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

GW CSPRI Newsletter

October 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

-Oct. 11, 8:00 a.m. - 10:45 a.m., **Master Classes: Today's Leading Government Cyber Security Innovators** - This session features keynotes and talks from Chris Painter, director, Office of the Coordinator for Cyber Issues, Department of State; Kimberly Watson, technical director of analysis and data fusion group, information assurance directorate, National Security Agency. The Willard Hotel, 1401 Pennsylvania Ave NW. More information.

-Oct. 11-13, **ISS World Americas: Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering** - This conference bills itself as the largest gathering of North American, Caribbean and Latin American law enforcement, intelligence, homeland security analysts and telecom operators responsible for lawful interception, electronic

investigations and network intelligence gathering. Sessions include talks on social media, privacy, and internet investigations; the basics of Internet intercept; cell phone intelligence training; wiretapping; digital forensics; and intercepting data stored in the cloud. Bethesda North Marriott Hotel & Conference Center, 5701 Marinelli Road Bethesda, Md. More information.

-Oct. 12, 12 noon – 2 p.m., CSPRI Seminar Series **– What GW (and Other Universities) Don't Teach You About Medical Record Cyber Security and Privacy.** A panel on medical record cyber security and privacy. See Announcement below.

-Oct, 12-13, **Cyber Security CPR: Coordinated Private Response to Computer Security Incidents** - What happens when a cyber incident brings down something essential to public welfare? Since many critical infrastructures are privately-owned, who is responsible for planning a response? In what situations can government direct private enterprise to take action? These are just three of the many questions facing public and private sector practitioners, policy-makers, and researchers. This event will engage participants by presenting response realities, sharing research ideas, brainstorming new approaches, and forming collaborative partnerships to address key challenges. National Rural Electric Cooperative Association (NRECA) Conference Center, 4301 Wilson Blvd, Arlington, Va. More information.

-Oct. 13, 9:00 a.m., **Understanding Consumer Attitudes About Privacy** - The Subcommittee on Commerce, Manufacturing, and Trade will hold a hearing. Witness list to be announced. Rayburn House Office Bldg., Room 2123. More information.

-Oct. 14, 11:30 a.m. - 1:30 p.m., **Agile System Development: Addressing OMB 25 Point Plan on Effectively Managing IT Programs** - The Association for Federal Information Resources Management hosts a panel discussion featuring experts from GSA, FBI, USDA, and the DoD. Hotel Sofitel, 806 15th Street, 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.

Announcements

George Washington University will host a panel discussion on Wednesday, Oct. 12 on medical record cybersecurity and privacy. A panel of experts in cybersecurity, medical financial operations, medical privacy law, and developing medical software -- including a practicing medical doctor -- will discuss information security from their viewpoint and react to their fellow panelists' sometimes conflicting views of information security. They will also look into their own crystal balls to see what challenges the Patient Protection and Affordable Care Act of 2010, along with the miniaturization and advances in electronic systems, will provide in the years ahead. Panelists will include **Robert Gellman**, a consultant and former chief counsel to the Subcommittee on Government Information in the House of Representatives; **Kim Klein**, an expert in healthcare IT strategic planning; **Sumit Sehgal**, director of information security at GW University Hospital; and **Mark Smith**, **MD**, director of the MedStar Institute for Innovation and professor and chairman of emergency medicine at the Georgetown University School of Medicine. The lecture begins at noon. Lunch will be provided at 1 p.m., to accompany a roundtable discussion. GW Marvin Center, 800 21st St. NW, Room 308. Please RSVP to lunch and/or the seminar at http://csprievents.eventbrite.com. (Please RSVP to lunch by 5 p.m. today.)

Legislative Lowdown

-House Republicans last week issued their cybersecurity legislative agenda. The agenda somewhat parallels the goals offered by the Obama administration and Senate Democrats, but it definitely has a tinge to it by limiting regulation and providing for voluntary incentives, GovInfoSecurity writes. “The 20-page Recommendations of the House Republican Cybersecurity Task Force generally seeks to limit new regulations and provide for voluntary incentives to get businesses to secure their information systems and assets,” said task force Chairman Mac Thornberry, R-Texas, in a briefing unveiling the report. Thornberry said the White House proposals are “more regulatory than we believe is wise.” Still, unlike most issues that divide Republicans and Democrats, compromise will be sought. “There's a lot of room to work together within Congress and with the White House,” Thornberry said. “It's essential that we do so because of the economic aspects and national security aspects [of IT].”

