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

GW CSPRI Newsletter

January 10, 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

-Jan 11, 5:00 - 7:00 p.m., **The Center for Democracy and Technology**'s Internet Caucus Advisory Committee will host an event titled "14th Annual Tech Exhibition and Reception". Room 902, Hart Building. More information.

-Jan. 12, 6:00 - 8:15 p.m., **Major International Privacy Developments and the Impact on Multi-National and Globally Networked Environments** - The Federal Communications Bar Association hosts the event. Bingham McCutchen LLP, 2020 K Street, NW. Registration deadline Jan. 10.

-Jan. 12-14, **Social Media Legal Risks and Strategy Conference** - Join 16 lead counsels from Coca-Cola North America, IBM Corporation, Wal-Mart, Chevron, T-Mobile, Capital One, Dell, Aon Corporation, CSC, Nationwide, and other fortune 500 companies as they discuss strategies to address and overcome the legal risks posed by engaging in social media. More information, registration.

-Jan. 13, 5:30 - 7:30 p.m., **Was Orwell Right? The Dark Side of the Internet** - The New America Foundation will host a lecture by **Evgeny Mozorov**, the author of The Net Delusion: The Dark Side of Internet Freedom. More information. 1899 L St. NW, Suite 400.

-Jan. 18-19, **7th Annual State of the Net Conference** - This year's conference will celebrate "15 Years of Internet Policy," marking not only the 15 year anniversary of the Congressional Internet Caucus itself but also 15 years of 42 U.S.C. Sec 230 and the anniversaries of other Internet legislation such as the Communications Decency Act and the 1996 Telecom Act. The conference will feature discussions with leading Internet policy experts and panel tracks focusing on privacy/security, telecommunications regulation, intellectual property, and innovation. More information. Hyatt Regency Capitol Hill, 400 New Jersey Avenue, NW,

The Summer Experience, Colloquium and Research in Information Technology (SECuR-IT) is a ten-week paid internship (June 13-August 19, 2011) with academic seminars, sponsored by TRUST partners UC Berkeley, Stanford University and San Jose State University with internships located in Silicon Valley and the San Francisco Bay Area.

SECuR-IT participation is open to graduate students (M.S. & Ph.D). Participation is limited to 30 people selected from a nationwide pool of applicants, who have demonstrated, outstanding academic talent. Women and historically underrepresented ethnic minority groups will be given strong consideration although everyone is encouraged to apply.

This is an excellent opportunity for students, having an emphasis in computer security, to gain invaluable research experience working with Silicon Valley technology companies. Students will attend computer security seminars at UC Berkeley, Stanford University, San Jose State University, and at Silicon Valley industry locations.

The application deadline is February 18, 2011. Additional information can be found here.

-CSPRI Seminar Series for 2011: Details for the entire year are here.

Announcements

-CSPRI has awarded 59 full-ride scholarships to GW students since 2002 to study computer security and is now recruiting applicants for 2011-2013. Rising juniors, seniors and graduate students who are U.S. citizens can apply. Complete details are here.

Grants Received

GWU Prof. Lance Hoffman has recently been awarded a supplemental grant from the National Science Foundation Scholarship for Service program to run boot camps to inform new SFS institutional recipients about practical issues in managing their grants. The audience is principal investigators or other officials from institutions around the country who have responsibility for grant administration. Best practices and lessons learned are explained by a team of veteran mentors, principal investigators who have had SFS grants for a number of years and who have been successful in educating students in cyber security and information assurance and in placing their graduates into government service.

Legislative Lowdown

-President Obama last week signed the **America Competes Reauthorization Act of 2010**, legislation that provides for the first major reorganization of the **National Institute of Standards and Technology** in a generation. The law directs NIST to collaborate with industry to develop cloud computing standards, formalizing NIST's cloud computing activities begun in the past two years. Another provision of the act gives the NIST director a promotion, to undersecretary of commerce for standards and technology, writes GovInfoSecurity.com. Along with NIST, the law details new programs and responsibilities for the National Science Foundation, the Energy Department, and the White House Office of Science and Technology Policy, **Federal News Radio** notes.

