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

GW CSPRI Newsletter

July 11, 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

-July 11-12, **Industrial Security Conference** - As the threat of terrorism and cyber attacks increases, so does the need to ensure your industrial security compliance program is up to date, robust and comprehensive. This Summit will provide proven-effective strategies for implementing strong security and compliance measures. The Westin Washington D.C. City Center, 1400 M. St. NW. More information.

-July 12, 10:00 a.m., **Cybersecurity Best Practices & Lessons for Enterprises Under Persistent Threat** - 'Night Dragon' and 'Stuxnet' attacks have unleashed a flurry of media coverage. As cybersecurity threats escalate and the level of process automation increases, the oil and gas industry is taking lessons from downstream plants and the utility industry. Nation state attackers are the biggest threat to the industry, but many

unknown threats also exist worldwide. This Webcast will address best practices from other Process Industries that are proactively addressing regulatory mandates, protecting the most sensitive enterprise data and industrial controls. More information.

-July 12, 6:30 p.m. - 8:00 p.m., **The Cyber Realm: A New Way Forward for U.S. Policy** - This panel will feature **Robert Butler**, deputy assistant secretary of defense for cyber policy, and **Samuel Visner**, vice president and cyber lead executive, Computer Sciences Corporation. UC - Washington Center, 1608 Rhode Island Ave, NW. More information.

-July 15, 8:00 a.m. - 5:00 p.m., **DC Cybersecurity Symposium** - This conference will focus on the state of the U.S. cyber protection one year after the stand-up of U.S. Cyber Command. The gathering also will explore CYBERCOM's interface with the five military services, the Unified Commands/COCOMs, DHS, Civilian Agencies, Industry, and Coalition Partners - as these enmeshed interrelationships unfold, and the framework for collaboration strengthens. Capital Hilton, 1001 16th St. NW. More information.

-July 15, 10:00 a.m., **The Promises We Keep Online: Internet Freedom in the OSCE Region** - The Commission on Security and Cooperation in Europe will hold a hearing to examine the current trends in Internet governance in the OSCE region, with a particular focus on Belarus, Russia, Azerbaijan and Central Asia. The hearing is precipitated by recent arrests of bloggers, blocking of websites, online intimidation and surveillance of peaceful political activists, aggressive denial of service attacks, and other acts by OSCE participating states that deter citizens from using the Internet as a forum for receiving and sharing information. Specifically, the hearing will address whether or not these countries are meeting international standards and OSCE commitments on freedom of expression and information in the online environment. 210 Cannon House Office Building. More information.

-July 18, 8:15 a.m. - 5:30 p.m., **Internet Governance Forum USA** - The one-day event will include expert panels and workshops on important Internet governance issues and serve as a prelude to the global United Nations-facilitated Internet Governance Forum. Topics of discussion include privacy, security, geo-location, government and law enforcement cooperation, transational location issues, and emerging challenges in Internet governance. Georgetown University Law Center, 600 New Jersey Ave., NW. More information.

Legislative Lowdown

Need a refresher on all of the proposed cybersecurity and privacy legislation introduced in the 112th Congress? The Center for Strategic and International Studies has published a handy list of the top bills, including proposals to clarify the government's role in securing cyberspace, increase cybersecurity research and development, beef up personal data privacy and security, and shore up the cybersecurity of the electric power grid. The guide, available at this link, divides the bills into Senate and House measures.

Cyber Security Policy News

-A top Department of Homeland Security official has admitted to Congress that imported software and hardware components are being purposely spiked with security-compromising attack tools by unknown foreign parties. In testimony before the House Oversight and Government Reform Committee, acting deputy undersecretary of the DHS National Protection and Programs Directorate Greg Schaffer told Rep. Jason Chaffetz (R-UT) that both Homeland Security and the White House have been aware of the threat for quite some time, FastCompany reports. When asked by Rep. Chaffetz whether Schaffer was aware of any foreign-manufactured software or hardware components that had been purposely embedded with security risks, the DHS representative stated after some hesitation, "I am aware of instances where that has happened." This supply chain security issue essentially means that, somewhere along the line, technology being marketed in the United States was either compromised or purposely designed to enable cyberattacks.

-U.S. workers looking for job security in a tough economic climate could do a lot worse than to pursue a career in information security. According to new statistics from the Department of Labor, employment among information security analysts in the United States soared this past quarter by 16 percent, with none of the professionals in this line of work reporting that he or she was out of a job. According to GovInfoSecurity.com, among the 12 computer-related job classifications tracked by the Department of Labor's Bureau of Labor Statistics, information security analysts, along with computer and information research scientists, were the ones to report no unemployment during the first two quarters of 2011. Computer network architects had a minute 0.5 percent jobless rate in the second quarter, compared with none in the first quarter. The number of people who consider themselves IT security analysts rose to 43,000 during the April-to-June period, up from the 37,000 from the previous three months, the publication reports.

-The big U.S. Internet service providers (ISPs) have agreed to a system that could allow them to disrupt service for people who habitually download copyrighted works via file-sharing networks, Wired.com reports. AT&T, Cablevision, Comcast, Time Warner and Verizon all have agreed to participate in the voluntary program. After four copyright offenses, the plan calls for these companies to initiate so-called "mitigation measures" that might include reducing internet speeds and redirecting a subscriber's service to an "educational" landing page about infringement. The internet companies may eliminate service altogether for repeat file sharing offenders, although the plan does not directly call for such drastic action.

-The Department of Energy's Pacific Northwest National Laboratory is working on restoring Internet connectivity and email services after being hit by a "sophisticated cyberattack" earlier this month. Computerworld's Jaikumar Vijayan writes that it is not immediately clear if the attack resulted in any data being stolen or compromised. A lab spokesman did not immediately respond to a request for comment, but a message on the spokesman's voicemail noted that Internet and email services were down because of a sophisticated attack.

-Google has hidden more than 11 million URLs from its search results as part of its ongoing effort against search spam, by blocking all sites ending in "co.cc," the San Francisco Chronicle writes. The top-level domain is owned by a Korean company, which lets other companies reserve 15,000 domains at a time for a bulk price of $1,000. Google's Matt Cutts said sites ending in co.cc were a major source of phishing attacks in 2010, and Google's anti-spam head recently explained (in a Google+ post, of all places) that the company reserves the right to block an entire domain "if we see a very large fraction of sites on a specific freehost be spammy or low-quality."

-The United States may seriously want to consider creating a new Internet infrastructure to reduce the threat of cyberattacks, according to Michael Hayden, President George W. Bush's CIA director. NextGov's Aliya Silverstein writes that several current federal officials, including U.S. Cyber Command chief Gen. Keith Alexander, have also floated the concept of a ".secure" network for critical services such as banking that would be walled off from the public Web. Unlike .com, .xxx and other new domains now proliferating the Internet, .secure would require visitors to use certified credentials for entry and would do away with users' Fourth Amendment rights to privacy. Network operators in the financial sector, for example, would be authorized to scan account holders' traffic content for signs of trouble. The current Internet setup would remain intact for people who prefer to stay anonymous on the Web.

-A federal inspection has uncovered weaknesses in Homeland Security Department systems that house information regarding critical U.S. networks. A report from the DHS inspector general's office examined the safeguards surrounding a pair of department systems that contain sensitive data about vital U.S. networks and infrastructure. A heavily redacted version of the report is available here.

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.