GW CSPRI Newsletter

May 20, 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.

Events

-May 21, 9:00 a.m. - 12:30 p.m., **Threat and Response: Combating Advanced Attacks and Cyber-Espionage** - The Center for Strategic and International Studies will host an event. The speakers will include David DeWalt, chairman of the board and chief executive officer, FireEye; Ashar Aziz, founder, vice chairman, and CTO, FireEye; Shane McGee, general counsel, Mandiant; James Mulvenon, vice president, Defense Group, Inc.; Shawn Henry, president, CrowdStrike; James Lewis, director and senior fellow, CSIS; Bruce McConnell, deputy under secretary for cybersecurity, National Protection and Programs Directorate, DHS; John Nagengast, director of government solutions, AT&T; John Gilligan, president, The Gilligan Group; and Robert Lentz, president, Cyber Security Strategies. CSIS, B1 Conference Center, 1800 K St., NW. More information.

-May 21, 10:00 a.m., **Cyber Threats and Security Solutions** - The House Commerce Committee will hold a hearing. Witnesses will include Patrick D. Gallagher, under secretary of commerce for standards and technology, and director National Institute of Standards and Technology; Dave McCurdy, president and CEO, American Gas Association; John M. "Mike" McConnell, vice chairman, Booz Allen Hamilton; R. James Woolsey, chairman, Woolsey Partners LLC; Michael Papay, vice president and chief information security officer, Northrop Grumman Information Systems; Phyllis Schneck, vice president and chief technology officer, McAfee; Charles Blauner, global head of information security, Citigroup; Duane Highley, president and CEO, Arkansas Electric Cooperative Corp.; Robert Mayer, vice president, industry and state affairs, U.S. Telecom Association. Rayburn House Office Bldg., Room 2123. More information.

-May 21, 2:00 p.m., **Cybersecurity: An Examination of the Communications Supply Chain** - The House Commerce Committee's Subcommittee on Communications and Technology will hold a hearing. The witnesses will include Jennifer Bisceglie, president and CEO, Interos Solutions Inc.; Robert B. Dix, Jr., vice president, government affairs and critical infrastructure protection, Juniper Networks Inc.; Mark L. Goldstein, director, physical infrastructure issues, Government Accountability Office (GAO); John Lindquist, president and CEO, Electronic Warfare Associates; David Rothenstein, senior vice president, general counsel and secretary, Ciena; Stewart A. Baker, partner, Steptoe & Johnson LLP; and Dean Garfield, president and CEO, Information Technology Industry Council. Rayburn House Office Bldg., Room 2123. More information.

-May 21, 6:30 p.m. - 8:00 p.m., **ISSA DC Meetup** - The National Capital Chapter of the ISSA is comprised of information security professionals located in the Washington D.C. Metropolitan Area. Members are actively involved in information security in government agencies, the military, non-profit organizations, and in large and small companies. This month's meeting topic will be "Continuous Monitoring for Large Scale Enterprises." Center for American Progress, 1333 H Street, NW. More information.

-May 21-22, **Safeguarding Health Information; Building Assurance Through HIPPA Security, 2013** - The conference will offer sessions exploring security management and technical assurance of electronic health information. Presentations will cover a variety of current topics including updates on the Omnibus HIPAA/HITECH Final Rule, identity management, strengthening cybersecurity in the health care sector, integrating security safeguards into health IT, managing insider threats, and securing mobile devices. Ronald Reagan Building and International Trade Center, 1300 Pennsylvania Avenue, NW. More information.

-May 22, 12:00 noon - 1:30 p.m., **Surveillance Cameras: Helpful or Harmful?** - The Information Technology and Innovation Foundation will host a panel discussion. The speakers will be Carrie Johnson, justice correspondent, NPR; Daniel Castro (ITIF); Paul Rosenzweig, founder, Red Branch Law & Consulting, LLC; Jay Stanley, senior policy analyst, ACLU; Julian Sanchez, research fellow, Cato Institute. ITIF/ITIC, Suite 610A, 1101 K St., NW. More information.

-May 22, 6:30 p.m. - 8:00 p.m., **OWASP NoVA Meetup** - The OWASP Northern VA Local Chapter meetings are free and open to anyone interested in learning more about application security. Living Social, Reston, 11600 Sunrise Valley Drive, Reston, VA, 20136. More information.

-May 23, 1:00 p.m. - 5:00 p.m., **Mobile Application Transparency** - The Department of Commerce's National Telecommunications and Information Administration will hold another in

its series of meetings regarding mobile application transparency. American Institute of Architects, 1735 New York Ave., NW. More information.

-May 23, 9:00 a.m. - 11:00 a.m., **The Geopolitics of Internet Governance** - The Center for Strategic and International Studies will host a panel discussion. The speakers will include Phil Verveer, former US coordinator, international communications and information policy, U.S. Department of State; Veni Markovski, ICANN, vice president for Russia, CIS and Eastern Europe; Sally Wentworth, senior director, Strategic Public Policy; Bill Smith, senior policy advisor, PayPal; Laura DeNardis, associate professor in the school of communication, American University. CSIS, B1 Conference Center, 1800 K St., NW. More information.

-May 24, 12 noon - 1:15 p.m., **Enabling Do Not Track Privacy: Is it Dead or Alive?** - The Congressional Internet Caucus will host a discussion on the present and future of voluntary, industry-led efforts to enable consumers to block advertisers from tracking their actions online. Rayburn House Office Bldg., Room B-339. More information.