-While talk about improving the economy and fiscal responsibility is likely to dominate the early days of the new Congress, lawmakers and key congressional committees are also expected to address a handful of homeland security issues through legislation and hearings in the next few months. And two of them involve technology issues, according to **NextGov**. In a Dec. 17 letter to President Obama, **Senate Majority Leader Harry Reid** said he plans to bring cybersecurity legislation to the Senate floor for consideration early in the 112th Congress. NextGov notes that Reid wants to combine cybersecurity provisions from bills written by the Senate Homeland Security and Governmental Affairs Committee and the Senate Commerce Committee, with input from lawmakers on other key panels such as Judiciary and Intelligence. "At the same time, lawmakers and the Obama administration must confront the issue of what to do with the SBInet program, which was created to build a virtual fence using technology along the southern border. About $1 billion has been spent to date," writes NextGov's Chris Strohm.

-Rep. Dan Lungren (R-Calif.), has been named chairman of the House Administration Committee and the **Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies**.

Cyber Security Policy News

-**Defense Secretary Robert Gates** recently updated his proposal to shift $100 billion in the Defense Department budget to help fund the dual-front war, identifying an additional $78 billion in cuts that will be put toward the federal deficit, including some from IT, reports Washington Technology. Gates' plan is the first stage of a three-year effort to carve away 10 percent of the staff-support contractors that DOD employs, slash $10 billion from IT expenditures and cancel some expensive weapons systems. The moves come as the Pentagon faces $13 billion less than initially planned for in the fiscal 2012 budget.

In other Defense IT news, **Defense Information Systems Agency** has created a "demilitarized zone" for unclassified applications to help manage access between the public Internet and Unclassified but Sensitive IP Router Network (NIPRNet), says Federal Computer Week..

-Military and government agencies mistakenly exposed the personal data of thousands of citizens in at least 104 incidents in 2010, up from 90 such data breaches the previous year, according a new report from the nonprofit **Identify Theft Resource Center**. Yet, far fewer personal records were released as a result -- 1.2 million in 2010, well under the 79.4 million exposed in 2009, observes NextGov's **Brian Kalish**.

-Malicious software disguised as a White House e-greeting card sent to dot-gov employees over the holidays duped many recipients into infecting their Windows computers with a virus that hoovered up gigabytes of sensitive documents, according to cybersecurity investigators. KrebsOnSecurity.com writes that among those victimized were an employee at the National Science Foundation's Office of Cyber Infrastructure, an intelligence analyst with the Massachusetts State Police, and an employee of the Financial Action Task Force, an intergovernmental body dedicated to the development and promotion of national and international policies to combat money laundering and terrorist financing. MSNBC writes that the attack bears all of the hallmarks of a group or individual that was very active in 2010 stealing secrets from government employees and contractors with the help of the ZeuS Trojan.

-The EA-18G Growler and the F-35 Joint Strike Fighter will both carry an airborne network invasion weapon, says the U.S. Navy's top intelligence official. An Aviation Week story says the "Next Generation Jammer" (NGJ) technology is part of a Navy effort from 2010 to 2020 to refocus research and development on non-kinetic capabilities like information operations, network invasion and electronic attack.

-**White House Security Coordinator Howard Schmidt** announced last week the formation of a National Program Office to oversee the administration's national strategy for trusted identities in cyberspace, ABC News Radio reports. The office will coordinate with industry to "create an online environment in which sensitive transactions are less risky."

-Assassins who killed a Hamas leader in Dubai in January 2010 used an email Trojan to track their target leading up to the hit, according to a story in the January edition of GQ

Magazine. One year ago, an elite Mossad hit squad traveled to Dubai to kill a high-ranking member of Hamas. They completed the mission, but their covers were blown, and Israel was humiliated by the twenty-seven-minute video of their movements that was posted online for the entire world to see.

-Metro area authorities are searching for clues in the baffling murder case of decorated former Army officer **John P. Wheeler**, a cybersecurity and information technology consultant whose body was found at a Delaware landfill on New Year's Eve. Five days before his body was found, Wheeler sent a longtime friend an email expressing concern that the United States wasn't sufficiently prepared for cyber warfare, the **Associated Press** writes. Wheeler's focus on computer warfare, and his ties to MITRE, have already attracted conspiracy theories involving the military industrial complex.

Meanwhile, U.K. authorities have published images of a man and a woman who may be connected to the mysterious death of a top British codebreaker, according to Wired.com. Gareth Williams, 31, was found dead and naked in a North Face duffel bag in the bathtub of his flat last August. According to reports, Williams -- described by those who knew him as a "math genius" -- worked for the U.K.'s Government Communications Headquarters (GCHQ) helping to break coded Taliban communications, among other things. He was just completing a year-long stint with MI6, Britain's secret intelligence service, when he died. The flat where he lived was part of a network of flats registered to an offshore front company and rented out to GCHQ workers.

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.