GW CSPRI Newsletter

October 22, 2012

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.

Events

-Oct. 22-23, **Cybersecurity Conference** - The 2012 Cybersecurity Conference is co-located with the 2012 Cloud and Virtualization Conference and Government Mobility Conference. Full conference attendees benefit from exclusive access to all three conferences. Expo only attendees will have access to the co-located Cybersecurity, Cloud & Virtualization, and Mobile Government Expo with free education sessions taking place right in the exhibit area. Grand Hyatt Washington, 1000 H Street NW. More information.

-Oct. 24, 10:00 a.m. -11:30 a.m., **Protecting Your Data in the Cloud** - This seminar is offered as part of GWU's observation of Cybersecurity Awareness Month. Marvin Center room 413/414. 800 21st Street, NW.

-Oct 24, 11:00 a.m., **The Battle for Control of Online Communication** - The George Washington University Department of Computer Science and the Cyber Security Policy and Research Institute is co-hosting a Colloquium on Wednesday by Nick Feamster of University of Maryland and Georgia Tech. Dr. Feamster will discuss a study of the network-level behavior of spammers, present a spam filtering system that classifies e-mail message based on the network-level traffic characteristics rather than the contents of the message. He will also describe emerging threats concerning domain name registration and methods to ascertain the legitimate reputation of domain names. Approaches to monitor and circumvent attempts to restrict and manipulate access to online information will also be discussed. Refreshments will be provided. Academic Center, 801 22nd St. NW, Computer Science Conference Room 736.

-Oct 24, 6:30 p.m. - 8:00 p.m., **Journalists' Digital Security** - What would you do if you found your computer had been hacked and sensitive emails with sources, story research and interview notes were now exposed? Or what if you learned someone had intercepted your cell phone conversations and used them to learn the identity of your would-be 'Deep Throat?' To raise awareness about just how serious the digital security problem is, the National Press Club's Press Freedom Committee will hold a panel discussion. This event is free and open to the public. National Press Club. 529 14th St. NW,, 13th Fl. More information.

-Oct. 24-25, **SINET D.C. Showcase & Workshops** - A chance to meet and listen to some of the nation's top cybersecurity leaders. The theme of the conference is finding ways to advance cybersecurity innovation through public-private partnerships. Keynotes include talks from U.S. Director of National Intelligence Stephanie O'Sullivan, White House Cybersecurity Coordinator Michael Daniels, and AT&T CSO Dr. Edward Amoroso. National Press Club, 529 14th Street, N.W., 13th Floor. More information.

-Oct. 25, 8:30 a.m. - 12 noon, **Building a Cyber Security Workforce Through Diversity** - An event focused on the importance of diversity in building the cyber security workforce of the future, with a specific focus on women. This half-day event will include a panel of experts from multiple sectors and will feature a keynote address by Janet Napolitano, Secretary of the Department of Homeland Security. CSIS 1800 K. St. NW. More information.

-Oct. 25, 9:30 a.m. - 5:30 p.m., **American the Virtual: Security, Governance and Interoperability in an Interconnected World** - American University Law Review's Cybersecurity Law Symposium presents a discussion for government officials, industry representatives, legal practitioners, and academic experts on the legal implications of cybersecurity threat responses such as regulation, standard setting, agency interactions, breach disclosures, and monitoring. at the Fulbright Conference Center of Hogan Lovells US LLP. Registration required. More information (PDF).

-Oct. 25 12:00 noon - 1:30 p.m., **Revising COPPA: A Discussion of the FTC's Proposals** - The Information Technology and Innovation Foundation (ITIF) will host a panel discussion on the Federal Trade Commission's proposed changes to the Children's Online Privacy Protection Act. The speakers will include Dan Castro of the ITIF; Emma Llanso, policy counsel, Center for Democracy & Technology; Morgan Reed, executive director, Association for Competitive Technology; Berin Szoka, president, Tech Freedom; and Stephen Balkam, chief executive officer, Family Online Safety Institute. This event is free and open to the public, and will be Webcast. Lunch will be served. ITIF, Suite 610A, 1101 K St., NW.

-Oct. 30, 12 noon - 1:00 p.m., **Cyber Security & Transformational Technologies: Keeping Systems and Data Safe** - This webcast will explore the results of the research, including how government is managing cyber security priorities and where they are investing limited funds to

keep their systems and data safe while serving the needs of their agencies. More information. Speakers include Scott Andersen, director of secure cloud computing strategies Lockheed Martin Information Systems & Global Solutions, and Cynthia Poole, director of research services, Market Connections. More information.

-Oct. 30-Nov. 1, **NICE Workshop Shaping the Future of Cybersecurity Workshop Connecting the Dots in Cyberspace** - The NICE Initiative is 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 2012 Workshop will focus on Connecting the Dots between Government, Academia, Industry and the Public in the cybersecurity education arena. NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD. More information.

-Oct. 31, 8:00 a.m. - 12:00 p.m., **Washington Post Cybersecurity Summit** - This Washington Post Live forum on cybersecurity will bring together leading experts to discuss the increasingly sophisticated attacks against business and government data and how to better protect it. The event is sponsored by the GW Cyber Security Policy and Research Institute.

Confirmed speakers include *Janet Napolitano, U.S. Secretary of Homeland Security; General James Cartwright, former Vice Chairman of the Joint Chiefs; William Lynn III, former US Deputy Secretary of Defense; Linda Cureton, CIO, NASA; Steven Bucci, Senior Research Fellow, Heritage Foundation; Albert Kinney, Director at U.S. Public Sector Hewlett-Packard Company; Jim Lewis, Senior Fellow, Center for Strategic and International Studies; Lena Smart, CSO, New York Power Authority; Raphael Mudge, Founder, Strategic Cyber LLC.* The Washington Post, 1150 15th St NW. More information.

