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

GW CSPRI Newsletter

February 28, 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

-Feb. 28, 5:00 - 9:00 p.m., **Cyber Social Happy Hour** - An infrequent event intended for cybersecurity professionals working for and in the U.S. government in the D.C. metro area. Chef Geoff's Downtown, 1301 Pennsylvania Ave., NW. More information.

-Mar. 1, 3:00 p.m., **Future of Privacy Forum Webcast** - This special webcast discussion will focus on privacy and human rights issues, and how they impact one another online. As the world continues to witness pro-democracy movements and organize and stage protests across the Mideast with the ability to literally topple regimes through mobilization efforts on the World Wide Web, what human rights and privacy issues need to be recognized during this historic period? And how can we reduce the vulnerability of

personal information from being used improperly, while still encouraging individual rights? These are the questions that will be asked, as Jeff Rosen, Professor of Law at George Washington University Law School and legal affairs editor of The New Republic, talks with Peter Swire, FPF Advisory Board member; Senior Fellow, Center for American Progress; and C. William O'Neill Professor of Law at the Ohio State University, about his new paper, "Social Networks, Privacy, and Freedom of Association: How Individual Rights Can Both Encourage and Reduce Uses of Personal Information." Please RSVP to lauren@futureofprivacy.org to obtain livestream link.

-Mar. 2-3, **6th Annual Homeland Security Law Institute** - The second day of this two-day conference features a breakout session on "Developments in the Federal Government & Data Protection Challenges within the Private Sector." Panelists include **David G. Delaney**, deputy general counsel, Office of General Counsel, U.S. Department of Homeland Security; **John C. Demers**, chief counsel for Network & Space Systems, The Boeing Company; **Nick Lantuh**, president of Netwitness Corp.; and **Brandon L. Milhorn**, staff director and chief counsel for the Senate Committee on Homeland Security and Governmental Affairs. Capitol Hilton. More information.

-Mar. 2-4: The National Institute of Standards and Technology's Information Security and Privacy Advisory Board will hold a three-day meeting. Among the topics up for discussion is the National Strategy for Trusted Identities in Cyberspace. 100 Bureau Drive, Stop 8930, Gaithersburg, MD. More information.

-Mar. 9, 12 noon, **Investigating Cybersecurity Threats: Exploring National Security and Law Enforcement Perspectives** - GWU Professor Federic Lemieux, from the College of Professional Studies, will speak about how federal agencies define success in computer crime investigations, and how they can facilitate the development and refinement of law enforcement strategy for addressing cyber threats. Through interviews with experienced computer crime investigators from the Federal Bureau of Investigation, the U.S. Secret Service, and the Air Force Office of Special Investigations, this project aims to identify how federal agencies conduct investigations related to cyber security and how they define operational success. Room 302, Marvin Center, 800 21st St. NW. Full abstract (PDF).

Announcements

CSPRI's **Professor Lance Hoffman** is on the program committee of the Tenth Workshop on Economics of Information Security (WEIS 2011) that will take place at George Mason University in Fairfax, Virginia on June 14–15, 2011. Submissions by economists, computer scientists, business school researchers, legal scholars, security and privacy specialists, as well as industry experts are encouraged; the deadline is today. The call for participation is here. Suggested topics include (but are not limited to) empirical and theoretical studies of:

Optimal investment in information security
Online crime (including botnets, phishing and spam)
Models and analysis of online crime
Risk management and cyberinsurance
Security standards and regulation
Cybersecurity policy
Privacy, confidentiality and anonymity
Behavioral security and privacy
Security models and metrics
Psychology of risk and security
Vulnerability discovery, disclosure, and patching
Cyberwar strategy and game theory
Incentives for information sharing and cooperation

Especially encouraged at this year's workshop are submissions of significant and novel research that consider the design and evaluation of policy solutions for improving information security and also those with empirical components. A selection of papers accepted to this workshop will appear in an edited volume designed to help policy makers, managers, researchers and practitioners better understand the information security landscape.

Legislative Lowdown

-**President Obama** last week signed into law the "FISA Sunsets Extension Act of 2011," which extends statutory sunsets for lone terrorist, business records and roving wiretap authority. These three provisions, powers granted to the government under the Foreign Intelligence Surveillence Act and USA PATRIOT Act, were to expire at the end of February, and this bill extends them for another three months. Supporters of a more lengthy or permanent extension say the uncertainty surrounding the measures could hinder the work of intelligence agencies that rely on them. But critics, such as **Reps. Barney Frank** (D-Ma) and **Bobby Scott** (D-Va.), lamented that they were once again denied a chance to revisit the provisions, which Scott has called "deeply troubling." The provisions give the government "power to secretly invade our private records, such as books we read at the library, by merely alleging that they are relevant to a terrorism investigation, but without having to show that the seized material is in connection with any specific suspected terrorists or terrorist activities," Scott said in a floor speech in opposition to the measures. "There is no requirement to show probable cause or even reasonable suspicion of being related to a specific act of terrorism, and therefore there is no meaningful standard to judge whether or not the material is in fact necessary."

