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

GW CSPRI Newsletter

October 17, 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

-Oct. 16-18, 9:00 a.m. - 5:00 p.m., **5th Transatlantic Market Conference** - This conference will provide a platform for an international cyber security dialogue to raise awareness on the need to act immediately, focus on new ways and technologies for protecting information technology systems and intellectual property. Speakers include Jeffrey Moss, professional hacker, chief security expert for ICANN, and founder of Black Hat and DEFCON; Melissa Hathaway, president, Hathaway Global Strategies LLC; David Kappos, undersecretary of commerce for intellectual property, U.S. Department of Commerce; and Terry Gudaitis, cyber intelligence director, Cyveillance Inc. Cannon House Office Building and Convention Center, Capitol Hill. More information.

-Oct. 17-18, 9:00 a.m. - 5:00 p.m., **The U.S. - China Economic and Security Review Commission** - The commission will hold one of a series of public meetings to consider drafts of material for its 2011 Annual Report to Congress. The topics to be considered in these meeting include "intellectual property protection and its 5-year plan, technology transfers, and outsourcing," and "China's foreign and regional activities and relationships, including those pertaining to Taiwan and Hong Kong." Conference Room 231, Hall of the States, North Bldg., 444 North Capitol St., NW. More information.

Oct. 18, 11:30 a.m. - 2:30 p.m., **Building a Better Internet: A Verisign Research Symposium**- An Internet infrastructure grant forum lunch hosted by Verisign. The following selected researchers will discuss their work, results, and future considerations for research: Shlomi Dolev, Ben-Gurion University of the Negev, will address "Internationalization of the Internet"; Anil Madhavapeddy, University of Cambridge, will address "Domain Name System (DNS) Security"; Brighten Godfrey, from University of Illinois at Urbana-Champaign, will address "infrastructure Applications"; Morley Mao, from University of Michigan, will talk about "Internet Infrastructure"; Chris Anderson, editor of Wired magazine, will address "The Long-Tail: Why the Future of Business is Selling Less of More"; and Anitesh Barua will address Verisign's contributions. Newseum, Knight Conference Center, 555 Pennsylvania Ave., NW. More information.

-Oct. 18, 7:30 a.m. to 3:00 p.m., **Symposium on Business Globalization: Managing the Cyber Security Challenge** - The George Mason University School of Management will hold a day-long symposium including keynotes from Gen. Michael Hayden, former director of the Central Intelligence Agency and visiting professor, George Mason University School of Public Policy; and Fareed Zakaria, CNN host, editor-at-large for TIME, and columnist for The Washington Post. The Ritz-Carlton, Tysons Corner, 1700 Tysons Blvd., McLean, Va. More information.

-Oct. 18-19, **Online Trust Forum 2011** - The Online Trust Alliance will hold a two-day forum on consumer security and privacy. Speakers include Ron Plesco, president and chief executive at the National Cyber-Forensics & Training Alliance; Ari Schwartz, senior adviser for Internet policy, National Institute for Standards and Technology; Leslie Harris, president and chief executive, Center for Democracy & Technology; Hon. Rick Boucher, partner, Sidley Austin, former congressman in the House; Genie Barton, vice president of the Council for Better Business Bureaus; and Julie Brill, commissioner, Federal Trade Commission. Washington Plaza Hotel, 10 Thomas Circle NW. More information.

-Oct. 20-21, **ISSA International Conference** - This second annual event will feature several talks by several noted security experts from around the world, including Shawn Henry of the FBI on "the case for two Internets"; General Keith B. Alexander of USCYBERCOM/NSA on national cybersecurity strategy and policy; Jeff Moss of BlackHat on his new role as CSO for ICANN; Kevin Mandia, forensics expert; Kazuki Yonezawa of Symantec on security and business continuity efforts for the Japanese earthquake; Christopher Pearson of Royal Bank of Scotland privacy expert on the three most common data breaches. Baltimore Convention Center, One West Pratt Street, Baltimore, Md. More information.

Announcements

-Cryptography and molecular biology share certain aspects and operations that allow for a set of unified principles to be applied to problems in either venue. A recently published paper (Genomics-based Security Protocols: From Plaintext to Cipherprotein) on this topic by Prof. Hermann Helgert, Adjunct Professor Sayed Hussein, and graduate student Harry Shaw of the Department of Electrical and Computer Engineering, won a "Best Paper" award at the IARIA conference in Valencia, Spain in September 2010. This paper demonstrates a practical path to a composable, standardized biological internet security protocol that encompasses biological and computing domains.