-House lawmakers last week debated a proposal by the Federal Trade Commission to update a 1998 children's online privacy law, the government's first attempt at tweaking the measure to better apply to the proliferation of new mobile devices and Internet applications being used by children, The Washington Post reports. The House Commerce, Manufacturing and Trade Subcommittee debated recommendations by the Federal Trade Commission that Web firms be required to seek greater permissions from parents to collect information about children under the age of 13. But even with bipartisan support over some privacy bills, it will be difficult to pass new laws this session of Congress, analysts say, as lawmakers focus on jobs and the economy.

Cyber Security Policy News

-A computer virus has infected the cockpits of America's Predator and Reaper drones, logging pilots' every keystroke as they remotely fly missions over Afghanistan and other war zones, according to Wired.com's Noah Schactman. The virus, first detected nearly two weeks ago by the military's Host-Based Security System, has not prevented pilots at Creech Air Force Base in Nevada from flying their missions overseas. Nor have there been any confirmed incidents of classified information being lost or sent to an outside source. But the virus has resisted multiple efforts to remove it from Creech's computers, network security specialists say. And the infection underscores the ongoing security risks in what has become the US military's most important weapons system.

-The Obama administration is taking new steps to safeguard classified information and protect government computer networks against unauthorized disclosures such as last year's release of thousands of pages of secret documents by the website WikiLeaks, the Associated Press reports. An executive order signed Friday by the president is the result of a seven-month review by his administration, and sought a balance between security and the need for agencies to share classified information.

Wired.com reports that the updated policy focused on establishing committees, offices and task forces to work on implementing a balance between the needs of federal agencies to access classified data and the necessity of securing that data against improper usage and leaks.

But not everyone is convinced the new measures will be effective in preventing another damaging leak of classified information. Experts interviewed by The Hill warned that the next major cybersecurity breach might be completely different from the Wikileaks incident, and that the effectiveness of the order will depend on the specific security measures that the government implements.

The FBI said last week that by early 2012 it will have implemented a nationwide facial recognition service in select states that will allow local police to identify unknown subjects in photos. According to NextGov, "the federal government is embarking on a multiyear, $1 billion dollar overhaul of the FBI's existing fingerprint database to more quickly and accurately identify suspects, partly through applying other biometric markers, such as iris scans and voice recordings."

-In a move reminiscent of the Philip K. Dick science fiction novel-turned action flick "Minority Report," an internal document from the Department of Homeland Security indicates that a controversial program designed to predict whether a person will commit a crime is already being tested on some members of the public voluntarily. CNET reports that DHS is betting on algorithms: it's building a "prototype screening facility" that it hopes will use factors such as ethnicity, gender, breathing, and heart rate to "detect cues indicative of mal-intent." The latest developments, which reveal efforts to "collect, process, or retain information" on members of "the public," came to light through an internal DHS document obtained under open-government

laws by the Electronic Privacy Information Center. DHS calls its “pre-crime” system Future Attribute Screening Technology, or FAST.

-As he has for the past three years, President Obama has declared October to be Cybersecurity Awareness Month. In a declaration, the president called on Americans to observe the month with activities, events and trainings intended to enhance national and individual online security. National Cybersecurity Month is an event that dates back to 2004, and is the brainchild of the National Cyber Security Alliance, an education and outreach effort backed by companies like Cisco, Google, McAfee, Microsoft, and Symantec.

-Defense Secretary Leon Panetta announced the appointment of a new top cyber official at the Pentagon on Tuesday, The Hill writes. Eric Rosenbach will serve as deputy assistant secretary of Defense for cyber policy in the Office of the Assistant Secretary of Defense for Global Strategic Affairs. Rosenbach previously worked as the cybersecurity lead at Good Harbor Consulting. He replaces Robert Butler, who left DOD earlier this year.

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.