GW CSPRI Newsletter

April 22, 2013

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. 22-24, **Forensics Enabled Intelligence** - Speakers from the Office of the Provost Marshal General of the Army, the Naval Criminal Investigation Service, the Air Force Office of Special Investigations and the Department of Defense will give their views on where forensics is headed – challenges, strategies, roadmaps and more. Additionally, sessions from the FBI, Department of Justice and others will address the latest forensic technologies and employment techniques, as well as strategies for intelligence sharing. Holiday Inn, 625 First Street , Alexandria, Va. More information.

-Apr. 23, 2:15 p.m. - 3:45 p.m., **Cyber Security and Critical Infrastructure** - The American Bar Association will host a webcast and teleconferenced panel discussion on the legal issues concerning cyber threats to critical infrastructure. The speakers will be Tommy Ross, senior intelligence and defense advisor to Senate Majority Leader Harry Reid (D-Nev.); Bob Schwentker, senior vice president and general counsel, North Carolina Electric Membership Corporation; Lisa Sotto, managing partner, Hunton & Williams; and Christy Walsh, special counsel, Office of the General Counsel, Federal Energy Regulatory Commission. More information.

-Apr. 23-24, **Countering Transnational Organized Crime** - This two-day conference will cover a broad range of topics related to organized crime, including cybercrime and money laundering. Speakers include General John Kelly, US SOUTHCOM Commander; Ambassador Luis CdeBaca, Department of State; and other officials from the defense, intelligence, and law enforcement communities. Holiday Inn, 625 First Street, Alexandria, Va. More information.

-Apr. 23-24, **Mobile Device Security for Defense and Government** - This symposium's overall theme will focus on DOD's plan to maximize the potential uses of mobile devices within specific key areas: wireless infrastructure, mobile devices and mobile applications. The community goal of this event is to advance flexible and secure mobile devices to benefit the warfighter and keep pace with changing technology. Mary M. Gates Learning Center, 701 N. Fairfax St. Alexandria, Va. More information.

-Apr. 23-25, **DoD Cloud Computing and Assurance Conference** - This event will provide a forum for individuals who have a variety of responsibilities involved with the implementation of cloud computing directives to engage emerging concerns. The discussions will revolve around how different groups across the DoD have begun moving certain applications to the cloud, are (or are planning to) ramp up their data management and security while consolidating, facilitate extended operational capabilities with the move to cloud, and prove cost-efficiency. Washington Plaza Hotel, 10 Thomas Cir. NW. More information.

-Apr. 24, 2:30 p.m., **A Status Update on the Development of Voluntary Do-Not-Track Standards** - The Senate Commerce Committee will hold a hearing, which will examine what steps, if any, industry stakeholders have taken to fulfill their public commitment to honor Do-Not-Track requests from consumers. Russell Senate Office Bldg., Room 253. More information.

-Apr. 25, 10:00 a.m., **The Electronic Communications Privacy Act (ECPA), Part 2: Geolocation Privacy and Surveillance** - The House Judiciary Committee's Subcommittee on Crime, Terrorism, Homeland Security and Investigations will hold a hearing. Witnesses TBD. Rayburn House Office Bldg., Room 2141. More information.

-Apr. 25, 7:00 p.m., **Charmsec Meetup** - An informal, all-ages, citysec-style meetup of information security professionals in Baltimore. Heavy Seas Alehouse, 1300 Bank Street, Baltimore, MD, 21231. More information.

Legislative Lowdown

-The House of Representatives last week passed a controversial cybersecurity bill, moving toward a possible showdown with the Senate and the White House. As the Los Angeles Times reports, the Cyber Intelligence Sharing and Protection Act of 2013, or CISPA, passed by a vote of 288 to 127, with 17 abstentions. The bill makes it easier for companies to share information with other companies and the government about cyber attacks. Large tech companies pushed hard for the legislation amid escalating cyber attacks, calling it a necessary step to shore up their defenses. But critics have argued that the bill makes it too easy for companies and the government to gain access to private data, absolves companies of too much legal liability, and fails to ensure that civilian rather than military agencies will facilitate the sharing of information. The issue now moves to the Senate, where a companion bill has yet to be introduced. But earlier this week, the Obama administration made clear its promise to veto the House version of CISPA unless greater provisions were made to protect privacy and civil liberties.