-Today is the deadline to submit comments to the National Institute of Standards and Technology's on the Computer Security Division's draft proposal titled, "Guidelines on Security and Privacy in Public Cloud Computing." More information (PDF).

Cyber Security Policy News

-The U.S. government has spent prodigious sums on information security over the past decade, but that figure pales in comparison to the growing share of the government overall IT budget that is being set aside for cybersecurity, The Hill reports. "Despite a ballooning federal debt and intense pressures on the federal budget, cyber security has become Washington's new growth industry," Hill reporters Kristin M. Lord and Travis Sharp wrote. "The U.S. government has spent over $600 billion on information technology over the last decade, with a growing amount devoted to cyber security. In its new Pentagon budget request, the Obama administration designated $2.3 billion to strengthen Department of Defense cyber security operations, including activities of the Pentagon's new Cyber Command and half a billion dollars for new cyber technology research. These figures exclude growing spending on "black" cyber security activities, embedded within the approximately $80 billion annual intelligence budget."

-The U.S. intelligence community should jointly create a policy on cybersecurity and determine the degree to which the U.S. should protect intellectual property and national infrastructure of other nations, urges an article in the American Intelligence Journal (PDF). **Dr. Chris Bronk**, the Baker Institute fellow in information technology policy, also urges the United States government to be far more proactive and aggressive in its cyber-spying activities.

-The **U.S. Department of Health and Human Services** levied its first civil penalty ever last week for privacy violations laid out in the 1996 Health Insurance Portability and Accountability Act (HIPPA). Cignet Health of Prince George's County has been fined a total of $4.3 million for allegedly violating 41 patients' rights in 2008 and 2009 by not providing them access to their medical records in a reasonable amount of time. The rules require health insurers to make medical records available to patients who request them within 60 days. The fine was quickly followed by the second major HIPPA enforcement action by federal authorities, in which Massachusetts General Hospital and its physicians organization have entered into a resolution agreement that calls for paying a $1 million settlement and taking corrective action to avoid future violations. The case involved the loss of documents that included information on patients with HIV/AIDS.

-Cybersecurity is expected to be a topic of discussion on the agenda this week as the nation's governors gather in Washington, D.C. for their annual winter meeting, Government Technology reports. The National Governors Association is expecting to discuss the latest threats facing governments in cyberspace, and the potential ramifications of these threats and steps governors may take to better protect their computer networks and electronic systems.

At the same time, the National Association of Chief Information Officers (NASCIO) issued a new call to action which directs attention to current cybersecurity risks. Specifically, NASCIO urges government leaders to take steps to know the risks, know the landscape, know your government cyber assets and know your opportunities.

-The oil and gas companies that were anonymously alluded to in a January 2010 exposé on a series of targeted cyberattacks dubbed "Night Dragon" have since been named as Shell, Exxon Mobil, BP, Marathon Oil, ConocoPhillips and Baker Hughes. The attacks were first reported by the Christian Science Monitor in January 2010, and were mentioned in a report from **McAfee** earlier this month. The attackers appear to have been after legal and financial data. Media reports indicate the attacks may have been going on for as long as four years. The McAfee report says the attacks were traced to IP addresses in China.

-In a recent round of domain name seizures, the Justice and Homeland Security Departments shut down potentially thousands of websites that hadn't broken the law, falsely accusing them of child pornography crimes, according to Bloomberg. “During the course of a joint DHS and DOJ law enforcement operation targeting 10 websites providing explicit child pornographic content, a higher level domain name and linked sites were inadvertently seized for a period of time,” Cori Bassett, an Immigration and Customs Enforcement spokeswoman said in an e-mailed statement. “Those sites were restored as soon as possible to normal functionality.” DHS didn't say how many legitimate Web sites were mistakenly shuttered, but a story at online file sharing news site **TorrentFreak** puts the number at 84,000.

-Chinese officials are tightening their censorship of Web content in response to a series of protests in the Middle East that spread, in part, due to the use of social media, according to a report in The Wall Street Journal. The paper writes that domestic security chief Zhou Yongkang told official media Monday that Chinese officials must act to defuse social unrest on the Web before it reaches the streets. Chinese president Hu Jintao on Saturday also called for tighter Web censorship to prevent protests.

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.