GW CSPRI Newsletter

January 22, 2013

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

Events

Legislative Lowdown

Cyber Security Policy News

CSPRI Publications

Events

-Jan. 23, 5:00 p.m. - 7:00 p.m., **ISSA Baltimore Meetup** - A gathering of the Baltimore chapter of the Information Systems Security Association. The scheduled speaker is Dan Wiley, senior security consultant, Checkpoint Software Technologies. Concurrent Technologies Corporation, 8530 Corridor Road, Savage, MD, 20763. More information.

-Jan. 23, 12:00 p.m. - 2:15 p.m., **Communications Law and Policy in the Digital Age: The Next Five Years** - The Free State Foundation will host an event to discuss the recently published book by the same name. The speakers will include four of the contributing authors: Christopher Yoo, professor, University of Pennsylvania Law School; Daniel Lyons, professor, Boston College Law School; Ellen Goodman, professor, Rutgers School of Law, and Seth Cooper, author of the chapter titled "Restoring a Minimal Regulatory Environment for a Healthy Wireless Future." National Press Club, 529 14th St. NW, 13th Floor. More information (PDF).

-Jan. 22-23, **9th Annual State of the Net Conference** - The State of the Net Conference is the largest information technology policy conference in the U.S. and the only one with over 50 percent Congressional staff and government policymakers in attendance. This year's conference will feature a keynote luncheon discussion between Travis Kalanick, CEO & Co-Founder, Uber, and Congressman Bob Goodlatte (R-VA), Co-Chair, Congressional Internet Caucus. Hyatt Regency, 400 New Jersey Ave. NW. More information.

-Jan. 24, 6:00 p.m. - 7:00 p.m., **America the Cyber-Vulnerable** - CSPRI and GW's Computer Science Department are sponsoring a talk by Joel Brenner, former senior counsel at the National Security Agency. This event will be open to the public, and the topic of discussion will be the new faces of cyber-security threats, and what these threats mean to government, businesses, and the public. Computer Science Department Conference Room 736, Phillips Hall, 801 22nd Street, NW. More information (PDF).

-Jan. 24, 6:30 p.m. - 8:00 p.m., **Communications and Technology Policy in the 113th Congress** - The Federal Communications Bar Association Legislative Committee will host an event. The participants will include House and Senate staff. Georgetown University law school, Gewirz Student Center, 12th Floor, 120 F St., NW. More information.

-Jan. 31, 12:30 p.m., **A Conversation on Internet Freedom** - George Washington University Law School is partnering with Microsoft Corporation to host a conversation with the former Cybersecurity Coordinator of the Obama Administration, Howard A. Schmidt. This talk will highlight the role cybersecurity plays in Internet Freedom. Microsoft Innovation and Policy Center, 11th Floor, 901 K Street NW. More information.

-Jan. 31, 7:00 p.m. - 10:00 p.m., **CharmSec Meetup** - Part of the CitySec movement, this is a monthly informal meetup of information security professionals in Baltimore. Heavy Seas Alehouse, 1300 Bank Street, Baltimore, MD, 21231. More information.

Legislative Lowdown

-Rep. Zoe Lofgren (D-Calif.) has drawn up a new bill called "Aaron's Law" to amend the US Computer Fraud and Abuse Act used to prosecute Swartz until his death last week, The Register reports. Internet prodigy Swartz, 26, took his life on last week in the midst of a lengthy computer fraud case against him. The charges were brought after he copied 4.8 million scientific articles from the nonprofit journal archive JSTOR to allegedly redistribute online. In the days after he was found dead at his New York home on Friday, Swartz's family said their son's suicide was "the product of a criminal justice system rife with intimidation and prosecutorial overreach". Her bill, titled "Aaron's Law," would specify that violating a company's terms of service agreement does not constitute criminal hacking under the law.

-Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.) said last week that he will renew his push for legislation that would require police to obtain a warrant before reading people's emails, Facebook messages and other forms of electronic communication, The Hill reports. Leahy said that his desire to pass the legislation, which would amend the Electronic Communications Privacy Act (ECPA), is one of the reasons he decided to stay on as chairman of the Judiciary Committee in the new Congress.

