THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE
Thoughtful Analysis of Cyber Security Issues

GW CSPRI Newsletter

October 24, 2011

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

Upcoming Events

-Oct. 25, 11:00 a.m. - 12:30 p.m. ET, **A Discussion of Online Privacy** - Speakers include Erin Egan, director of privacy, Facebook; Mark Rasch, director of cybersecurity and privacy consulting, CSC; and Stephen Balkam founder and CEO of the Family Online Safety Institute. Ogilvy Washington Headquarters, 1111 19th St. NW, 10th Floor. More information.

-Oct. 25, 2:00 p.m. - 3:00 p.m., **Lessons from a National Intelligence Agency's Private Cloud: Realizing Cost Savings while Achieving Operational Excellence** - In a climate of numerous technologies, providers, security concerns, and budget restrictions, how can an agency realize the benefits of the cloud while successfully navigating its challenges? This Webcast aims to provide answers. Speakers to include Ira 'Gus' Hunt, chief technology officer, CIA; Robert Shelton,

CTO/advisor, National Security Group, Microsoft Federal; and Jeffrey Lush, CTO, Dell Services Federal Government. More information.

-Oct. 25, 8:30 a.m. - 12:30 p.m., **Google IT Summit** - This conference, put on by Google and the Cloud Sherpas, includes a special presentation about the Google Apps platform. Among the topics to be covered are how Google manages security and privacy best practices for deploying Google Apps. Crystal City Marriott, 1999 Jefferson Davis Hwy., Arlington, Va. More information.

-Oct. 25-26, **Security Innovation Network Showcase** - Supported by the Department of Homeland Security Science & Technology Directorate, the SINET Showcase 2011 is designed to showcase innovative technologies in the cybersecurity domain. Speakers include Keith Alexander, commander of the U.S. Cyber Command; Robert Bigman, information assurance group, Central Intelligence Agency; Earl Crane, director of cybersecurity strategy, Department of Homeland Security Office of the Chief Information Officer. National Press Club, 529 14th Street, N.W., 13th Floor. More information.

-Oct. 27, **Cybersecurity: Protecting our Nation's Assets** - CSPRI is the academic sponsor for a Washington Post Live breakfast panel discussion on cybersecurity at 8:00 a.m. at The Washington Post headquarters, 1150 15th Street, NW. Be our guest to hear leaders including Janet Napolitano, Secretary of the US Department of Homeland Security, and General Michael Hayden, former Director of the CIA, discuss the high-stakes public policy issues around cyber security that are important to us all. Space is limited. To register for this event, visit http://washingtonpostlive.com/conferences/cybersecurity. If you cannot attend in person, there is a live webcast of the cyber security panel discussion Thursday at 8:30 a.m. at washingtonpostlive.com.

-Oct. 31, 8:00 a.m. - 5:00 p.m., **The 7th Annual IT Security Automation Exposition** - Hosted by the National Institute of Standards and Technology, the National Security Agency (NSA), Defense Information Systems Agency (DISA), and Department of Homeland Security (DHS), this conference will provide a common understanding for using specific open standards and new security technologies across various domains of interest including continuous monitoring, software assurance, IT security threats, network security automation, management and compliance. Hyatt Regency Crystal City, 2799 Jefferson Davis Hwy., Arlington, Va. More information.

Legislative Lowdown

-Senate Judiciary Chairman Patrick Leahy (D-Vt.) said last week that he plans to schedule a markup to update the Electronic Communications Privacy Act before the end of the year, almost 25 years to the day since the law was first signed, The Hill reports. Leahy unveiled proposed updates to ECPA in May that would require the government to obtain a warrant before accessing an individual's email, digital communications, or geolocation information. He was adamant on Thursday that the law has failed to keep up with changes in technology and the changing mission of law enforcement agencies after the Sept. 11, 2001, terrorist attacks. In other cybersecurity

legislative news, several senior Obama administration officials representing the military and agencies with jurisdiction over cybersecurity met behind closed doors with the bipartisan leaders of the relevant Senate committees to discuss the need to move forward on comprehensive legislation this year. Senate Majority Leader Harry Reid's (D-Nev.) office indicated a desire to move on the issue before the end of the year and said progress has been made via the bipartisan cybersecurity working group that features those same committee heads and ranking members.

