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

GW CSPRI Newsletter

January 31, 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

-Jan. 31, 7:30 - 11:30 a.m., Cyber Security Conference for Business, "Are You Secure?" - Hosted by **Congressman Roscoe Bartlett**, this symposium will examine threats and techniques to secure electronic and information infrastructure. Ft. Detrick, Md. More information.

-Feb. 2, 12:00 - 1:00 p.m., Prof. Diana Burley of GW's School of Education and Human Development discusses "Recruiting, Educating, and Retaining Cyber Security Professionals in the Federal Workforce: Lessons Learned but not yet Applied" (PDF abstract). More information. (This is part of the CSPRI Seminar Series for 2011: Details for the entire year are here.)

-Feb. 3, 12:00 - 1:30 p.m., **Cybersecurity Research** - Ron Deibert, co-founder and principal investigator of the OpenNet Initiative and the Information Warfare Monitor

projects, discusses cyber security research, threat identification, and cyber espionage. Lunch will be provided. RSVP to Katrina Timlin at ktimlin@csis.org or at 202-775-3158. Center for Strategic and International Studies, 1800 K Street, NW. More information.

-Feb. 3, **Identity Protection and Management Symposium** - This free government event, produced by **Digital Government Institute**, will review the significant progress made by public and private organizations who are actively addressing improved identity management and protection on a national scale. Keynote speakers include Richard Spires, chief information officer, Department of Homeland Security, and Jim Lewis, director and senior fellow of the technology and public policy program at the Center for Strategic and International Studies. Ronald Reagan Building, Polaris Suite, 1300 Pennsylvania Ave. NW. More information.

-Feb. 9, 2:00 - 3:00 p.m., **Cyber Security: How to Protect Sensitive Client Information** - Sponsored by the SMB Cyber Security Alliance, this presentation focuses on the risk to customer personal confidential information and basic steps that should be take to better protect your business and the privacy of your customers. The SMB Cyber Security Alliance is a volunteer-run initiative by leading industry cyber security professionals, college professors, and cybercrime researchers seeking to increase cyber security awareness in small business communities through education, awareness training, free resources, and active engagement between local information security professional and small businesses. 113 South Columbus St., Suite 100, Alexandria, Va. 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.

Cyber Security Scholarships - Application Deadline Today!

-CSPRI has awarded 59 full-ride scholarships to GW students since 2002 to study computer security and is now recruiting applicants for 2011-2013. Rising juniors, seniors, and graduate students who are U.S. citizens can apply. The deadline for submitting applications, including reference letters and transcripts, is today. Complete details are here.

SECuR-IT Summer Internships in California

The Summer Experience, Colloquium and Research in Information Technology (SECuR-IT) is a ten-week paid internship (June 13-August 19, 2011) with academic seminars, sponsored by TRUST partners UC Berkeley, Stanford University and San Jose State University with internships located in Silicon Valley and the San Francisco Bay Area.

SECuR-IT participation is open to graduate students (M.S. & Ph.D). Participation is limited to 30 people selected from a nationwide pool of applicants, who have demonstrated, outstanding academic talent. Women and historically underrepresented ethnic minority groups will be given strong consideration although everyone is encouraged to apply.

This is an excellent opportunity for students, having an emphasis in computer security, to gain invaluable research experience working with Silicon Valley technology companies. Students will attend computer security seminars at UC Berkeley, Stanford University, San Jose State University and at Silicon Valley industry locations.

The application deadline is February 18, 2011. Additional information can be found here.

Legislative Lowdown

-Senate Democrats last week reintroduced a bill that is expected to be the foundation for another try at passing broad cybersecurity legislation this year. The bill, the "Cybersecurity and American Cyber Competitiveness Act" (S. 21) and introduced by Senate Majority Leader **Harry Reid** (D-Nev.), is light on specifics for the moment, but is expected to include most of the elements of a bill (PDF) introduced last session by **Sens.**

Joseph Lieberman (I-Conn.) and **Susan Collins** (R-Maine). According to a statement posted at Democrats.Senate.gov, the bill calls for urgent action to safeguard critical infrastructure, including the electric grid, military assets, the financial sector, and telecommunications networks; urges incentives for the private sector to assess the risk of cyber terrorism and take action to prevent it and promote investments in the American IT sector; seeks to improve the capability of the U.S. government to assess cyber risks, and to prevent, detect, and respond to attacks; calls for safeguards to protect consumers by preventing identity theft and guarding against abuses of personal information; and seeks to promote cooperation between nations in responding to cyber threats.

