GW CSPRI Newsletter

April 23, 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.

CSPRI in the News

Prof. Lance Hoffman, CSPRI Director and principal investigator for GW's Scholarship for Service Program, was part of a CNN feature on the dearth of qualified cybersecurity workers in the U.S. See *Media Appearances* below.

Contents

Events

-Apr. 24, 2:00 p.m., **America is Under Cyber Attack: Why Urgent Action is Needed** - The House Homeland Security Committee's Subcommittee on Oversight, Investigations, and Management will hold a hearing. Room 311, Cannon House Office Building. More information.

-Apr. 24, 2:00 p.m. - 3:30 p.m., **Should I Sue? The Perils of Litigation in the Age of Anonymous** - The American Bar Association will host a webcast and telecast panel discussion. This panel will cover hacking attacks launched in retaliation for the filing of lawsuits. The speakers will include Tanya Forsheit, attorney InfoLawGroup, LLP; Marcia

Hofmann, senior staff attorney, Electronic Frontier Foundation (EFF); Steven Teppler, partner, Edelson McGuire LLC; and Gib Sorebo, chief cybersecurity technologist, SAIC. More information.

-Apr. 26, 10:00 a.m., **Iranian Cyber Threat to the U.S. Homeland** - The House Homeland Security Committee's Subcommittee on Counterterrorism and Intelligence and Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will hold a joint hearing. Room 311, Cannon House Office Building. More information.

-Apr. 26, 7:30 a.m. - 11:30 a.m., **Securing Information in a World Without Boundaries** - Join government agency and industry leaders to discuss the different ways of securing agency information and documents within today's mobile environment. The keynote speaker will be Andrew Jackson, deputy assistant secretary for technology, information and business services at the Department of the Interior. More information.

Media Appearances

Interest continues to run high in GW's newly announced Master's of Science degree program in Cybersecurity in Computer Science. A piece on the need for cybersecurity specialists aired this weekend on CNN, featuring interviews with Homeland Security Secretary Janet Napolitano, Kevin Mandia of Mandiant Corporation, and Prof. Lance Hoffman, CSPRI's director and the principal investigator for GW's Scholarships for Service program. It can be seen at this link (or the readable, non-video version can be read here).

Legislative Lowdown

-Prospects for passage of comprehensive cybersecurity legislation this year are looking dimmer as the presidential and congressional elections draw nearer, according to Jim Lewis, a cybersecurity expert with the Center for Strategic and International Studies (CSIS). Lewis spoke with GovInfoSecurity about the outlook for each of the bills. Lewis said though the House bills likely won't make it through the Senate, the upper chamber's Cybersecurity Act of 2012 could serve as a vehicle for lawmakers to get some form of IT security legislation enacted this year.

House Republicans said last week that on Thursday, April 26, the House would begin considering the "Cyber Intelligence Sharing and Protection Act of 2011" or "CISPA" (HR 3523). The GOP expects to finish consideration of the bill the following day. The measure has met resistance from civil liberties and privacy groups, who say language in key sections of the proposal is broad and could raise concerns. In a letter (PDF) to the bill's co-sponsors, Rep. Mike Rogers (R-Mich.) and Rep. Dutch Ruppersberger (D-Md.), a coalition of groups -- including the Competitive Enterprise Institute, the Liberty Coalition, Freedom Works, and Americans for Limited Government -- warned that the

measure "risks unduly expanding federal power, undermining freedom of contract, and harming U.S. competitiveness in the technology sector".

CISPA is but one of four cybersecurity bills that will come up for a vote before the full House of Representatives, House Speaker John Boehner said last week. Rep. Darrell Issa's (R-Calif.) Federal Information Security Act (FISMA) amendments would provide for stronger oversight of the security of federal computer systems. The Cybersecurity Enhancement Act, sponsored by Rep. Michael McCaul (R-Texas), aims to better coordinate federal research into cybersecurity. Finally, the House will vote on a bill from Rep. Ralph Hall (R-Texas) that will reauthorize research and development of new computing technology, called the Networking and Information Technology Research and Development (NITRD) program.

Notably absent from the House vote lineup is the PRECISE Act, another sweeping cybersecurity bill. The House Homeland Security Committee approved the measure last week, writes The Hill.

Cyber Security Policy News

-The Federal Communications Commission is clearing Google of wrongdoing in connection to its intercepting Americans' data on unencrypted Wi-Fi routers. Wired.com writes that the commission concluded Friday, in an order unveiled Monday, that no wiretapping laws were violated when the search giant's Street View mapping cars eavesdropped on open Wi-Fi networks across America. The FCC said that, between 2008 and 2010, "Google's Street View cars collected names, addresses, telephone numbers, URL's, passwords, e-mail, text messages, medical records, video and audio files, and other information from internet users in the United States." Last year, a federal judge ruled that the search-and-advertising giant could be held liable for violating federal wiretapping law, giving the green light to lawsuits seeking damages over Google's objections. Google is currently appealing that ruling because it says the unencrypted Wi-Fi signals were "readily accessible to the general public", per the wiretap law's language.

-Now that the Federal Aviation Administration (FAA) has cleared the way for drone aircraft to enjoy widespread use in U.S. domestic airspace, the chairmen of a congressional privacy caucus want to know how FAA will protect Americans from surveillance by operators of these aircraft, including police departments, NextGov reports. The FAA Modernization and Reform Act, which President Obama signed on Feb. 14, calls for FAA to integrate operation of drones into its National Airspace System by 2015. The agency in March kicked off a rule-making to set up six unmanned aircraft system test ranges by this summer. The language in the FAA bill and the rule-making both deal with safety issues and control of unmanned aircraft, but not privacy concerns, an issue the agency should address, Reps. Ed Markey, D-Mass., and Joe Barton, R-Texas, co-chairmen of the Bipartisan Congressional Privacy Caucus, said in a letter sent Thursday to Michael Huerta, acting FAA administrator.

The concern surfaces as the U.S. military is looking for industry partners to develop a radar detection system that can lock onto moving targets even through clouds and dust, according to a contracting document. The technology, when mounted on remotely-piloted aircraft, could improve the quality of drone imagery, increase the precision of air strikes and reduce collateral damage in warzones.

-The U.S. Army is having a hard time manning its IT staff because it cannot find military personnel with the right networking and IT security qualifications. The Department of Defense (DOD) Directive 8570.01-M is a military regulation first published in 2005 that puts forward considerable detail on the workplace and related training and certifications that military personnel -- and now contractors as well -- must have to operate DOD-related information systems for information assurance purposes. But the problem for the Army at this point is that it doesn't have enough personnel with the required training, said Lisa Lee, information assurance program manager, Program Executive Office, Enterprise Information Systems in the U.S. Army. According to Computerworld's Ellen Messmer, to cope with the shortage of certified personnel, the Army is altering its guidelines so that not as many individuals working in areas it calls "an enclave boundary" -- defined as a specific set of routers and firewalls -- will have to meet the previous requirements.

-The FBI's former top cyber cop has taken a job with a startup company to help protect private-sector computer networks that he says are already under constant attack with intrusions. Shawn Henry recently left the FBI after more than 20 years with the bureau. In a post on the company's blog, Henry said he decided to work at California-based CrowdStrike to fill a void in protecting private sector networks. The federal government is responsible for protecting military and government networks, but there is no one — except CrowdStrike's business rivals — charged with protecting the private sector dot-com domain, Henry said.

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*.