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

GW CSPRI Newsletter

February 22, 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. 22, 10:00 a.m., Webinar: What is the National Electric Sector Cybersecurity Organization (NESCO) - In this free webinar, **Patrick Miller**, CEO of EnergySec and the principal investigator on the NESCO project, will guide attendees through: What NESCO is, why NESCO was created, its mission and goals, the differences between NESCO and EnergySec, the supporting role of NESCO, funding structure, the critical role of industry, its partnerships, outreach efforts and more. More information.

-Feb. 22-24, **AFCEA Homeland Security Conference** - Topics of discussion include identity management, interagency collaboration, and DHS/state and local secure information-sharing. Speakers include **Gen. Keith Alexander**, director of the National

Security Agency and commander of the U.S. Cyber Command. Ronald Reagan International Trade Center. More information.

-Feb. 23, 3:00 - 6:00 p.m., **5th Annual GW School of Engineering and Applied Science Student Research & Development Showcase** - This fifth annual event is designed to provide highlights into the latest R&D activities at SEAS. This year's event will feature approximately 60 student R&D projects in the form of individual posters hosted by the graduate students and their faculty advisers. The posters accompanied by the students' oral presentations will be judged by a panel of expert reviewers and the top winners will be presented cash awards at the concluding Awards Ceremony. The William Corcoran Ballroom, The Four Seasons Hotel, Washington. More information.

-Feb. 24, 8:00 a.m. - 12 noon, **FedScoop's 2nd Annual CyberSecurity Summit** - The summit will host discussions on topics such as "Securing the Cloud," and "Law Enforcement's Perspective on Cyber Crime," and feature talks from U.S. Defense Command and Control Infrastructure Admiral (Ret.) **Betsy Hight**; Justice Dept. CIO **Vance Hitch**; Dept. of Defense Deputy CIO **Robert Carey**; and Symantec Vice President **GiGi Schumm**, among others. Newseum, 555 Pennsylvania Ave, NW. More information.

-Feb. 24, 2:00 p.m., Webinar: State Legislation Past and Present, and the Effects of Data Breach Notification and Resolution - A free Webinar about how companies that have experienced data breaches have fared given the new state data breach disclosure laws. Speakers include **Christopher Wolf**, partner and leader of the privacy and information management practice at Hogan Lovells LLP, and **Reed Freeman**, partner at Morrison & Foerster LLP. More information.

-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.

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 February 28, 2011. 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's 2012 budget includes nearly $80 billion in federal IT spending, including a hefty amount of new spending on cybersecurity programs, InformationWeek reports. The budget calls for $2.3 billion in new and ongoing spending on operational cybersecurity and cybersecurity research and development at the Department of Defense and greater joint planning efforts on cybersecurity between DoD and the Department of Homeland Security, as well as $119 million "to support full operational capability" for the military's new Cyber Command. At DHS, the President's budget seeks $459 million to support the operations of the National Cyber Security Division, which is responsible for helping to secure civilian agency IT systems. Also, $97 million will be spent on improving the security of online transactions, cybersecurity education, cybersecurity R&D, and network security at small agencies, according to Computerworld.

-Responding to charges that their legislation would establish an Internet "kill switch," the top members of the Senate Homeland Security Committee introduced legislation late Thursday that would specifically keep the president from shutting down the Internet, numerous press outlets report. The committee's chairman, **Sen. Joe Lieberman**, I-Conn., and ranking member, **Sen. Susan Collins**, R-Maine, joined Sen. Tom Carper, D-Del., in revising and reintroducing their Cybersecurity and Internet Freedom Act.

The kill switch concerns have intensified recently amid political protests in many countries in the Middle East that have been met with Internet censorship, including a near total Internet blackout in Egypt. Interestingly, what killed the Internet in Egypt was not a kill switch, but rather intimidation of local ISPs by the government, writes the New York Times.

-Lawmakers in the Senate plan to offer legislation this year targeting Web sites that traffic in digital piracy or counterfeited goods, according to Grant Gross of IDG News Service. "Sen. Patrick Leahy, a Vermont Democrat, promised Wednesday to introduce a bill targeting so-called rogue Web sites, although he did not say how closely the new legislation would mirror the Combating Online Infringement and Counterfeits Act (COICA)." That bill, which the Senate failed to act on, would have given the U.S. Department of Justice new authority to force domain name registrars to shut down Web sites that allegedly infringe copyright.

Cyber Security Policy News

-The annual RSA conference, the world's largest computer security conference, was center stage for some important pronouncements and speeches on cybersecurity and cyber this past week. **Howard Schmidt**, the White House cybersecurity coordinator, used the event to defend a new federal program that would allow individual Internet users to authenticate their online identities, the Wall Street Journal reports. Schmidt argued that the National Strategy for Trusted Identities in Cyberspace is meant to serve as a catalyst for the private sector to adopt however it sees fit, and will “balance privacy, anonymity and security.”

General Keith Alexander, Director of the U.S. Cyber Command, told RSA attendees that the U.S. military had made strides in the realm of cyber security with the creation of a unified Cyber Command, but that broader, national programs of digital literacy and investment in core sciences were needed to ensure the nation's long term security. The U.S. Military's top officer in charge of cyber security said that the country must invest more in so-called "STEM" programs - science, technology, engineering and math - to avoid being outflanked in a world where cyber offensive- and defensive operations are the keys to military victory, writes Kaspersky Labs' ThreatPost.

As if to buttress Alexander's point, a new study from **(ISC)2** found that threats on mobile devices and added responsibilities have many IT security professionals showing signs of strain. In addition, the study pointed to a severe gap in skills needed industry-wide.

-More than 100 foreign intelligence agencies have tried to breach U.S. defense computer networks, largely to steal military plans and weapons systems designs, the Associated Press reports, citing top Pentagon officials. "Deputy Defense Secretary William Lynn said that while foreign governments and rogue states may try to launch more destructive attacks against military networks, most may stick to theft and spying because they are worried about a U.S. counterattack."

-**Secretary of State Hillary Clinton** last week announced that former **National Security Council Director Christopher Painter** will head the department's new cybersecurity post. Bloomberg reports that Clinton’s announcement came in a broad speech on Internet freedom, coming against the backdrop of citizens using social networking sites run by

Facebook Inc. and Twitter Inc. to organize demonstrations spreading across the Mideast and North Africa.

-**Rear Adm. William Leigher**, deputy commander for the Tenth Fleet, the Navy's component of the U.S. Cyber Command, said in an interview with Federal News Radio that the service will turn on a new system next week that will give the Navy its first real-time view into all traffic coming in and going out of its networks.

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.