-The Senate Judiciary Committee is expected to approve legislation this week that would require police to obtain a warrant to search emails and other private online content, reports The Hill's Brendan Sasso. Leaders of the committee said they expect to approve a package of proposed changes to the Electronic Communications Privacy Act (ECPA) of 1986. Under the current law, police only need a subpoena, issued without a judge's approval, to read emails that have been opened or that are more than 180 days old. A copy of the bill to be voted on is here (PDF), and a step-by-step analysis of the proposed amendments to the current ECPA is at this link (PDF). As mentioned in above “Events” section, the House Judiciary Committee’s Subcommittee on Crime, Terrorism, Homeland Security and Investigations will also be holding a hearing on the ECPA next week.

-The House passed a long-pending update to the Federal Information Security Management Act (FISMA), the law which mandates steps that federal agencies have to take to protect their networks and computers from hackers and malicious software, Federal News Radio writes. Critics have charged that the current FISMA places too much emphasis on having agencies write reports and meet static requirements instead of forcing them to test their own networks as malicious hackers would, by probing them for some of the most common system configuration weaknesses. The House also passed H.R. 756 (PDF), the Cybersecurity Enhancement Act of 2013, and H.R. 967 (PDF), the Advancing America's Networking and Information Technology Research and Development Act of 2013, with little debate or challenge.

Cyber Security Policy News

-The American Civil Liberties Union filed a federal complaint last week accusing the nation’s largest wireless carriers of “deceptive” business practices for failing to keep the software on tens of millions of Android smartphones updated — a shortcoming that can make the devices vulnerable to hackers, according to The Washington Post. Security companies have documented a surge of malicious software targeting Android phones, whose operating systems are made by Google, over the past year. Older phones that do not receive routine updates are particularly exposed, security experts say, yet the wireless carriers who sell most of the phones in the United States have struggled to keep the software current. The problem has caused smartphones featuring Android, which is the most popular mobile operating system in the world, to be more vulnerable to hackers than those of its leading rivals, such as Apple’s iPhone, which receives regular software updates

In other mobile policy news, the Federal Trade Commission wants to learn more about privacy threats raised by the so-called "Internet of Things." The FTC said last week it is seeking feedback on the privacy risks posed by everyday devices — such as cars, medical devices and appliances — that are connected to the Internet. The commission last week said it is seeking public comment on the matter, and that it plans to hold a workshop on the topic in November.

-Pretrial hearings in the Guantanamo war crimes tribunals have been delayed to address the mysterious disappearance of defense legal documents from Pentagon computers, military officials said on Thursday, Reuters says. The long-troubled military trials at Guantanamo Bay were hit by revelations earlier this year that a secret censor had the ability to cut off courtroom proceedings, and that there were listening devices disguised as smoke detectors in attorney-client meeting rooms. Now, another potential instance of compromised confidentiality at the military commissions has emerged: Defense attorneys say somebody has accessed their email and servers. ProPublica has published an update on this story that includes a statement from a Pentagon spokesman who disputed the characterization of an email and data breach, arguing that government prosecutors never saw the content of any privileged communications.

-The U.S. Federal Energy Regulatory Commission proposed to revise its cybersecurity standards for the nation's electric grid, expanding the rules to more than 60 additional companies. According to Bloomberg, the agency last week voted to start the process for updating the existing critical infrastructure protection standards. The revisions are aimed at enhancing the security posture of companies that link to the grid. Cybersecurity is becoming a critical issue for electric utilities as components such as generators, power meters and appliances are interconnected using the Internet. White House National Security Adviser Thomas Donilon said in a March 11 speech that the U.S. is concerned about "cyber intrusions emanating from China at a very large scale." As mentioned above, in the "Events" section, The American Bar Association will also be holding a webcast discussing these legal issues later this week.

- The Pentagon has for the first time detailed $30 million in spending on Air Force cyberattack operations and significant new Army funding and staff needs for exploiting opponent computers, NextGov writes. Since 2011, top military brass have acknowledged the United States has the capability to hack back if threatened by adversaries in cyberspace. Now, the Defense Department is providing lawmakers and taxpayers with evidence of network assault programs to sustain funding, budget analysts say. The Air Force in fiscal 2014 expects to spend $19.7 million on "offensive cyber operations," including research and development, operations, and training, according to budget documents circulated this week.

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.