Announcements

-The Fall 2011 issue of Issues in Science and Technology recently published GW Professor Amitai Etzioni's new article, "Cybersecurity in the Private Sector" (preview available online: http://www.issues.org/28.1). The article examines the role of American corporations in the management of national cybersecurity issues, their relationship to the military and government agencies, and what measures have been taken to protect sensitive online data in the private sector. As the vast amount of sensitive information held by private security companies is often overlooked, regulation has lagged to a dangerous degree. The article concludes that stronger regulation of private institutions' data management is needed, but will not be implemented without fierce political battle.

Cyber Security Policy News

-Security experts last week discovered what they called the son of the Stuxnet worm. Nicknamed "Duqu," the malicious software shares much of the same code base with Stuxnet, strongly suggesting it was authored by the same individual or group. Experts said Duqu is technically a keylogger, and appears designed to steal sensitive data from infected systems and relay it back to the attackers, disguising the stolen keystroke logs as an image file to make it look like innocuous Internet traffic. Symantec published an in-depth examination of the malware. Not everyone is convinced Duqu is all that scary, or that it deserves so much attention. Antivirus firm Sophos points out that, unlike Stuxnet -- which only ran its destructive payload when it detected it was being run inside of systems that controlled a very specific set of industrial control system equipment -- Duqu is not targeted, and appears happy to run on any system it infects, making it little more than an overhyped keylogger.

-The Obama administration considered using cyber weapons against Libya earlier this year, The New York Times reports. Just before the American-led strikes against Libya in March, the Obama administration intensely debated whether to open the mission with a new kind of warfare: a cyberoffensive to disrupt and even disable the Qaddafi government's air-defense system, which threatened allied warplanes.

-Following closely on the breach of nearly 5 million health records, the Defense Department, General Services Administration, and NASA released a proposed regulation last week requiring all contractors that handle federal records containing personally identifiable information to complete privacy training. According to NextGov's Bob Brewin, the proposed regulation comes just one month after defense contractor Science Applications International Corp. reported the

theft of a computer tape containing the health records of 4.9 million TRICARE beneficiaries from an employee's car, and four days after the filing of a class action lawsuit asking Defense to pay $4.9 billion in damages from that theft.

-The computer networks that control power plants and financial systems will never be secure enough and a new, highly secure alternative Internet should be considered for development, a top FBI cybersecurity official told the Associated Press last week. Shawn Henry, the FBI's executive assistant director, said critical systems are under increasing threat from terror groups looking to buy or lease the computer skills and malware needed to launch a cyber attack. Henry said jihadist militants looking to harm the U.S. can tap organized crime groups who are willing to sell their services and abilities to attack computer systems. He would not say which terror group or whether any insurgent networks have actually been able to acquire the high-tech capabilities. But he said one way to protect critical utility and financial systems would be to set up a separate, highly secure Internet.

-Sen. Jay Rockefeller (D-W.Va.), chairman of the Senate Commerce, Science and Transportation Committee, asked the Federal Trade Commission on Wednesday to prepare a report on how facial recognition technology affects consumer privacy. The Hill writes that Rockefeller expressed concern over a Facebook feature that suggests the names of friends in photos based on facial recognition software. He also pointed to a now-scrapped Google project that would have allowed a user to take a photo of someone and scan the Internet to find a match. He described one mobile app that monitors the age and gender statistics of crowds in bars.

-Facebook could face fines of more than 100,000 Euros following allegations that the company retains user data long after users have deleted it. The Guardian writes that an Austrian law student discovered the social networking site held 1,200 pages of personal data about him, much of which he had deleted. Max Schrems, 24, decided to ask Facebook for a copy of his data in June after attending a lecture by a Facebook executive while on an exchange program at Santa Clara University in California. Schrems was shocked when he eventually received a CD from California containing messages and information he says he had deleted from his profile in the three years since he joined the site.

-The Securities and Exchange Commission (SEC) Division of Corporation Finance (CF) issued disclosure guidance ("Guidance") on October 13, 2011, regarding cybersecurity matters and cyber incidents. While the Guidance does not change existing disclosure requirements, it does add specificity to existing requirements. In some respects, that specificity is helpful, but the Guidance fails to take into account the uncertainty that inevitably accompanies efforts to assess and disclose cybersecurity matters and incidents. See Hunton & Williams' summary of the Guidance and thoughts regarding its effects, including its impact on disclosures both before and after a cyber incident, enforcement-related proceedings and potential litigation.

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.