# GW CSPRI Newsletter

May 14, 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 15, 1:00 p.m. - 2:30 p.m. ET, **Data Privacy in the Global Era** - This live, online presentation will provide an overview of data privacy and security issues from a U.S. and global perspective. Managing Partner at Hunton & Williams, Lisa Sotto, will be joined by Jimmy Lin, VP of Product Management and Corporate Development at The Network, to discuss how maintaining data integrity and having a proactive approach to compliance are necessary to reduce corporate risk, protect your reputation, and avoid costly litigation. More information.

-May 16, 12:00 noon – 2:00 p.m., **Is America Ready to Vote on the Internet? Concerns for National Security** - The expert panelists will include Prof. Alex Halderman, University of Michigan; Dr. Costis Toregas, Assistant Director, George Washington University Cyber Security Policy and Research Institute and an advisor to local, national and global organizations; and Matt Masterson, Deputy Elections Administrator, Office of the Ohio Secretary of State. CSPRI Seminar Series. Details below in Announcements.

-May 16-17, **IRMI Cyber & Privacy Risk Conference** - This conference centers on topics related to cyber risk and cybersecurity insurance. Homeland and national security expert and author Richard A. Clarke will deliver the keynote address. Hyatt Regency, 300 Light St., Baltimore, Md. More information.

-May 16-17, **The Security Summit 2012 East -** The Security Network works closely with an expanding number of companies, countries, military and government agencies and sponsors and other partners to identify and promote rapid adoption of dual-usage security products and services from innovative companies around the world. The event will focus on topics including cybersecurity, anti-terrorism, GIS, port and maritime security, rapid technology fielding and international collaboration. Renaissance Arlington Capital View Hotel, 2800 South Potomac Ave. Arlington, Va. More information.

-May 16-17, **Counter Terror Expo -** This two day conference features several talks about emerging cyber threats, including attacks from hacktivist groups, corporate espionage, supply chain and information sharing. Washington Convention Center, 801 Mt. Vernon Pl., NW. More information.

-May 17, 7:30 a.m. - 11:30 a.m., **Fortifying Cybersecurity: Focus on Risk Mitigation -** This half-day conference, put on by Federal Computer Week, will examine how agencies are working to defend their digital infrastructures with more robust network monitoring, threat detection, vulnerability analysis, identity management, and targeted cyber-defense solutions that are aligned with specific risk mitigation strategies. The Willard InterContinental Hotel, 1401 Pennsylvania Avenue NW. More information.

-May 17, 10:00 a.m., **Geolocational Privacy and Surveillance Act -** The House Judiciary Subcommittee on Crime, Terrorism and Homeland Security will hold a hearing on this proposed legislation. Room 2141, Rayburn House Office Building. More information.

# Announcements

-Please join us at 12 noon on Wednesday, May 16 for a discussion about the security of electronic voting machines titled, "Is America Ready to Vote on the Internet? Concerns for National Security." There are at least two major forces tugging at the success of new, modern electronic systems that will take advantage of all society knows about technology. One is the desire for an easy system with convenient access for all, minimal administrative barriers, and allowing voters to participate in new ways that expand participation and bring people who could not or would not participate in the traditional election cycles. The other is the growing awareness of the almost remarkable ease with which systems can be hacked from near or (important to some) abroad. Technological and other "fixes" for this insecurity are not satisfactory to many. In addition, other concerns about the massive transition costs for procuring new, secure systems and training the primarily volunteer work force that administers elections may at times sideline or ignore strong opinions about the use of new technology. These conflicting forces will be explored in the upcoming CSPRI seminar, cosponsored by the Verified Voting Foundation.

The program will be moderated by Prof. Lance Hoffman, Director, GW Cyber Security Policy and Research Institute. The expert panelists will include Prof. Alex Halderman, University of

Michigan Dept. of Electrical Engineering and Computer Science (who, with his students, carried out what some have called "a totally epic hack of the DC Internet voting system pilot program"); Costis Toregas, Assistant Director, George Washington University Cyber Security Policy and Research Institute and an advisor to local, national and global organizations; and Matt Masterson, Deputy Elections Administrator, Office of the Ohio Secretary of State.

