GW CSPRI Newsletter

May 28, 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

-May 30 - June 1, **Open Meeting of the Information Security and Privacy Advisory Board** - The National Institute of Standards and Technology holds a three-day meeting. Panel discussion topics will include the Joint Cybersecurity Service Program; automated indicator sharing; privacy research; and SEC security breach notification regulations. Heritage Room, Administration Building, at the National Institute of Standards Technology (NIST), 100, Bureau Drive, Gaithersburg, Maryland. More information.

-May 30, 8:30 a.m., **Building Cybersecurity Partnerships and Promoting Voluntary Action: Stopping Botnets** - White House Cybersecurity Coordinator Howard Schmidt will host an event with industry leaders, consumer advocates and US government officials to announce new and revitalized efforts to address one of the biggest risks to Internet security: botnets. This event will be Webcast.

-May 31, 7:30 a.m. - 12 noon, **Why an Effective Identity Ecosystem is Essential** - This conference will cover current initiatives to strengthen identity proofing for trusted government, business, and individual online communications and transactions, as well as how organizations large and small can protect their intellectual property, employee privacy, and sensitive business

information. Other topics of discussion including trends in identity theft, data breaches, and how to defend against them. Speakers include Jeremy Grant, senior executive advisor for identity management, National Institute of Standards and Technology, Department of Commerce; and Gregory Wilshusen, director of information security issues, U.S. Government Accountability Office. The Willard InterContinental Hotel, 1401 Pennsylvania Avenue NW. More information.

-May 31, 10:15 a.m., **International Proposals to Regulate the Internet** - The Subcommittee on Communications and Technology has scheduled a hearing on efforts to give the United Nations more control over the Internet. Room 2322, Rayburn House Office Bldg. More information.

-May 31, 8:30 a.m. - 4:00 p.m., **Cyber Security Conference & Expo** - The Digital Government Institute's 5th annual Cyber Security Conference, which is free for government professionals to attend, will explore today's cyber threats and offer an opportunity for those supporting government security initiatives to collaborate on how to detect, protect, and respond to these challenges. Ronald Reagan Building, The Pavilion Room, 1300 Pennsylvania Ave., NW. More information.

-June 1, 9:30 a.m., **Cyber Threats to Capital Markets and Corporate Accounts** - The House Committee on Financial Services will hold a hearing. 2128 Rayburn House Office Bldg. More information.

-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 6-7, **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.

Legislative Lowdown

-Last week, Rep. Blaine Luetkemeyer (R-MO) introduced legislation (H.R. 5817) to limit the obligations of certain financial institutions to provide an annual privacy notice to consumers, according to an analysis at InsidePrivacy. Under the Gramm-Leach-Bliley Act (GLBA), financial institutions must provide customers an initial privacy notice and, for the duration of a customer relationship, an annual privacy notice that describes the company's information-sharing practices. While anything is possible in Washington, particularly in a Presidential election year, the expectation is that this bill is unlikely to progress to enactment. Under H.R. 5817, a financial institution would not be obligated to provide customers with an annual privacy notice so long as the company shares information only in certain limited respects (that are more narrow than those permitted under federal law) and provided that the company has not changed its privacy policies or practices from those disclosed in its most recent privacy notice.

-Lawmakers in Congress are calling on the Justice Department to reopen an investigation into Google for possible privacy violations, Computerworld reports. Representatives Frank Pallone Jr., a New Jersey Democrat, and John Barrow, a Georgia Democrat, called on the DOJ to fully investigate Google's actions for potential violations of federal wiretapping laws. In light of a recently released U.S. Federal Communications Commission report on Wi-Fi snooping by Google Street View cars, the DOJ should take a new look at the company's actions, wrote the lawmakers, in a Thursday letter to U.S. Attorney General Eric Holder.

Cyber Security Policy News

-The FBI has recently formed a secretive surveillance unit with an ambitious goal: to invent technology that will let police more readily eavesdrop on Internet and wireless communications, according to CNet's Declan McCullagh. The establishment of the Quantico, Va.-based unit, which is also staffed by agents from the U.S. Marshals Service and the Drug Enforcement Agency, is a response to technological developments that FBI officials believe outpace law enforcement's ability to listen in on private communications.

-The Obama Administration, acknowledging the explosion in mobile technology, has unveiled a "digital government" strategy that requires every federal agency to make at least two services available to the public via mobile applications within a year. GovInfoSecurity notes that the strategy emphasizes the importance of addressing privacy issues as the government takes greater advantage of the latest advances in information technology. For example, it calls for standardized implementation of privacy controls.

-One or more unauthorized users gained access to the inner workings of a website run by the U.S. Justice Department, a department spokeswoman acknowledged last week after the hacker group Anonymous said they were behind the incident. The hackers accessed a server that operates the Bureau of Justice Statistics' website, Reuters reports. The bureau is responsible for collecting and analyzing data about crime - including computer security incidents - from throughout the United States.

Meanwhile, a sophisticated cyberattack on the computer of a third-party Thrift Savings Plan contractor has compromised the personal information of tens of thousands of TSP participants. NextGov's Amanda Palleschi writes that the Federal Retirement Thrift Investment Board and Serco Inc., a contractor that provides services to the TSP, learned in April of a July 2011 attack on a Serco computer. The FBI told Serco and the board that the incident led to “unauthorized access” to accounts of as many as 123,000 TSP participants and other recipients of TSP payments. The TSP is a 401(k)-style investment program for federal employees.

-Proposed legislation in both chambers would require New York-based websites, such as blogs and newspapers, to "remove any comments posted on his or her website by an anonymous poster unless such anonymous poster agrees to attach his or her name to the post," according to Wired.com. Republican Assemblyman Jim Conte said the legislation would cut down on "mean-spirited and baseless political attacks" and "turns the spotlight on cyberbullies by forcing them to reveal their identity," but civil liberties groups say the proposal would essentially destroy the ability to speak anonymously online on sites in New York.

-The White House has selected the head of the intelligence branch in its budget office to be President Barack Obama's top adviser on cybersecurity issues, a move that comes as Congress and the Obama administration are at odds over how best to protect critical U.S. industries from crippling electronic attacks by cybercriminals, foreign governments and terrorists, the Associated Press reports. Michael Daniel, a 17-year veteran of the Office of Management and Budget's national security division, will replace Howard Schmidt as Obama's cybersecurity coordinator, the White House announced Thursday. Schmidt, who was appointed by Obama in December 2009, is retiring and returning to private life, according to the announcement. Before his White House appointment, Schmidt had worked as chief information security officer at eBay and chief security officer at Microsoft. But as Taylor Armerding writes for Information Week, Daniel is a relative unknown to many experts in the security industry.

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.