GW CSPRI Newsletter

July 28, 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

-July 31, 7:00 p.m. – 10:00 p.m., **CharmSec Meetup** – Heavy Seas Alehouse, 1300 Bank Street, Baltimore, MD, 21231. An informal, all-ages, citysec-style meetup of information security professionals in Baltimore. More information.

-Aug. 14, 8:15 a.m. – 4:45 p.m., **Washington D.C. Tech-Security Strategies Conference** -Washington Plaza Hotel, 10 Thomas Circle NW. More information.

Legislative Lowdown

-Senate Judiciary Chairman Patrick Leahy (D-Vt.) is close to an agreement with Obama administration on how to rein in government surveillance, according to The Hill. "Leahy said on Tuesday that he is 'impressed' with the administration's efforts to work towards a compromise. Tech companies and privacy advocates initially rallied behind the USA Freedom Act, The Hill's Kate Tummarello writes, "but some of the bill's co-sponsors later yanked their support for the bill as it made its way to the House floor, citing concerns that it had been 'watered down' through eleventh-hour negotiations between the administration and House leadership."

-The New York Times today ran an editorial that highly praises the surveillance reform bill as "a significant improvement over the halfhearted measure passed by the House in May." The Times' story breaks down what's in the bill and why its passage would be a good thing. To wit: "One of the best parts of the bill is a set of changes to the operation of the secretive Foreign Intelligence Surveillance Court, which is often asked to approve the government's intelligence actions. Currently the judges on the court hear the government's case without hearing an opposing side. Mr. Leahy's bill would create a panel of advocates to argue before the court in support of privacy rights and civil liberties, and would require the court to issue public summaries of its decisions that specifically detail the impact on those rights." Read more here.

-The House of Representatives is slated to consider several cybersecurity bills on Monday, including the National Cybersecurity and Critical Infrastructure Protection Act; the Critical Infrastructure Research and Development Act; the Homeland Security Cybersecurity Boots-on-the-Ground Act; and the Safe and Secure Federal Websites Act of 2013.

Cyber Security Policy News

-The Washington Post last week delved into how and why the National Security Agency tends to keep its custom malicious software tools and other spy toys to itself and away from law enforcement agencies. "The prospect that classified capabilities could be revealed in a criminal case has meant that the most sophisticated surveillance technologies are not always available to law enforcement because they are classified," writes The Post's Ellen Nakashima. "And sometimes it's not just the tool that is classified, but the existence itself of the capability — the idea that a certain type of communication can be wiretapped — that is secret."

-A newly disclosed government rulebook reveals just how easy it is to get placed on a terrorist watch list—and how difficult it can be to get taken off, according to The National Journal. "So broad are their criteria that an individual is able to be placed onto a watch list—and kept there—even if he or she is acquitted of a terrorism-related crime. Additionally, the guidelines note that a deceased person's name may stay on the list because such an identity could be used as an alias by a suspected terrorist," The NJ's Dustin Volz writes. "The rationale for adding someone to a watch list has gone from broad and opaque under the Bush administration to even more expansive under the Obama administration."

-Wired.com's Kim Zetter writes about a new technology startup called Dark Mail that plans make it easier to hide your metadata from the NSA. "Metadata is the pernicious transaction data involving the 'To', 'From' and subject fields of email that the NSA finds so valuable for tracking communications and drawing connections between people. Generally, even when email is encrypted, metadata is not. Dark Mail ambitiously aims to

revamp existing email structures to hide this data while still making the system universally compatible with existing email clients.

- The highest court in Wisconsin has upheld the warrantless use of cell phone tracking devices, better known as "stingrays." As Ars Technica reports, the court found that while the Milwaukee police did not specifically have a warrant to use the stingray to locate a murder suspect, it did have a related judicial order that essentially served the same purpose. "The court order specifically approved 'the installation and use of a trap and trace device or process,' and 'the installation and use of a pen register device/process, and 'the release of subscriber information, incoming and outgoing call detail…and authorizing the identification of the physical location of a target cellular phone,'" Cyrus Farivar writes. "Earlier this year, Wisconsin passed a new law that specifically requires a probable cause warrant in order to track someone's phone. That law was not in effect at the time of the 2009 murder."

-The European Central Bank (ECB) Web site was hacked last week, with the intruders stealing personal information and holding it for ransom. As the BBC reports, the hacker demanded money for stolen data, which included contact information for people who had registered for events at the ECB. The hack plus ransom demand followed similar intrusion and extortion attacks against the Wall Street Journal and Vice, and experts say the same hacker has claimed credit for both.

- A former employee at the U.S. Internal Revenue Service and two others were arrested and charged in an alleged identity theft scheme involving the theft of personally identifying information on individuals to open credit card accounts and make fraudulent purchases that totaled more than $1.2 million, GovInfoSecurity reports. "After the information was stolen from the victims, the conspirators allegedly opened up credit card accounts in the victims' names or added themselves as authorized users of the victims' existing accounts, authorities say," Jeffrey Roman writes. "The conspirators then allegedly used the accounts to buy goods and services at locations throughout California."

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.