Cyber Security Policy News

-Google engineers outlined a new scheme to help eliminate passwords. In this month's engineering journal IEEE Security & Privacy Magazine, Google's security team outlines a new ring-finger authentication system that can allow users to log in to their accounts with a simple tap of a ring on their finger against a computer. According to Wired.com, they're experimenting with new ways to replace the password, including a tiny Yubico cryptographic card that — when slid into a USB (Universal Serial Bus) reader — can automatically log a web surfer into Google. They've had to modify Google's web browser to work with these cards, but there's no software download and once the browser support is there, they're easy to use. You log into the website, plug in the USB stick and then register it with a single mouse click.

-Researchers at Russian security firm Kasperksy Labs published findings last week about a massive cyberspying network driven by sophisticated malicious software that infected hundreds of computer networks in diplomatic, governmental, and scientific research organizations around the world. The malware campaign, dubbed by Kaspersky as "Red October," is one of the most advanced espionage platforms ever discovered, the company claims. Ars Technica writes that the malware network's operators had more than 1,000 modules at their disposal, allowing them to craft highly advanced infections that were tailored to the unique configurations of infected machines and the profiles of those who used them. Most of the tasks the components carried out—including extracting e-mail passwords and cryptographically hashed account credentials, downloading files from available FTP servers, and collecting browsing history from Chrome, Firefox, Internet Explorer, and Opera—were one-time events. They relied on dynamic link library code that was received from an attacker server, executed in memory, and then immediately discarded. That plan of attack helps explain why the malware remained undetected by antivirus programs for more than five years.

-Proposed legislation in the European Union would force tech companies that have access to user data — such as Facebook, Google, and Microsoft — to report any security breaches to local cybersecurity agencies, the Financial Times reported last week. This is the European Commission's effort to make private companies accountable for privacy and security problems, European Commission Vice President Neelie Kroes told the Financial Times. If passed, the measure would require each of the EU's 27 member states to set up local cybersecurity agencies to implement security standards on online networks. Social networks, e-commerce companies, and large online platforms that have access to users' data would all have to report any server issues and security breaches to these agencies, or face sanctions.

-Security experts in Poland on Thursday quietly seized domains used to control the Virut botnet, a huge army of hacked PCs that is custom-built to be rented out to cybercriminals. NASK, the domain registrar that operates the ".pl" Polish top-level domain registry, said that on Thursday it began assuming control over 23 .pl domains that were being used to operate the Virut network. The company has redirected traffic from those domains to sinkhole.cert.pl, a domain controlled by CERT Polska — an incident response team run by NASK. The company says it will be working with Internet service providers and security firms to help alert and clean up affected users. "Since 2006, Virut has been one of the most disturbing threats active on the Internet," CERT Polska wrote. "The scale of the phenomenon was massive: in 2012 for Poland alone, over 890 thousand unique IP addresses were reported to be infected by Virut."

-Chinese tech giant Huawei on Monday criticized U.S. claims the company might be a security risk as trade protectionism that harms consumers. The Associated Press writes that the comments came as Huawei Technologies Ltd., a maker of network switching gear and smartphones, disclosed details of its 2012 performance in an effort to show transparency and allay security concerns. In October, a U.S. congressional panel recommended phone carriers avoid doing business with it or its smaller Chinese rival, ZTE Corp. Beijing rejected the report as false and an effort to block Chinese companies from the U.S. market. The U.S. and Australian actions highlight concern about Beijing's cyber warfare efforts, a spate of hacking attempts aimed at Western companies and the role of Chinese equipment providers, which are expanding abroad.

-A top cybersecurity official at the U.S. Department of Homeland Security is leaving his post after just nine months in the position, Federal News Radio reports. Mike Locatis, the assistant secretary for the Office of Cybersecurity and Communications (CS&C), stepped down effective last week. DHS Undersecretary Randy Beers, in a letter to employees, didn't give a reason for Locatis' departure, but wrote that he's disappointed to see Locatis leave the department for Colorado, where his family lives. Locatis, in Washington for the past three years, served as chief information officer at the Energy Department before joining DHS last spring.

CSPRI Publications

-CSPRI has published a research note titled Square Routed: How QR-Codes and URL Shorteners Expand our Digital Vulnerability. Evan Sills, Lance J. Hoffman, and Costis Toregas explore the growing threat from QR (quick-response) codes and other shortened or hidden URLs, which may be used maliciously to "bypass the human responses and social defenses that society has slowly built up to suspicious links and e-mails."

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.