For his part, Sen. Jay Rockefeller IV (D-W.Va.), the chairman of the powerful Senate Committee on Commerce, Science and Transportation, said he intends to make cybersecurity a priority in the upcoming year. Rockefeller said that in addition to pressing for a "comprehensive" cyber security legislation and improving the public safety communications network, he wants to enhance the current level of consumer protection and investigate important online frauds, such as billing scams.

-Sen. Ron Wyden (D-Ore.) said last week that he plans to introduce a bill that would require law enforcement agencies to get court-ordered warrants to obtain location-based information from smartphones and other mobile devices, instead of just simple subpoenas and other methods that do not require strict court oversight, writes Grant Gross of the IDG News Service. Wyden said the legislation was necessary because there is confusion across the U.S. about the current standard needed for law enforcement to get location information from mobile phones, with court rulings conflicting with each other.

Cyber Security Policy News

-Federal banking regulators are soon expected to issue new online transaction authentication and security guidelines for banks, in the face of increasingly sophisticated and costly cyber attacks. The **Federal Financial Institutions Examination Council** (FFIEC, the regulatory body that issued the last round of guidance on secure electronic banking Authentication in an Internet Banking Environment (PDF) in 2005, plans to issue new online transaction authentication guidelines for banks to clarify existing recommendations, according to **Avivah Litan**, a noted fraud analyst with Gartner Inc. Current guidelines urge banks to use so-called "multi-factor authentication," but allow institutions great leeway in deciding what that standard means. "Not all financial institutions have kept up with the spirit of the 2005 guidance," Litan said. "The threats and associated risk levels have clearly moved ahead of the safeguards many banks and credit unions, and their service providers have in place today."

-U.S. military and law enforcement officials say the government has made significant strides in figuring out who is responsible for complex cyber attacks, a fundamental but elusive first step to determine whether the U.S. should strike back, whom to strike, and how hard, the Associated Press reports. "U.S. authorities are using a mix of high-tech forensics and a greater emphasis on spying within the online world, although officials

won't reveal exactly how they are ferreting out cyber criminals in the vast, often anonymous Internet universe," the story notes. "Officials familiar with the issue say the escalating cyber security threat has triggered a greater government-wide emphasis on collecting intelligence related to computer crimes. The broader approach includes spycraft methods from electronic surveillance and satellites to international cooperation and the everyday tactics and techniques that undercover agents use."

-The Homeland Security Department is in the final stages of deploying the second stage of its intrusion detection and prevention system -- known as "Einstein" -- across civilian government networks, but it is already making preparations for a third iteration of the program. **DHS Secretary Janet Napolitano** said in a speech at **George Washington University's Homeland Security Policy Institute** that DHS would finish development of and begin deploying Einstein 3 in 2011. Federal News Radio has more on Napolitano's speech and DHS's plans. Einstein 3 has raised concerns among privacy experts, who worry that the system is almost certain to involve greater federal oversight of and visibility into private-sector communications networks. DHS's privacy impact assessment of the program is available here (PDF).

-The new National Terrorism Advisory System- a project the Department of Homeland Security is rolling out to replace its widely-ignored, color-coded terrorism alert system -- will distribute alerts not only through traditional law enforcement and news media channels but also through social media, the department said last week. DHS set up a new Twitter account (@NTASAlerts) on Jan. 27 to carry the new alerts, and has erected a Facebook page that all Facebook users can 'friend' for updates. DHS Secretary Janet Napolitano said the new two-tiered alert system will distribute targeted alerts about specific or credible terrorist threats. Depending on the nature of the threat, the alerts may be distributed to the public at large or they may be distributed in a limited fashion to the potentially targeted individuals. The threats will be labeled “imminent” or “elevated". Each alert will summarize the potential threat, describe the measures officials are taking and recommend steps for people to take, Napolitano said.

-When the Egyptian government disconnected the majority of the country's Internet access last week in response to anti-government protests, the volume of junk e-mail and malicious software activity emanating from the area also declined precipitously, experts found. Security wonks at data leak prevention company Unveillance charted a major drop in malicious software activity, while security experts at Sophos were able to chart the disconnection by showing that spam from the nation completely vanished. Meanwhile, American officials and tech groups urged Egyptian leaders to restore Internet communications.

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.