Roque learned how to hack email accounts at GoDaddy.com, a domain registration company, by searching the Internet, according to a criminal complaint unsealed after the arrests.

-The Obama administration held a public meeting at the White House last week to discuss industry and government efforts to combat botnet activity. Among those was a pilot program to share information about botnet victims between banks and Internet service providers, KrebsOnSecurity.com writes. Although a number of ISPs already notify customers of bot infections, there is no uniform method for reporting these events. Attendees at Wednesday's meeting are expected to announce — among other things — an information sharing pilot between ISPs and financial institutions that are part of the Financial Services Information Sharing and Analysis Center, an industry consortium dedicated to disseminating data on cyber threats facing banks. The pilot to be announced this week will draw on a nascent extension of IODEF, an Internet standard developed by the Anti-Phishing Working Group to share data about phishing attacks in a common format that can be processed automatically and across multiple languages.

-The Federal Communications Commission (FCC) is seeking comment from the public on how to protect the privacy of cellphone users. The FCC is soliciting comments regarding the privacy and data- security practices of mobile wireless service providers with respect to customer information stored on their users' mobile communications devices, and the application of existing privacy and security requirements to that information. In a public notice posted late last week, the FCC said that in the past few years, technological advancements have given wireless companies access to new personal information about their customers. "The devices consumers use to access mobile wireless networks have become more sophisticated and powerful, and their expanded capabilities have at times been used by wireless providers to collect information about particular customers' use of the network — sometimes, it appears, without informing the customer," the FCC wrote. A copy of the request for comments is available here (PDF).

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*.