-David Alan Grier, associate professor of international science and technology policy at GW, has been voted IEEE Computer Society 2012 president-elect. The Computer Society is the largest unit of the Institute of Electrical and Electronics Engineers (IEEE), which is the world's largest professional technical body. A member of CSPRI's Advisory Board, Prof. Grier teaches the cornerstone course in the International Science & Technology Policy Program. He writes the column and blog "The Known World" for IEEE Computer and has served as the editor-in-chief of the IEEE Annals of the History of Computing. He has written three books: Too Soon To Tell, When Computers Were Human, and The Company We Keep.

Legislative Lowdown

-The future of the Homeland Security Department's cybersecurity office is up in the air, according to NextGov. The House Homeland Security Committee last week approved H.R. 3116, by a party line vote of 19-13. Democratic members, in a report prepared by their staff, argued the measure "does not authorize this directorate, even as the issues of infrastructure protection and cybersecurity have emerged as critical concerns." The full House is poised to vote on the measure that would not create a permanent Homeland Security Department cybersecurity office, after a committee on Thursday passed authorization legislation that does not mention the program. The move represents a departure from the Senate's version of the bill, which would retain and rename the office to better reflect a new focus on safeguarding critical commercial sectors, including information technology.

-Rep. Mary Bono Mack (R-Calif.), chairman of the House Energy and Commerce's subcommittee on Commerce, Manufacturing and Trade, said last week that she is seeking the attention of full Committee Chairman Fred Upton (R-Mich.) to move forward with her data security bill. The Secure and Fortify Electronic (SAFE) Data Act (PDF) would establish a national standard for when companies are required to notify consumers that their personal information has been breached.

-A new resource from the CipherLaw Group aims to provide up-to-date information on the status of cybersecurity legislation pending in the House and Senate. The Cybersecurity Legislation Tracker is currently following two dozen pending bills before both houses of Congress, including

a brief synopsis of each, its cosponsors, a link to the latest text of the legislation, and its progress through each chamber.

Cyber Security Policy News

-The Securities and Exchange Commission is pressing for more disclosure, issuing new guidelines this week that make clear that publicly traded companies must report significant instances of cybertheft or attack, or even when they are at material risk of such an event, Reuters reported last week. The guidance, posted late on Thursday by the U.S. Securities and Exchange Commission, lays out examples of things that companies may be required to disclose. The guidance comes after Senator John Rockefeller asked the SEC to issue it amid concern that companies were failing to mention data breaches in public filings. The SEC said in its guidance that if a cyber event occurs and leads to losses then companies should "provide certain disclosures of losses that are at least reasonably possible."

The guidelines come as the SEC itself is reeling from a new data breach affecting its own staffers. Last week, the commission warned staffers that their personal brokerage account information may have been compromised, after it uncovered security flaws with an ethics compliance program. In an October 7 letter to SEC employees, Chief Information Officer Thomas Bayer said that the contractor hired to operate a computer program that tracks trades had violated its agreement with the SEC by providing names and account numbers to a subcontractor without permission. The contractor, Financial Tracking Technologies LLC, was selected by the SEC in the second quarter of 2009 to set up the new ethics system.

-Congress is curious to know about the potential privacy impacts of Amazon's new Silk Web browser, writes Ars Technica. At a privacy hearing last week, Rep. Joe Barton (R-TX) expressed outrage at the way Silk's 'split' design can funnel all user browsing data through Amazon's backend servers. "My staff yesterday told me that one of our leading Internet companies, Amazon, is going to create their own server and their own system and they're going to force everybody that uses Amazon to go through their server and they're going to collect all this information on each person who does that without that person's knowledge. Enough is enough." Rep. Ed Markey (D-Mass.) also sent a letter (PDF) to Amazon CEO Jeff Bezos about the same privacy concerns. "Consumers may buy the new Kindle Fire to read 1984, but they may not realize that the tablet's 'Big Browser' may be watching their every keystroke when they are online," Markey said in a statement.

-Squabbling on Capitol Hill isn't anything new, but cyber threats spanning sectors and disciplines are growing and time is running out for the current Congress to pass laws to address the critical need, according to a panel of Hill staffers and cybersecurity experts, says Federal Computer Week's Amber Corrin. "Several federal agencies, including the White House, Homeland Security and the Defense and Energy departments, have put forth their own cyber policies and reviews, but now, investment in more than rhetoric is becoming acutely necessary," Corrin wrote.

-The computer virus that hit the Pentagon's Predator drone program last month was not directed at the military systems but was common malware used to steal log-ins and passwords used in online gaming, the Associated Press reports. According to Air Force Space Command, the virus did not get into the flight controls for the drones, which are flown remotely by pilots at Creech Air Force Base in Nevada. Instead, it got into ground control systems that run backup power supplies, environmental controls and work stations.

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.