The discussion will be held in Room 302, Marvin Center at 800 21st St. NW. A hot buffet lunch will be provided, but registration is required. Please RSVP *today* to http://internetvoting.eventbrite.com.

# Legislative Lowdown

-More than 30 civil liberties groups are now officially opposed to the leading cybersecurity bill in the senate, Federal News Radio writes. In a letter to Congress, the groups said the Cyber Security Act of 2012 would allow companies like Facebook and Verizon to share customer information with the government. The measure is meant to help the government identify cybersecurity threats. But the privacy groups note that the bill, as it is currently written, would permit the government to use customer information for nearly any criminal investigation. They say that violates Fourth Amendment protections against unreasonable searches and seizures.

-Senate lawmakers clashed last week over plans to implement the Obama administration's privacy framework, reports The Hill. Sen. Jay Rockefeller (D-W.Va.) called the current regime of self-regulation inherently one-sided, and warned that without greater protections, the need to monetize consumer data would always win out over privacy concerns. Sen. Pat Toomey (R-Pa.) argued that lawmakers don't know what privacy protections are called for because most consumers don't have a strong sense of what they want in this regard either.

# Cyber Security Policy News

-Several alerts issued by the Department of Homeland Security indicate that a major series of cyberattacks has been underway over the past few months directed at U.S. natural gas pipeline companies. MSNBC writes that at least three confidential "amber" alerts – the second most sensitive next to "red" – were issued by DHS beginning March 29, all warning of a "gas pipeline sector cyber intrusion campaign" against multiple pipeline companies. But the wave of cyber attacks, which apparently began four months ago – and may also affect Canadian natural gas pipeline companies – is continuing.

-Gen. Keith Alexander, the head of the nation’s largest spy agency and its cyberwarfare command, is urging adoption of legislation to require companies providing critical services such as power and transportation to fortify their computer networks against cyber attacks, The Washington Post reports. Though he did not specify a particular bill, Alexander, commander of the U.S. Cyber Command and director of the National Security Agency, said in a letter Friday to Sen. John McCain (R-Ariz.) that “recent events have shown that a purely voluntary and market driven system is not sufficient” to protect such networks.

At the same time, The director of intelligence at U.S. Cyber Command said the command has the capacity to significantly damage a country's infrastructure if necessary, the Associated Press reports. Rear Adm. Samuel Cox said such an attack would only come after officials at the highest levels of government approved the operation because there would be a risk of collateral damage.

Meanwhile, The FBI is asking Internet companies not to oppose a controversial proposal that would require firms, including Microsoft, Facebook, Yahoo, and Google, to build in backdoors for government surveillance, according to a report from CNet. In meetings with industry representatives, the White House, and U.S. senators, senior FBI officials argue the dramatic shift in communication from the telephone system to the Internet has made it far more difficult for agents to wiretap Americans suspected of illegal activities, CNET has learned. The FBI general counsel's office has drafted a proposed law that the bureau claims is the best solution: requiring that social-networking Web sites and providers of VoIP, instant messaging, and Web e-mail alter their code to ensure their products are wiretap-friendly.

-The Federal Bureau of Investigation is advising travelers to avoid updating software while using hotel or other public Internet connections, warning that malicious actors are targeting travelers abroad through pop-up windows while they are establishing an Internet connection in their hotel rooms. From the FBI's advisory: "Recently, there have been instances of travelers’ laptops being infected with malicious software while using hotel Internet connections. In these instances, the traveler was attempting to set up the hotel room Internet connection and was presented with a pop-up window notifying the user to update a widely used software product. If the user clicked to accept and install the update, malicious software was installed on the laptop. The pop-up window appeared to be offering a routine update to a legitimate software product for which updates are frequently available.”

*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.*