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

GW CSPRI Newsletter

September 12, 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

-Sept. 12-15, **Gridweek -** A technology conference focused on efforts to develop and protect the smart energy grid. Conference agenda. Walter E. Washington Convention Center, 801 Mount Vernon Place, NW.

-Sept. 13, 7:30 a.m. - 9:30 a.m., **Focus on Defense: Leveraging Technology for Innovation -** This conference by Government Executive brings together the Defense Department's top technology leaders. Speakers include Frank Konieczny, chief technology officer, U.S. Air Force; Rob Carey, deputy chief information officer, Department of Defense; Mike Krieger, deputy chief information officer, U.S. Army; Barbara Hoffman, deputy chief information officer, U.S. Navy. Crystal Gateway Marriott, Salon A & B. 1700 Jefferson Davis Highway, Arlington, Va. More information.

-Sept. 13, 7:30 a.m. - 11:30 a.m, **DOD Network Security Forum** - Defense Systems and McAfee for the third conference to hear directly from government and industry practitioners who are fighting the cyber defense war behind the scenes. Speakers include Mark Orndorff, director, mission assurance and network operations, Defense Information Systems Agency; Jeffrey Schilling, chief, current ops, Army Cyber Command/NETCOM; Eric Rinderer, chief of cybersecurity, NJVC and senior technical executive, National Geospatial Intelligence Agency; John Toomer, former deputy director, cyber and information operations directorate, U.S. Air Force. Willard InterContinental Hotel, 1401 Pennsylvania Ave., NW. More information.

-Sept. 13, 8:00 a.m. - 10:00 a.m., **Ethics and Privacy on the Internet: What Communicators Need to Know** - This PRSA-NCC Professional Development Workshop will provide some rules of the road for ethics and privacy on the Internet as they relate to professional communicators and journalists. Speakers include Randy Barrett, communications director, Center for Public Integrity; Justin Brookman, director, Consumer Privacy Project, Center for Democracy & Technology; Christian Olsen, vice president for the Digital and Social Media team at Levick Strategic Communications. Navy Memorial, 701 Pennsylvania Avenue, NW. More information.

-Sept. 15, 8:15 a.m. - 5:00 p.m., **Washington DC Tech Security Conference** - This conference features 25-30 vendor exhibits and several industry experts discussing current tech-security issues such as email security, VoIP, LAN security, wireless security, and USB drive security. L'Enfant Plaza Hotel, 480 L'enfant Plaza SW. More information.

-Sept. 15, 9:30 a.m., **Internet Privacy: The Impact and Burden of EU Regulation** - The Subcommittee on Commerce, Manufacturing, and Trade has scheduled a hearing. Witness list to be announced. Rayburn House Office Building, Rm. 2322. More information.

-Sept. 20, 9:00 a.m. - 10:30 a.m., **Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch** - McAfee's Alperovich and SCADA expert Langer will discuss the actualities of cyberdeterrence. Langner argues that deterrence is unlikely to prevent intense cyberwar and cyberterrorist attacks because they can be carried out by small international teams and prepared months or years in advance. He also points out cyberattacks against critical infrastructure and terrorist targets such as chemical facilities and nuclear power plants can and must be prevented by solid cyber protection. Alperovitch, on the other hand, presents a case for a strategic declaratory deterrence policy to counter highly destructive cyberthreats from nation-state actors against critical infrastructure and other crucial national security and economic assets. The Brookings Institution, Falk Auditorium, 1775 Massachusetts Ave, NW. More information.

Legislative Lowdown

-The House Energy & Commerce Committee last week released its agenda for the fall legislative session. Cybersecurity and privacy issues are expected to dominate the technology agenda for the panel this year, according to The Hill. The subcommittee on manufacturing will be tasked with examining privacy issues such as how information about consumers is collected and used online.

The committee has already held hearings on the issue and is expected to take part in the upcoming debate over comprehensive privacy legislation.

GovInfoSecurity reports that **Sen. Richard Blumenthal** (D-Conn.) has introduced a new bill aimed at protecting consumers by punishing businesses, individuals and data brokers that misuse or fail to protect their data. **The Personal Data Protection and Breach Accountability Act** would require businesses with the personal information of more than 10,000 customers to implement privacy and security programs to ensure the safety of pertinent data.

Cyber Security Policy News

The Obama administration is asking for legislation that would impose minimum sentences for anyone convicted of cyber attacks or attempted attacks on critical infrastructure, PC Magazine writes. The administration's proposed updates to the Cyber Fraud and Abuse Act would also make it clear that RICO, the Racketeering Influenced and Corrupt Organization Act, a major law enforcement tool against organized crime, applies to such offenses.

The White House proposal isn't sitting well with some members on the Senate Judiciary Committee, who expressed concerns at a hearing last week that the administration might be overreaching in criminalizing some online behavior, according to Government Computer News. **Committee Chairman Patrick Leahy** (D-Vt.) said he supported the thrust of the bill, but cautioned later that “we want to concentrate on the real cyber crimes” and not turn minor violations of service agreements into federal crimes. Leahy and ranking **Republican Chuck Grassley** of Iowa also were uneasy about a legislative proposal that would impose minimum sentences for anyone convicted of attacks or attempted attacks on critical infrastructure. Leahy said he would not recommend including minimum sentences in a cybersecurity bill now before his committee.

-Google says it will be implementing changes to help combat abuse against a feature of its Google Maps tool. The New York Times reported last week that some companies have been complaining that their businesses are being erroneously listed as “permanently closed” on Google Maps and Google Places and that their attempts to remedy the situation do not last. Google has been allowing users to mark businesses as closed without vetting the changes. Google Maps includes a “Not True” button, the Times reports that those abusing this feature are persistent enough to make it appear as though targeted businesses have shut their doors.

-A federal appeals court on Tuesday ordered the Justice Department to turn over information about cases where the government accessed cell phone location data without a warrant, The Hill's Brendan Sasso reports. The court's decision was a victory for the American Civil Liberties Union, which first requested the information four years ago. A three-judge panel of the U.S. Court of Appeals for the District of Columbia ordered the Justice Department to reveal the names and docket numbers of cases that resulted in a conviction or guilty plea in which the government accessed location data. The court did not grant the ACLU's request to reveal information about cases that did not result in a conviction.

The decision comes as Microsoft faces a lawsuit about the privacy issues surrounding its use of location tracking features in Windows Phone 7. The Guardian writes that Microsoft tracks the location of its mobile users even after customers turned the software off, a lawsuit filed on Wednesday alleges. The legal action claims that owners of Windows Phone 7 smartphones are being unwittingly tracked when the camera on their phone is switched on. The lawsuit, filed in a Seattle federal court, claims that Microsoft collects data about the whereabouts of its users even after customers have opted out of location tracking.

-Ten years after the terrorist attacks of Sept. 11, 2001, the nation faces a critical threat to its security from cyberattacks, a new report by a bipartisan think tank warns. ComputerWorld writes that the report, released by the Bipartisan Policy Center's National Security Preparedness Group (NSPG), offers a broad assessment of the progress that the public sector has made in implementing the security recommendations of the 9/11 Commission. The comments about cybersecurity are part of broader discussion on nine security recommendations that have yet to be implemented.

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.