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

GW CSPRI Newsletter

September 19, 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. 19-20, **Military Electronic Health Record Systems (EHRS): Where Do We Stand?** This conference brings together experts from government and industry who are defining and developing the solutions to these and other issues, and who are modernizing the military Healthcare IT infrastructure. Holiday Inn Rosslyn at Key Bridge, 1900 N Fort Myer Drive, Arlington, Va. 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 Alperovitch and SCADA expert Langner 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.

-Sept. 20-22, The National Institute of Standards and Technology (NIST) is hosting the second annual **National Initiative for Cybersecurity Education (NICE) Workshop** at its Gaithersburg, MD campus. NICE is a national campaign focused on enhancing the overall cybersecurity posture of the United States by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population. The theme of the 2011 Workshop is "Shaping the Future of Cybersecurity Education – Engaging Americans in Securing Cyberspace." This event opens discussions around the three goals: 1. Raise awareness among the American public about the risks of online activities; 2. Broaden the pool of skilled workers capable of supporting a cyber-secure nation; and 3. Develop and maintain an unrivaled, globally competitive cybersecurity workforce. Registration is now closed but one can attend some sessions via webcast.

-Sept. 22, 8:00 a.m. - 10:00 a.m., **An FBI Briefing of the Cyber Threat to Our Critical Infrastructure in the 21st Century** - This presentation will focus on the cyber threat to our critical infrastructure. The guest speaker, Steven R. Chabinsky, will discuss how cyber threats continue to evolve, foreign vs. domestic threats, and international law. ICF International, 1725 I St. NW. More information.

-Sept. 23, 10:00 a.m. - 11:00 a.m., **Cybersecurity for Electrical Cooperatives** - The National Electric Sector Cybersecurity Organization (NESCO) has performed a demonstration project in partnership with AlienVault, Tofino Security, N2NetSecurity, and Trusted Metrics to provide Electric Cooperatives with proven, incremental guidelines for addressing cybersecurity. In this webinar the process and results are described by NESCO, AlienVault, Trusted Metrics, and subject co-operative staff involved in organizing and performing the project. More information http://cyber4co-ops.eventbrite.com/.

-Sept. 27, 8:30 a.m. - 5:00 p.m., **2nd Annual Cybersecurity Summit** - Some of the industry's leading experts and government insiders discuss vital strategies, tactics, and tips for protecting both government and private-industry cyber infrastructure. 1777 F. St. NW. More information.

-Sept. 27, 2:00 p.m., **Securing the Government's Domain Name System with DNSSEC** - The White House issued a mandate for all federal agencies to implement Domain Name System Security – otherwise known as DNSSEC. This Webinar is about what it takes to implement DNSSEC and the value it brings to securing Internet infrastructure and enabling the business of government. More information.

-Sept. 28, 8:00 a.m. - 5:00 p.m., **FedCyber.com Government-Industry Summit** - This conference will focus on crafting action-oriented strategies that will help the federal and security

community shape models for the next decade of national cyber defense. This event is free for government cyber practitioners. Newseum, 555 Pennsylvania Ave. NW. More information.

Current Research

Associated CSPRI researchers have produced numerous papers over the past year. Claire Monteleoni (with Kamalika Chaudhuri and Anand Sarwate) has written about differentially private empirical risk minimization. Hoeteck Wee has researched threshold and revocation cryptosystems via extractable hash proofs. Nan Zhang (with Xin Jin, Aditya Mone, and Gautam Das) has written about randomized generalization for aggregate suppression over hidden web databases. For links to these and other works, see the CSPRI website.

Legislative Lowdown

-A bill introduced by Senator Richard Blumenthal (D-Conn.) would punish companies that are careless with customers' information. The Personal Data Protection and Breach Accountability Act of 2011 (PDF) would introduce regulations for companies that store online data for more than 10,000 people. The New York Times reports that the rules would require companies to follow specific data storage and protection guidelines, and those who violate the terms would be subject to stiff fines.

Cyber Security Policy News

-The White House is rolling back security reporting requirements for federal agencies. Since 2002, federal agencies have been required to catalog key information assets and to produce annual reports about security incidents and protections against hackers and malicious software. The old guidelines, spelled out in the nearly 10-year-old Federal Information Security Management Act (FISMA) have long been criticized as ineffective—good at producing expensive reports and lucrative contracts for audit companies, but little in the way of progress on better securing federal agencies against cyberattacks and data theft. New government wide procedures place emphasis on continuous monitoring, tracking and testing of agency networks and assets, NextGov reports.

-The Federal Trade Commission is proposing changes to online privacy rules for children, according to the Seattle Post Intelligencer. The proposed amendments to the Children's Online Privacy Protection Rule (COPPA) would expand the definition of personal information to include geolocation data and tracking cookies used by behavioral advertisements. They would also streamline the parental notice sites must give before collecting minors' information. The FTC is seeking public comment on the proposed new rules.

-Online attacks that steal financial information or target U.S. financial institutions are increasingly sophisticated and effective, federal officials told the House Financial Services panel last week. The Hill reports that the hearing comes as House Republicans are mulling their

response to the comprehensive cybersecurity proposal unveiled by the White House in May. Senate Democrats have been hammering out the details of their own proposal in recent months, after settling a standoff over jurisdiction earlier this year. Both parties have framed cybersecurity as critical to both national security and the economy, making it likely that some sort of package will reach the floor in both chambers this fall.

-Google says people will soon be able to opt-out of the company's Wi-Fi mapping efforts. Didn't know Google was mapping the precise location of your home network? The search giant has been harvesting information and mapping wireless access points via its constantly roving fleet of Street View cars and trucks. That means the same cars that take photos of your front door and make them available via Google Maps may allow Google to map your wireless router to that location as well. The move comes thanks to complaints from privacy advocates in Europe, writes Steven J. Vaughan-Nichols for ZDNet.

-Microsoft said last week that the next version of its Windows operating system -- Windows 8 -- will ship with anti-virus software built-in. Expected to be released the third quarter of 2012, Windows 8 will include the functionality offered by Microsoft Security Essentials, a program that is currently offered as a separate, free online download to protect against viruses and other cyber threats. SC Magazine writes that the move could help Microsoft better protect its customers, but it could also gain the interest of antitrust regulators, if the established anti-virus industry -- which now sports more than 50 anti-virus vendors, raises a stink over the move.

-A new report finds that the United States needs better cyber intelligence. That conclusion, from a report (PDF) issued by the Intelligence and National Security Alliance, says the United States must develop cyber intelligence that can better predict and stop computer-related threats.

-The Health and Human Services department has awarded a $40 million cybersecurity contract to provide cybersecurity operational support services to the Computer Security Incident Response Center at HHS. The five-year contract was awarded to Merlin International, a veteran owned business that provides IT services to the 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.