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

GW CSPRI Newsletter

January 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

-Jan. 25-26, The Nuclear Energy Institute's Cyber Security Implementation Workshop - The U.S. Nuclear Regulatory Commission requires both a cyber security plan and an implementation schedule from licensees and applicants. The plan describes how licensees will meet the cyber security requirements of their regulations. The implementation workshop will assist licensees by providing insights into the implementation of the cyber security plan. Hilton Baltimore. More information.

-Jan. 26, 5:30 - 6:30 p.m., **Cyber Warfare, Stuxnet and Beyond** - The Center for Strategic and International Studies (CSIS) hosts a discussion about the sophisticated malware that is being blamed for delaying Iran's nuclear program. Moderated by CBS

News Chief Washington Correspondent **Bob Schieffer**, the panelists include: **John Markoff**, science reporter, The New York Times; **David Sanger**, chief Washington correspondent, The New York Times; **James Lewis** director of CSIS's technology and public policy program. CSIS, B1 Conference Center, 1800 K. St., NW. More information. (Also at the CSIS website is a list of "Significant Cyber Incidents Since 2006", with a focus on "successful attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars".)

-Jan. 26, **Location-Tracking Technology and Privacy** - The CATO Institute hosts a forum featuring **Sen. Ron Wyden** (D-OR); **Julian Sanchez**, Research Fellow, Cato Institute; and **Jim Harper**, Director of Information Policy Studies, Cato Institute. The Cato Institute 1000 Massachusetts Avenue, NW. More information.

-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.

-CSPRI Seminar Series for 2011: Details for the entire year are here. The next seminar at noon on February 2, 2011 features Prof. Diana Burley of GW's School of Education and Human Development discussing "Recruiting, Educating, and Retaining Cyber Security Professionals in the Federal Workforce: Lessons Learned but not yet Applied" (PDF abstract). Details are here.

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 Nears

-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 January 31. 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 Majority Leader Harry Reid (D-Nev.) is hoping to bring comprehensive cybersecurity legislation to a floor vote this year, and the earlier the better, according to eSecurity Planet. In the coming year, Reid is hoping to meld the frameworks of several competing measures crafted in the last session, and move a bill to the floor once the

administration and industry groups weigh in with their input on what the final legislation should look like, the publication reports.

Cyber Security Policy News

-The European Commission suspended trading in greenhouse gas emissions permits on Wednesday for at least a week after the theft of permits worth millions of euros via online attacks, the New York Times reports. The Emissions Trading System was a target of "recurring security breaches" over the last two months, the commission, the executive agency of the European Union, announced on its Web site Wednesday. The commission said it needed to shut the system down until at least Jan. 26 because "incidents over the last weeks have underlined the urgent need" for enhanced security measures.

-Cyberattacks on critical infrastructure systems should be considered the 'new normal,' as emphasis shifts from protecting critical systems from attack to finding ways to bounce back quickly from such assaults, Government Computer News' **William Jackson** observes in a column this week. The ability to recover from attacks takes on greater importance in the new reality of cyber war in which specialized weapons like Stuxnet can quietly disable your most vital systems, expert warns.

-The Obama administration will provide universities and businesses with government intelligence and law enforcement information about malicious Internet activities so that they can protect their critical assets, the president's cyber czar said last week. "I think we all recognize that the government has unique access to information," **Howard Schmidt**, cybersecurity coordinator and special assistant to the president, told congressional staff, policymakers and interest groups at a Washington conference. "We need to continue to look for ways to share that information, but also give our universities and our businesses information to be able to protect themselves."

-The U.S. Army's released an update to its Army Social Media Handbook, a document meant to offer social network usage guidance for soldiers, personnel and families, Mashable.com's **Radhika Marya** reports. The new social media handbook now provides additional tips and best practices, along with information on operations security tips, branding information, checklists, regulations and frequently asked questions, such as setting privacy options to "friends only," and turning off the GPS function of smartphones to avoid geotagging. The new handbook comes as the existing social media guidelines (PDF) set by the U.S. Department of Defense are getting ready to expire. The regulations are set to expire on March 1, and the specter of the DoD missing the deadline is prompting some to wonder whether that might leave the future of social media at DoD in limbo. A Pentagon spokesperson said the DoD has no plans to ban the use of social media, and that the department intends to fully utilize those capabilities.

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.