Legislative Lowdown

-Rep. Hank Johnson (D-Ga.) last week introduced new legislation that would require mobile application developers to provide clear notice to consumers and get their consent before collecting personal data from mobile devices, Computerworld writes. Johnson's bill, the Application Privacy, Protection and Security Act of 2013 (HR1913), would force mobile application developers to disclose what data they collect and how they will use, share and store that data. They would be required to disclose the specific categories of data they collect and the third parties with whom they share the data. Mobile application developers would need to have a clearly spelled out privacy and data retention policy that tells consumers how long data is stored and the choices they have for deleting or opting out of such collection. The Federal Trade Commission would be responsible for enforcing the provisions of the bill, known as the Apps Act.

-A bipartisan group of House lawmakers have introduced legislation that would require federal agencies to obtain a court order before seizing telephone records. The Hill reports that the bill, the Telephone Records Protection Act, is a reaction to the Justice Department's seizure of two months' worth of phone records of Associated Press journalists as part of an investigation into the leak of national security information (see next article below). Under current law, investigators need a warrant from a judge to wiretap a phone line, but they can obtain call records from a phone company with only a subpoena. The records often include information such as the numbers of incoming and outgoing calls, call duration and subscriber information.

Cyber Security Policy News

-The Justice Department secretly obtained two months' worth of telephone records of journalists working for the Associated Press as part of a year-long investigation into the disclosure of classified information about a failed al-Qaeda plot last year. The Washington Post cites the AP's president last week saying that federal authorities obtained cellular, office and home telephone records of individual reporters and an editor; AP general office numbers in Washington, New York and Hartford, Conn.; and the main number for AP reporters covering Congress. He called the Justice Department's actions a "massive and unprecedented intrusion" into newsgathering activities.

Meanwhile, Bloomberg News has found itself in the hotseat over accusations that it abused its access to client research and trading activity to give the company's reporters an advantage over competing publications in covering the markets. As CNN reports, traders, regulators and central bankers throughout the financial world depend on Bloomberg terminals for real-time data on markets of all kinds as well as news and instant messaging. The machines reportedly rent for $20,000 a year and are used by thousands of subscribers, bringing in a substantial portion of the company's revenue. Executives at Goldman Sachs (GS, Fortune 500) first voiced concern over the surveillance to Bloomberg a few weeks ago after one of the company's reporters spoke to a Goldman executive about the terminal login habits of another Goldman executive. This prompted concern from Goldman that Bloomberg journalists could be tracking users on the terminals.

-Three months after hackers working for a cyberunit of China's People's Liberation Army went silent amid evidence that they had stolen data from scores of American companies and government agencies, they appear to have resumed their attacks using different techniques, The New York Times says. The Obama administration had bet that "naming and shaming" the groups, first in industry reports and then in the Pentagon's own detailed survey of Chinese military capabilities, might prompt China's new leadership to crack down on the military's highly organized team of hackers — or at least urge them to become more subtle. But Unit 61398, whose well-guarded 12-story white headquarters on the edges of Shanghai became the symbol of Chinese cyberpower, is back in business.

-If your smartphone is encrypted and protected by a long passcode, you're going to keep most people from being able to get at the data stored on it. However, companies like Apple and Google are being asked by law enforcement officials to bypass these protections to aid in investigations, and the frequency of requests is creating lengthy wait lists—one agent at the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) was reportedly told by an Apple legal representative that the agency would need to wait at least seven weeks to have a phone unlocked. As CNetreports, court documents show that federal agents were so stymied by the encrypted iPhone 4S of a Kentucky man accused of distributing crack cocaine that they turned to Apple for decryption help last year. An agent at the ATF, the federal Bureau of Alcohol, Tobacco, Firearms and Explosives, "contacted Apple to obtain assistance in unlocking the device," U.S. District Judge Karen Caldwell wrote in a recent opinion. But, she wrote, the ATF was "placed on a waiting list by the company."

-Six months after a U.S. cybersecurity bill died in the Senate, some Obama administration officials and lawmakers are optimistic they can get a new law passed amid heightened public awareness of hacking attacks and cyber espionage, according to Reuters. "With top intelligence officials warning that cyber attacks have replaced terrorism as the leading threat against the United States, the White House and lawmakers have spent months discussing how to improve the flow of information between the government and the private sector," Reuters wrote. "A second go-around for the Cyber Intelligence Sharing and Protection Act (CISPA) was approved by the Republican-controlled House of Representatives in a bipartisan vote on April 18, though the White House has again threatened to veto the bill unless more protections for privacy and civil liberties are added. Still, senior Obama administration officials say behind-the-scenes talks with lawmakers this time around are constant, more serious and more productive."

-Public companies already face requirements from the U.S. Securities and Exchange Commission to report on their financial statements any security breaches that could materially impact the company's bottom line. But in an editorial for Forbes, BeyondTrust CEO John Mutch maintains that more cybersecurity regulations may be in the offing from the SEC. "This is going to be an even steeper climb if the SEC requires companies to disclose on their cyber risk," Mutch notes. "In his April 9 letter to the SEC Chair, Senate Commerce Chairman Jay Rockefeller (D-W.Va.) urged the SEC to step-up the requirements on its guidance (issued in October 2011) for companies to disclose information about their ability to defend against attacks on their networks.

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.