-Oct. 31, 7:30 a.m. - 9:30 a.m., **Leveraging Public-Private Partnerships to Protect Critical Infrastructure** - This two-hour event will cover a number of topics, including how cyber information sharing between the public and private sector can work under existing authorities, and how a collaborative approach to cyber standards - heavily involving industry - can be effective. Speakers include Lisa Kaiser, program manager, Control Systems Cybersecurity Standards and Tools, Department of Homeland Security; and Mark Engels, enterprise technology security and compliance director, Dominion. National Press Club, 529 14th Street NW. More information.

Announcements

-Carl Landwehr, Lead Research Scientist at the SEAS Cyber Security Policy and Research Institute, was inducted into the national Cyber Security Hall of Fame at a ceremony in Baltimore on October 17. More on Carl and his accomplishments are on its site and the CSPRI site.

Congratulations, Carl!

Legislative Lowdown

-A new White House executive order would direct U.S. spy agencies to share the latest intelligence about cyberthreats with companies operating electric grids, water plants, railroads and other vital industries to help protect them from electronic attacks, according to The Associated Press. The seven-page draft order, which is being finalized, takes shape as the Obama administration expresses growing concern that Iran could be the first country to use cyberterrorism against the United States. The military is ready to retaliate if the U.S. is hit by cyberweapons, Defense Secretary Leon Panetta said. But the U.S. also is poorly prepared to prevent such an attack, which could damage or knock out critical services that are part of everyday life. The White House declined to say when the president will sign the order. The draft order would put the Department of Homeland Security in charge of organizing an information-sharing network that rapidly distributes sanitized summaries of top-secret intelligence reports about known cyberthreats that identify a specific target.

Cyber Security Policy News

-Computerized hospital equipment is increasingly vulnerable to malware infections, according to participants in a recent government panel. These infections can clog patient-monitoring equipment and other software systems, at times rendering the devices temporarily inoperable, MIT's Technology Review reports.

At the same time, the U.S. Food and Drug Administration is looking for ways to improve how it tracks medical device safety and security issues, such as malware risks, according to GovInfoSecurity.com. The FDA has taken into account the findings of a recent Government Accountability Office report that recommended the FDA develop a plan to improve post-market surveillance of information security issues in medical devices.

The renewed interest in the topic comes as security researchers are demonstrating new techniques that could turn medical devices into a deadly weapon. At a security conference in Australia earlier this month, IOActive researcher Barnaby Jack demonstrated how Pacemakers could be infiltrated to deliver deadly shocks. SC Magazine writes that Jack used a laptop to send a series of 830-volt shocks to a remote pacemaker, and used some sort of unclear “secret function” the pacemakers possess, which could be used to activate all pacemakers and implantable defibrillators within a 30-foot radius. The devices would give up their serial numbers, which would allow the would-be assassin to breach their firmware and upload nefarious malware that could spread to other pacemakers like a virus. The devices could also

give up personal data, and even supposedly secure data from the manufacturer.

- An expanded information-sharing program will potentially allow more than 2,600 defense suppliers access to top-secret Pentagon communications with select companies about indications of cyber threats, partly by adding context understandable to a wider audience. NextGov reports that the defense industrial base collaboration initiative started as a pilot program during summer 2011. In May, the Pentagon allowed the whole industry to join. Participants receive disclosures when the military detects signs of unfolding malicious campaigns so that their in-house technical teams can take protective measures. The Defense Department also distributes reports about breaches participating companies have suffered, after deleting identifying information to avoid exposing the weaknesses of competitors. Around the time the initiative began ramping up, the General Services Administration signed a deal with Lockheed Martin Corp. worth up to $454 million for help running the Defense Cyber Crime Center, or DC3, which operates the program.

-The Federal Trade Commission (FTC) is challenging citizens to create solutions that will block illegal robocalls. According to robocall.challenge.gov, these solutions should block robocalls on landlines and mobile phones and can operate on a proprietary or non-proprietary device or platform. Entries can be proposed technical solutions or functional solutions and proofs of concept. The vast majority of telephone calls that deliver a prerecorded message trying to sell something to the recipient are illegal. As technology has advanced over the years, so have the number of illegal robocalls. The winning solution will win $50,000 in cash, as well as opportunities for promotion, exposure, and recognition by the FTC. Solvers will retain ownership of their solutions. Companies with over 10 employees will be eligible to compete for the Federal Trade Commission Technology Achievement Award, which does not include a cash prize. For more information about prizing please see the Official Rules.

-A long-planned anti-piracy measure will be rolling out over the next few weeks for customers of some of America's largest Internet service providers. Back in July 2011, a coalition of U.S. Internet providers -- including AT&T, Verizon, Comcast, Cablevision, and Time Warner Cable -- signed on to an agreement to crack down on online copyright infringers. Or, well, to "crack down." The terms of the agreement emphasized user education over user punishment: Instead of cutting infringing users off from Internet services, the providers dreamed up a "six strikes" approach to infringement notification: Copyright holders would do their standard scanning for infringement. They would then cross-reference suspect IP addresses against the ISPs that control them. The copyright holders would then send a message to infringers -- and, under the agreement, the ISPs would in turn commit to forwarding those messages to their customers. For up to six of those messages. The agreement's goal, Ars Technica noted at the time, was to "educate and stop the alleged content theft in question, not to punish. No ISP wants to lose a customer or see a customer face legal trouble based on a misunderstanding, so the alert system provides every opportunity to set the record straight." But according to a report in The Hill, the infringement alert system will be implemented "over the next several weeks."

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.