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

GW CSPRI Newsletter

October 3, 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 1

Announcements 2

Legislative Lowdown 3

Cyber Security Policy News 3

Upcoming Events

-Oct. 4, 10:00 a.m. - 12:00 noon, **Cyber Threats and Ongoing Efforts to Protect the Nation** - The House Intelligence Committee will hold an open hearing. The witnesses will be Michael Hayden, principal of the Chertoff Group, and Arthur Coviello, executive chairman, RSA. Capitol Visitor Center, Room HVC 210. More information.

-Oct. 5, 9:00 a.m., **Protecting Children's Privacy in an Electronic World** - The House Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade will hold a hearing. Rayburn House Office Building, Room 2123. More information.

-Oct. 5, 10:00 a.m., **Intelligence Sharing and Terrorist Travel: How DHS Addresses the Mission of Providing Security, Facilitating Commerce and Protecting Privacy for Passengers Engaged in International Travel** - The House Homeland Security Committee Subcommittee on Counterterrorism and Intelligence will hold a hearing. Cannon House Office Building, Room 311. More information.

-Oct 5, 1:00 p.m. - 5:00 p.m., **The Department of Homeland Security's Data Privacy and Integrity Advisory Committee** will meet. Navy League Building, 2300 Wilson Boulevard, Arlington, VA. More information.

-Oct. 6, 10:00 a.m., **Cloud Computing: What are the Security Implications?** - The House Homeland Security Committee Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies will hold a hearing. Cannon House Office Building, Room 311. More information.

-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, and 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** – Panel on medical record cyber security and privacy. See announcement below.

Announcements

CSPRI's seminar series for 2011-12 starts with 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 formerly 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, M. D**., director of the MedStar Institute for Innovation and professor and chairman of emergency medicine at the Georgetown University School of Medicine. The panel begins at noon. Lunch will be provided at 1 p.m. during a roundtable discussion. GW Marvin Center, 800 21st St. NW, Washington, DC, Room 308. Please register, even if you may not stay for lunch, at http://csprievents.eventbrite.com/.

Legislative Lowdown

-The prospects are dim for congressional passage of any cybersecurity measures making their way through Congress in 2011, according to a detailed analysis by former White House cybersecurity adviser Melissa Hathaway. Writing for BankInfoSecurity, Hathaway looks at the outlook for more than 30 cybersecurity and privacy bills awaiting action.

The prognosis? "The 112th Congress has an opportunity to drive a new legislative conversation and address the shortfalls in our laws," Hathaway writes. "But it won't be easy. There are competing views on how to position cybersecurity legislation; the Senate is pushing for an omnibus bill that comprises elements from each of the bills developed by its key committees, whereas the House of Representatives desires incremental reform via the introduction and passage of serial bills. This will be compounded by the work of the Joint Select Committee on Deficit Reduction, which is charged with developing a long-term plan to reduce the federal government's debt by at least $1.5 trillion over the next 10 years. As with nearly all other ongoing government programs, cybersecurity initiatives will face budget pressures and possibly funding cuts. Going forward, a premium will be placed on developing cost-neutral programs." Read more here, including a chart of most of the cybersecurity legislation in the 112th Congress.

Cyber Security Policy News

-House lawmakers urged the Federal Trade Commission to investigate “supercookies,” extremely persistent digital files that some companies are using to track consumers' activity online. The Wall Street Journal first reported last month that websites including MSN and Hulu were installing tools on users' computers that continued to track their activities online even after traditional tracking files, known as “cookies,” were deleted. In their letter to FTC Chairman Jon Leibowitz, Congressional Bi-Partisan Privacy Caucus members Reps. Edward Markey (D-Mass.) and Joe Barton (R-TK) called supercookies “unacceptable. We believe this new business practice raises serious privacy concerns and is unacceptable,” the lawmakers wrote in their letter. They ask the FTC whether it plans to investigate the use and impact of supercookies.

Facebook was known to have tracked users with supercookies even when they had already logged out of the site, writes PC Magazine. Facebook changed that behavior in the past week with a software update to its network, but Barton and Markey said they “remain concerned about the privacy implications for Facebook's 800 million subscribers.”

-Several wireless carriers keep cell phone call data for more than a year, according to a Justice Department document released by the American Civil Liberties Union. The document (PDF) was

intended to help law enforcement agents who were seeking cell phone records for their investigations, but the ACLU obtained it via a Freedom of Information Act request. The document shows that four national wireless carriers all keep records of which cell phone towers a phone uses for at least a year. This information could potentially be used to determine a person's location. Wired.com's David Kravets reports that Sen. Patrick Leahy (D-Vermont) has proposed legislation to alter the Electronic Privacy Communications Act to protect Americans from warrantless intrusions.

-Under pressure from federal lawmakers, automobile communication system OnStar said last week that it would not follow through with changes to its privacy policy. OnStar, which is owned by General Motors, notified its customers earlier this month that the company would continue to collect data about cars even after customers had canceled their OnStar service. Customers would have had to contact the company to opt out of the program. OnStar also said it was reserving its right to sell driver data to third parties. Last week, Democratic Sens. Al Franken (Minn.) and Chris Coons (Del.) urged the company to reconsider the changes last week, and Sen. Charles Schumer (D-N.Y.) asked the Federal Trade Commission to launch an investigation into whether the changes amounted to unfair trade practices. Last week, OnStar President Linda Marshall said in a statement that if the company "ever decides to collect data from customers who have canceled their service, customers would have to opt into the program," The Hill reports.

-The National Institute of Standards and Technology's computer security division released four publications to help businesses and organizations improve their cybersecurity posture. The first is a 49-page PDF titled "Guide to Bluetooth Security"; the second is a 24-page guide to "Securing Wireless Local Area Networks"; the third is an 85-page how-to on conducting risk assessments; the final document shows how to set up graphs to determine how a hacker is most likely to hit your network.

-Science Applications International Corp. said backup computer tapes containing sensitive health information of 4.9 million Military Health Care System TRICARE beneficiaries treated in the San Antonio, Texas, area since 1992 were stolen from an employee's car Sept. 14, NextGov reports. A SAIC spokesman said the employee was transporting the tapes from one federal facility to another in the San Antonio area and reported the theft the same day to TRICARE and the San Antonio Police Department. But Sandra Gutierrez, a police spokeswoman, said the theft, according to a report filed by SAIC, occurred sometime between 7:53 a.m. and 4 p.m. on Sept. 13 at an SAIC facility at 300 Convent Ave., indicating the tapes had been left in a parked car for most of the day, with the company reporting the robbery on the 14th.

-The Justice Department takes too long to report cyber incidents and does not have cyber incident reports from all of its departments, Federal News Radio reports. The Justice Security Operations Center (JSOC), established in 2007, monitors DoJ's IT systems for cyber threats. JSOC coordinates with the Homeland Security Department's U.S. Computer Emergency Readiness Team (US-CERT) to defend against cyber attacks. The IG also found JSOC did not have a comprehensive picture of potential cyber threats. Six of DoJ's 32 components have not provided all information to JSOC. In particular, the FBI does not report incidents it categorizes as "under investigation."

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.