GW CSPRI Newsletter

February 6, 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

-Feb. 8-10, **2nd Annual Advanced ITAR Compliance** - This event will provide an analysis of new regulations resulting from the implementation of the US Export Reform Initiative. Speakers from Northrop Grumman Corp., BAE Systems, and General Dynamics. Westin Alexandria,400 Courthouse Square, Alexandria, Va. More information.

*-CSPRI EVENT: Feb. 15, 12 noon - 2:00 p.m., **The End of K Street Deals?: Is Netizen Direct Lobbying the New Norm?** - Panelists include Susan Aaronson, Associate Research Professor at GW's Elliott School of International Affairs; Dean C. Garfield, President and CEO of the Information Technology Industry Council; Michael Nelson, Research Associate for the CSC Leading Edge Forum and Visiting Professor of Internet Studies at Georgetown University; Mitch Glazier, Senior Executive Vice President, Recording Industry Association of America. Lance Hoffman, Director, Cyber Security Policy and Research Institute, will facilitate the discussion. Sign up for seminar and the following lunch (provided by CSPRI) at http://netizenlobbying.eventbrite.com.*

-Feb. 15, 7:30 a.m. - 11:25 a.m., **Secure Cyber Operations Start Here: Who Are You and How Can I Be Sure?** - Speakers from the Department of Defense, Health and Human Services and a number of private companies address how they are proceeding to support secure, scalable identity protection and management systems for government enterprises. The Willard InterContinental Hotel, 1401 Pennsylvania Ave NW. More information.

Announcements

The Systems & Security Group at The George Washington University Computer Science Department is looking for scholars with a desire to advance the field of computer security. It has funded PhD and postdoctoral positions available starting in Fall 2012. The successful applicant will work with Prof. Michael Clarkson and the large cybersecurity community in DC to advance the state of the art in the scientific foundations of computer security. Click here for more information.

Legislative Lowdown

-A comprehensive cybersecurity bill (PDF) passed a major hurdle in the House. It was voted through the House Homeland Security Subcommittee after series of markups. The bill is sponsored by California Congressman Dan Lungren. It mirrors the Senate version by protecting critical infrastructure, expanding the role of the Homeland Security Department and sharing threat data with the private sector.

-Bolstered by the successful campaign against online piracy legislation, an advocacy group is hoping to derail another bill from House Judiciary chairman Lamar Smith (R-Texas) aimed at combating child pornography. The Hill writes that an online protest against H.R. 1981, the Protecting Children From Internet Pornographers Act, by Demand Progress has resulted in roughly 75,000 emails to lawmakers, opposing what the group has termed an "Internet snooping bill." Privacy advocates have raised concerns about the H.R. 1981 when it passed Committee last summer, arguing it would increase the incentive for hackers to attack Internet service providers. The bill would force ISPs to retain data on which IP addresses were used by consumers for up to 18 months.

-The House Committee on Science and Technology is expected to meet at 10 a.m. on Tuesday, Feb. 7 to consider H.R. 3834, the "Advancing America's Networking and Information Technology Research and Development Act of 2012." 2318 Rayburn House Office Building.

Cyber Security Policy News

-Information gleaned from public filings to the Securities and Exchange Commission indicate that at least a half-dozen major U.S. companies whose computers have been infiltrated by cyber criminals or international spies have not admitted to the incidents despite new guidance from securities regulators urging such disclosures. A review from Reuters found that more than 2,000

filings since the SEC guidance indicated that some companies, including Internet infrastructure company VeriSign and credit card and debit card transaction processor VeriFone Systems, revealed significant new information about hacking incidents. Verisign declined to offer additional details about the stated breach, leading some security experts to question whether the company may have had a breach that endangered its most sensitive business - the issuance of Secure Sockets Layer (SSL) certificates that protect the communications between its customers and their customers.

-FBI Director Robert Mueller told Congress last week that threats from cyber-espionage, computer crime, and attacks on critical infrastructure will surpass terrorism as the number one threat facing the United States. Mueller and National Intelligence Director James Clapper, addressing the annual Worldwide Threat hearing before the Senate Select Committee on Intelligence, cited their concerns about cyber-security and noted that China and Russia run robust intrusion operations against key U.S. industries and the government, ABC News reports.

Addressing leaders on Capitol Hill, Clapper said he and all of the U.S. intelligence leadership agree the United States is in a type of cyber Cold War, losing some $300 billion annually to cyber-based corporate espionage, and sustaining daily intrusions against public systems controlling everything from major defense weapons systems and public air traffic to electricity and banking.

-Activists allegedly allied with the hacking group "Anonymous" appear to have eavesdropped on a conference call between the FBI and foreign law enforcement authorities aimed at corralling the group. The Associated Press reports that hackers allied with group sat in on a call between investigators from the FBI and Scotland Yard that was intended to collate information about suspected members of the group that have claimed responsibility for a string of embarrassing attacks across the Internet. Anonymous published the roughly 15-minute-long recording of the call on the Internet on Friday, gloating in a Twitter message that "the FBI might be curious how we're able to continuously read their internal comms for some time now."

-As of March 1, 2012, all companies storing the personal information of Massachusetts residents with a third-party service provider must contractually require the service provider to maintain data security measures “consistent” with the Massachusetts data security regulations, according to InsidePrivacy.com. Among other things, those regulations—most of which took effect in March 2010— require companies to implement a written information security program containing certain elements, including a requirement that personal information be encrypted when transmitted wirelessly or across public networks, and when stored on portable computing devices (including laptops). The regulations also require companies to take “reasonable steps” when selecting a service provider to ensure that the provider is capable of maintaining appropriate measures for the protection of personal information.

-Leading privacy officials in Europe have asked Google "for a pause" in the company's planned consolidation of user data "in the interests of ensuring that there can be no misunderstanding about Google's commitments to the information rights of their users and EU citizens," according to the Electronic Privacy Information Center (EPIC). EU Commissioner Vivian Reding has expressed support, tweeting "Good that Europe's data protection authorities are ensuring

@Google's new privacy policy complies with EU law." EPIC has urged the United States to begin the process of ratification of Council of Europe Privacy Convention, which would establish global standards for privacy protection. The move comes as Google is backing off a recent privacy policy change, saying the changes would not apply to US federal agencies.

-The Federal Deposit Insurance Corporation (FDIC) has issued additional guidance for banks and financial institutions warning that certain third-party payment processors could prove to be security liabilities. In its revised guidance for payment processor relationships, the FDIC says certain deposit accounts with payment processors pose unusual risks, writes GovInfoSecurity. "Payment processors that deal with telemarketing and online merchants may have a higher risk profile because such entities have tended to display a higher incidence of consumer fraud or potentially illegal activities than some other businesses," the guidance states. "Financial institutions should understand, verify, and monitor the activities and the entities related to the account relationship."

-More than two months after authorities in the United States and abroad shut down a massive Internet traffic hijacking scheme, the malicious software that powered the criminal network is still running on computers at half of the Fortune 500 companies, and on PCs at nearly 50 percent of all federal government agencies. The malware, known as the "DNSChanger Trojan," quietly alters the host computer's Internet settings to hijack search results and to block victims from visiting security sites that might help scrub the infections. Internet Identity, a Tacoma, Wash. company that sells security services, found evidence of at least one DNSChanger infection in computers at half of all Fortune 500 firms, and 27 out of 55 major government entities.

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.