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

GW CSPRI Newsletter

January 18, 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. 18-19, **7th Annual State of the Net Conference** - This year's conference will celebrate "15 Years of Internet Policy," marking not only the 15 year anniversary of the **Congressional Internet Caucus** itself but also 15 years of 42 U.S.C. Sec 230 and the anniversaries of other Internet legislation such as the Communications Decency Act and the 1996 Telecom Act. The conference will feature discussions with leading Internet policy experts and panel tracks focusing on privacy/security, telecommunications regulation, intellectual property and innovation. More information. Hyatt Regency Capitol Hill, 400 New Jersey Avenue, NW,

-Jan. 18-19, **Black Hat DC 2011** - Two days of presentations on some of the world's most advanced research on new and emerging threats to physical and cyber security. Hyatt Regency Crystal City, Va. Agenda and registration.

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

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.

New Reports

New reports from CSPRI are now available at our website:

1- Patricia MacTaggart & Stephanie Fiore, "Healthcare Reform and Medical Data Security and Privacy", Report GW-CSPRI-2010-1
2- Jeffrey Rosen, "From Perfect Citizen to Naked Bodyscanners: When is Surveillance Reasonable?", Report GW-CSPRI-2010-2
3- Lance Hoffman, "Building the Cyber Security Workforce of the 21st Century: Report of a Workshop on Cyber Security Education and Workforce Development", Report GW-CSPRI-2010-3
4- Ross A. Lumley, "Cyber Security and Privacy in Cloud Computing: Multidisciplinary Research Problems in Business", Report GW-CSPRI-2010-4

Legislative Lowdown

-The chairman of the House Homeland Security Committee is asking the Obama administration to present Congress with a detailed timeline for its plan to secure the Mexico-U.S. border following its move to scrap a flawed, tech-heavy $1 billion border fence initiative, Hillicon Valley reports. Department of Homeland Security **Secretary Janet Napolitano** announced the discontinuation of the SBInet program last Friday, outlining a new plan that will replace SBInet with unmanned aerial vehicles, thermal imaging cameras, and a variety of other surveillance tools.

-Capitol Hill watchers may not expect much from this new session of Congress, but a number of tech policy experts expect congressional action on several high-tech issues in 2011, writes Computerworld's **Grant Gross**. Tech related bills likely to move forward this year include a revamp of the 25-year-old Electronic Communications Privacy Act. Breaking competing, broader cybersecurity measures down into more bite-sized chunks may prompt movement on comprehensive cybersecurity legislation, Gross notes.

Cyber Security Policy News

-Attacks on computer systems now have the potential to cause global catastrophe, but only in combination with another disaster, according to a report (PDF)released Monday by The Organization for Economic Cooperation and Development (OECD). The study, part of a wider OECD project examining possible “Future Global Shocks” such as a failure of the world’s financial system or a large-scale pandemic, said there were very few single “cyber events” that could cause a global shock, Reuters' Michael Holden reports: "Examples were a successful attack on one of the technical protocols on which the Internet depends, or a large solar flare that wiped out key communications components such as satellites. But it said a combination of events such as co-ordinated cyber attacks, or a cyber incident occurring during another form of disaster, should be a serious concern for policy makers."

-An international treaty to establish regulations for computer security -- such as a pact outline which networks or offensive cyber weapons might be off limits in a time of conflict -- might be unattainable, according to a new report by the think tank **EastWest Institute**. NextGov says the organization's leaders determined that cybersecurity legislation isn't the best fix for the frail digital economy. Rather, the report notes, voluntary private sector agreements and international standards are more practical avenues to pursue, they said. The report comes as lawmakers in both chambers have pledged to make comprehensive cybersecurity legislation a top priority this Congress.

-Despite the ongoing development of energy grid security standards, the organization that regulates the electrical system lacks the power to enforce those standards, a new report (PDF) from the **Government Accountability Office** (GAO) found. The standards for a smart grid are being assembled by the National Institute of Standards and Technology under the Energy Independence and Security Act of 2007; EISA also directed the Federal Energy Regulatory Commission, the primary federal regulator of the electricity system, to adopt standards for smart grid security and interoperability. The GAO notes that while a framework of standards for securing an intelligent energy grid is emerging, it is not yet complete and federal overseers lack the authority to require industry compliance, writes Government Computer News.

-The first global trial of Internet Protocol version 6 (IPv6) is scheduled to take place on June 8, 2011. The event, being coordinated by the Internet Society, is being held to raise awareness about the imminent change from version 4 of the addressing scheme to version 6, according to the BBC. For a 24-hour period, participants, including Facebook, Google and Akamai, will make their pages available via IPv6. Companies are being encouraged to switch to IPv6, as it is estimated that IPv4 addresses will run out by the end of this year.

-**The Associated Press** reports that the Senate is pursuing unresolved questions about how and when the Pentagon conducts cyber warfare, and the guidelines surrounding military action in the event of a concerted cyber attack on the United States.

A brief written exchange between Senate questioners and the Pentagon's assistant secretary for special operations shows that the Pentagon failed to disclose clandestine cyber activities in a classified report on secret military actions that goes to Congress. **Adm. Mike Mullen**, chairman of the Joint Chiefs of Staff, told reporters Wednesday that the cyber threat from China is significant and that the Defense Department needs to focus more on cyber warfare.

-The Department of Homeland Security is planning to underwrite a cyber security testbed at the University of Southern California's Information Sciences Institute, according to Federal News Radio. The publication writes that the 5-year, $16 million project is called DETECT, and its mission is to expand the outreach to cyber researchers to diversify the research resources available to academia, industry and government.

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.