GW CSPRI Newsletter

April 21, 2014

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

-Apr. 21-22, **Protecting the Defense Industrial Base from Cyber Attack** - This NDIA Cyber Forum is designed to assemble a group of cyber practitioners and experts from both government and industry to articulate the current nature of the cyber threat against the DIB, expand the awareness of selected programs, measures and organizations designed to protect DIB networks and systems from malicious cyber incursions, and to identify areas where greater effort and more extensive government-industry collaboration is necessary to safeguard them from compromise. Lockheed Martin Global Vision Center, 2121 Crystal Drive Suite 100, Arlington, VA 22202. More information.

-Apr. 22, 8:15 a.m. - 4:45 p.m., **ISACA NCA Meetup: Federal IT and Security** - During this one-day cyber-security conference, attendees will learn about the recent security breaches and prevention techniques, emerging risks and remediation strategies in the field of Cybersecurity, as well as new cyber policies, standards, and frameworks being developed to combat the risks. Holiday Inn, Rosslyn at Key Bridge, 1900 North Fort Myer Dr., Arlington, Va., 22209. More information.

-Apr. 22, 10:00 a.m. - 12 noon, **Privacy Principles in the Era of Massive Data** - Experts from the public and private sectors will join public policy experts from the Georgetown University McCourt School of Public Policy and privacy law experts from the Georgetown Law Center to examine the privacy issues that arise with massive data. Speakers will include Maureen Ohlhausen, commissioner, Federal Trade Commission; Edward Montgomery, dean, McCourt School of Public Policy; Julie Cohen, Georgetown Law; Robert Groves, provost, Georgetown University; Benjamin Wittes, Brookings Institution; Chris Wolf, Hogan Lovells. Georgetown University Law Center, Hart Auditorium, 600 New Jersey Ave. NW. More information.

-Apr. 23, 2:30 p.m. - 3:30 p.m., **Privacy Roundtable: Recent California Privacy Legislation** - The American Bar Association will host a teleconferenced panel. The speakers will include Joanne McNabb, director of privacy, education and policy, Office of the Attorney General, California Department of Justice; and Aryeh Friedman, Dun & Bradstreet. More information.

-Apr. 24, 8:30 a.m. - 3:00 p.m., **Cybersecurity: Innovation and Challenges From Mobiles, Automobiles, Internet of Things to Insider Threats** - A day of presentations featuring updates on the latest innovations in cybersecurity, and subsequent challenges, in areas ranging from automobiles and transportation to medical devices and the smart home. As traditionally non-internet enabled products morph into internet-enabled technologies, the need for advanced cybersecurity is increasing rapidly. The speakers and panelists at this event will discuss the impact this is having on the field and what changes are occurring in policy, technology, and leadership initiatives in order to provide this new level of cybersecurity. George Mason University, 4400 University Drive, Fairfax, VA, 22030. More information.

-Apr. 24, 7:00 p.m. - 10:00 p.m., **CharmSec Meetup** - CharmSec is an informal, all-ages, citysec-style meetup of information security professionals in Baltimore. Heavy Seas Alehouse, 1300 Bank St., Baltimore, Md., 21231. More information.

-Apr. 25, 12 noon - 1:15 p.m., **Revising the Electronic Communications Privacy Act (ECPA): Should Congress Require a Warrant?** - The Internet Caucus will hold a panel discussion. The speakers will include James Dempsey, Privacy and Civil Liberties Oversight Board, Center for Democracy & Technology; Richard Downing, the Justice Department's Computer Crime and Intellectual Property Section; and Katie McAuliffe, Americans for Tax Reform. Rayburn House Office Bldg., Room 2226. More information.

-Apr. 29 - May 2, **US Cyber Crime Conference** - This conference covers the full spectrum of topics facing defenders as well as law enforcement responders. All aspects of computer crime will be covered, including intrusion investigations, cyber crime law, digital forensics, information assurance, along with research and development, and testing of digital forensic tools. National Conference Center, 18980 Upper Belmont Pl., Leesburg, Va., 20176. More information.

Legislative Lowdown

-A House committee last week voted to delay the Obama administration's plan to give up oversight over certain technical Internet management functions. According to NextGov, Republicans are worried that the proposal, which would transfer power to an international nonprofit group, could open the door to an Internet takeover by authoritarian regimes. "The Republicans on the House Communications and Technology Subcommittee overrode vocal Democratic opposition to advance the DOTCOM Act, which would instruct the Government Accountability Office to investigate the administration's plan," Brendan Sasso writes. "The bill would block the transfer of Internet powers for up to a year while the office prepares a report. The bill now heads to the full Energy and Commerce Committee for consideration."

Cyber Security Policy News

-Two Supreme Court justices suggested late Thursday that the high court will likely decide the constitutionality of the National Security Agency's (NSA) surveillance programs, The Hill reports. Speaking at an event at the National Press Club event, liberal Justice Ruth Bader Ginsberg and Justice Antonin Scalia were asked whether the Supreme Court would take up cases related to NSA surveillance operations disclosed by former contractor Edward Snowden. "We can't run away and say, 'Well, we don't know much about that subject so we won't decide it,'" Ginsberg reportedly said. "Scalia, one of the most conservative justices, said the court might not be the best institution to wade into national security issues. He suggested, however, the Supreme Court would likely decide whether gathering a wide swath of telecommunications data violates the Fourth Amendment."

-The U.S. Securities and Exchange Commission (SEC) is preparing to conduct more than 50 examinations to gauge the cybersecurity preparedness in the securities industry, and to obtain information about the industry's recent experiences with certain classes of cyberthreats. GovInfoSecurity writes that "organizations to be examined by the SEC's Office of Compliance Inspections and Examinations include registered broker-dealers and registered investment advisers, according to an April 15 announcement. The examinations will focus on the entities' identification and assessment of risks; protection of networks and information; risks associated with remote customer access and funds transfer requests; risks associated with vendors and other third parties; detection of unauthorized activity; and experiences with certain cybersecurity threats."

-A report released last week posits that the Commerce Department's voluntary cybersecurity framework could wind up undermining the very online protections it seeks to encourage, The Hill reports. "The report out on Thursday from George Mason University's Mercatus Center claimed that the plan amounts to "opaque control" of the Internet, which could undermine the 'spontaneous, creative sources of experimentation and feedback that drive Internet innovation.' Companies, the authors wrote, 'already have intrinsic incentives to develop cybersecurity solutions' without a formal government plan."

-The breach of some 40 million credit and debit cards at Target last year, as well as similar break-ins at other retailers, has prompted the creation of a new industry group for collecting and sharing intelligence about cybersecurity threats, Reuters reports. "The National Retail Federation said Monday it will establish an Information Sharing and Analysis Center, or ISAC, for the retail industry in June," according to Reuters. "ISACs are industry groups set up under terms of a 1998 presidential directive to foster sharing of security information between the public and private sector. There are more than a dozen such organizations among industries including financial services, emergency services, healthcare, technology companies, public transportation and utilities."

News of the new ISAC came as nationwide arts and crafts retailer Michaels Stores divulged more information about a breach of its payment card systems that was first disclosed in January 2014. Michaels said that two separate eight-month-long security breaches at its stores and at that of some Aaron Brothers stores may have compromised as many as three million customer debit and credit cards.

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.