GW CSPRI Newsletter

June 30, 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

Announcements

A webinar sponsored by the ACM on Cybersecurity and Public Policy, based on the new National Research Council book "At the Nexus of Cybersecurity and Public Policy", is now available on demand. The "launch presentation" button is at the bottom of the page: http://w.on24.com/r.htm?e=808454&s=1&k=1B2118B9D0DACA6A999B94A86E81B355. The book is available for free download at http://www.nap.edu/catalog.php?record_id=18749.

It's very comprehensive at a high level and easy to follow for techical and nontechnical people. It is a great introductory lecture (25 min) for anyone wanting a quick overview of the field and the public policy issues related to cybersecurity.

Events

-June 30, 1:00 p.m. – 2:30 p.m., **NIST Cyber-Physical Systems Public Working Group Kickoff Webinar** – The event will bring together experts to help define and shape key aspects of CPS to accelerate its development and implementation within multiple sectors of the economy. The four initial workgroups of the CPS PWG will cover

(1) Definitions, Taxonomy and Reference Architecture, (2) Use Cases, (3) Timing and Synchronization, and (4) Cybersecurity and Privacy. More information.

-July 2, 10 a.m., **PCLOB Public Meeting on Section 702 Report** – In this public session, the Privacy and Civil Liberties Oversight Board will vote on the formal issuance of its report to the President, Congress and the public. Additional information on the Board's review of the surveillance program, such as its prior public hearings, is available at www.pclob.gov. The July 2nd meeting is open to the public and a meeting notice has been published in the Federal Register at https://www.federalregister.gov/a/2014-14603 Pre-registration is not required. JW Marriot Hotel, 1331 Pennsylvania Ave NW, Washington, DC in Salon III.

-July 8, 4:00 p.m., **You're Gonna Need A Warrant for That: The Path to Digital Privacy Reform** – A unanimous Supreme Court recently declared that that our networked mobile devices merit the highest level of Fourth Amendment protection against government searches, since these devices often contain more sensitive information than even "the most exhaustive search of a house" would reveal. Yet increasingly, the vast troves of personal data they contain are synched to "the cloud," where the outdated Electronic Communications Privacy Act of 1986 allows many types of information to be accessed without a warrant. The need to bring the law up to date has been recognized not only by privacy advocates, but major technology companies, more than half of the House of Representatives, and even federal law enforcement officials. This discussion will tackle the questions of how and why to drag federal privacy law into the 21st century, with keynote remarks by Rep. Ted Poe (R-TX) and a panel discussion featuring both policy experts and representatives of the tech firms we increasingly entrust with our most private data. The event also will be Webcast. CATO Institute, 1000 Massachusetts Ave. NW. More information.

Legislative Lowdown

-More than two dozen civil liberties and privacy groups say they oppose a new cybersecurity bill in the Senate. In a letter (PDF) sent last week to Majority Leader Harry Reid and other top Senate lawmakers, a coalition of groups laid out their opposition to the Cybersecurity Information Sharing Act of 2014 (CISA), saying that the bill threatens to create a gaping loophole in existing privacy law. It would permit the government to approach private companies and ask for "voluntary" cooperation in sharing sensitive information, including communications content, and then use that information in various law enforcement investigations – including the investigation and prosecution of government whistleblowers under the Espionage Act. "In the year since Edward Snowden revealed the existence of sweeping surveillance programs, authorized in secret and under classified and flawed legal reasoning, Americans have overwhelmingly asked for meaningful privacy reform and a roll back of the surveillance state created since passage of the Patriot Act," the letter charges. "This bill would do exactly the opposite."

-An amendment to the Defense Department's spending bill bars funding for any programs which might seek to install security vulnerabilities in U.S.-made technology equipment, CNet reports. According to CNet, the amendment "is in response to alleged activity revealed late last year by German newspaper Der Spiegel, which reported that the US agency intercepts deliveries of electronic equipment to plant spyware to gain remote access to systems once they are delivered and installed. According to the report, the NSA has planted backdoors to access computers, hard drives, routers, and other devices from companies such as Cisco, Dell, Western Digital, Seagate, Maxtor, Samsung and Huawei."

Cyber Security Policy News

-The U.S. Supreme Court last week struck a major victory for privacy rights in the digital age last week, handing down a unanimous decision that police need to obtain warrants to search the cell phones of anyone they arrest. "While the decision will offer protection to the 12 million people arrested every year, many for minor crimes, its impact will most likely be much broader," The New York Times reported. "The ruling almost certainly also applies to searches of tablet and laptop computers, and its reasoning may apply to searches of homes and businesses and of information held by third parties like phone companies."

-The top court in Massachusetts ruled last week that a criminal suspect can be compelled to decrypt his seized computer. As Ars Technica writes, the ruling online applies to cases in the state of Massachusetts; other courts at the state and federal level have issued conflicting rules on whether being forced to type in a decryption password is a violation of the Fifth Amendment right to protect against self-incrimination.

-Attackers last year successfully infiltrated servers at a major U.S-based hedge fund, stealing information about the organization's trading strategy by briefly diverting trades to systems they controlled before sending the trades on their way to their rightful desintation. The report, first aired in a CNBC report with BAE Systems, did not name the affected hedge fund, but said the attack was one of the most complex the company had seen in terms of data extraction. As if that isn't scary enough, the BAE technician interviewed by CNBC said in recent weeks they "have also spotted a cyberattack that used malware to take over a large property and casualty insurer's underwriting system. Using the compromised system, the criminals created fake insurance policies and filed claims against them."

-A newly released report from The RAND Corp. suggests that there is a shortage of highly trained cybersecurity workers – particularly in the federal government – with potentially serious consequences for national security. CBSNews reports on the RAND study, which recommends a series of steps to attract more cybersecurity workers to the federal sector, such as relaxing federal hiring rules, investing in cybersecurity education programs, and finding ways to attract more women into the profession.

-Europol and the EU Union Agency for Network and Information Security inked a strategic cooperation agreement last week to share data on cyber threats and to cooperate on cyber capacity building and training. The agencies cautioned that the data sharing would not include personal information about European citizens.

-In a move that may wind up helping spammers, Microsoft is blaming a new Canadian anti-spam law for the company's recent decision to stop sending regular emails about security updates for its Windows operating system and other Microsoft software. "Asked about the reason for the change, a Microsoft spokesperson said email communication was suspended to comply with a new Canadian anti-spam law that takes effect on July 1, 2014," writes KrebsOnSecurity.com. "Some anti-spam experts who worked very closely on Canada's Anti-Spam Law (CASL) say they are baffled by Microsoft's response to a law which has been almost a decade in the making, noting that the law contains carve-outs for warranty and product safety and security alerts that would more than adequately exempt the Microsoft missives from the regulation."

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.