GW CSPRI Newsletter

July 29, 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

-July 29, 9:30 a.m. - 11:00 a.m., **Iran: How a Third Tier Cyber Power Can Still Threaten the United States** - While hopes for a diminution of US-Iran differences have risen since the election of Hassan Rouhani as Iran's next president, neither Iran nor the United States are likely to stop efforts to probe for weaknesses in each other's cyber defenses and to investigate offensive options. The United States and Israel are believed responsible for the Stuxnet virus that destroyed 1,000 Iranian centrifuges in 2010 and Iran is alleged to have responded last year with attacks on US financial institutions. Panelists will discuss Iran's capacity to mount damaging cyber attacks on US and allied targets and appropriate US strategy going forward. Cosmos Club Powell Room, 2121 Massachusetts Ave., NW. More information.

-July 30-31, **Global Intelligence Forum USA: Defining the Role of Intelligence for Cyber Missions** - Speakers from across the government, military, and industry will explore the role that the intelligence community can play in helping to ensure free and secure cyberspace operations – from setting requirements, to collecting and analyzing data, to delivering insights and recommendations. The discourse will look at where industry can partner with the government to provide cyber situational awareness and indications and warning. National Press Club, 529 14th St. NW. More information.

-July 31, 10:00 a.m., S**trengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs** - The Senate Judiciary Committee will hold a hearing. Witnesses will include James Cole, deputy attorney general, U.S. Justice Department; John C. Inglis, deputy director, National Security Agency; Robert S. Litt, general counsel, Office of the Director of National Intelligence; Sean M. Joyce, deputy director, Federal Bureau of Investigation; James G. Carr, senior judge, U.S. District Court for the Northern District of Ohio; James Jaffer, deputy legal director, American Civil Liberties Union; and Stewart Baker, partner, Steptoe & Johnson LLP. Dirksen Senate Office Bldg., Room 226. More information. .

-July 31, 1:00 p.m. - 2:30 p.m., **Leaks Happen! The Digital Security Gamble: How to Mitigate the High Stakes, Exposures, and Cost** - The American Bar Association will host a webcast panel discussion. The speakers will be Maureen Feinroth, principal, Capital Privacy Solutions; Rich Fruehauf, assistant general counsel, Westinghouse; Zara Gerald, assistant general counsel, Gemalto; Ben Wilson, general counsel, DigiCert; and Marc Pearl, president and CEO, Homeland Security & Defense Business Council. More information.

-Aug. 2, 9:00 a.m., **Examining the Skyrocketing Problem of Identity Theft Related Tax Fraud at the IRS** - The House Committee on Oversight and Government Reform will hold a hearing. Rayburn House Office Bldg., Room 2247. More information.

-Aug. 7, 2:00 p.m. - 3:00 p.m., **Data Privacy Best Practices: How to Avoid Insider Threats and the Headlines** - Julie Lockner, vice president of information lifecycle management strategy at Informatica, will lead a webinar to discuss new and existing sources of data theft and exposure; data-centric security approaches; best practices for deployment and ongoing compliance; and customer case studies. More information.

Legislative Lowdown

- A U.S. spy program that sweeps up vast amounts of electronic communications survived a legislative challenge in the House of Representatives on Wednesday, the first attempt to curb the data gathering since former NSA contractor Edward Snowden revealed details of its scope. Reuters reports that the House of Representatives voted 217-205 to defeat an amendment to the defense appropriations bill that would have limited the National Security Agency's ability to collect electronic information, including phone call records.

While the vote was a defeat for privacy and civil liberties activists, some opponents are feeling emboldened by the closeness of the vote, according to The Hill. Critics of the agency are reviewing their options and plotting their next move in an attempt to build on their surprisingly strong showing. The House amendment, authored by Rep. Justin Amash (R-Mich.), would have defunded the NSA's controversial collection of phone records. It drew opposition from both parties' leaders, national security officials and the White House, but still attracted the support of 94 Republicans and 111 Democrats in falling just seven votes short of passage.

-In other news, The Hill writes that The Senate Commerce Committee plans to mark up an industry-backed cybersecurity bill next week before Congress breaks for its August recess,

making the panel the first in the upper chamber to move forward on legislation that's aimed at protecting critical infrastructure from cyber attacks. The bill would codify a section of President Obama's cybersecurity order that tasks the Commerce Department's National Institute of Standards and Technology (NIST) to work with businesses to craft a framework of cybersecurity best practices and standards. In accordance with the president's order, NIST has held workshops with industry groups across the country to start drafting the framework and is on track to complete a preliminary version of it by October.

Cyber Security Policy News

-Ars Technica reports that the Director of National Intelligence (DNI) released a statement saying that its authorization to compel telephone companies to share metadata has been renewed by the Foreign Intelligence Surveillance Court. In early June, The Guardian published a document showing that Verizon was compelled to share call records of all of its customers with the National Security Agency (NSA). It is widely believed that similar orders exist for the other telecommunications companies and include both landline and mobile providers. But in a written statement, the DNI argued that there is no "legitimate expectation of privacy" over metadata, the information about communications that tells who called or email whom, and at what time. "Consistent with his prior declassification decision and in light of the significant and continuing public interest in the telephony metadata collection program, the DNI has decided to declassify and disclose publicly that the Government filed an application with the Foreign Intelligence Surveillance Court seeking renewal of the authority to collect telephony metadata in bulk, and that the Court renewed that authority. This surveillance is not authorized by Section 215 and violates the First and Fourth Amendments. Plaintiffs bring this suit to obtain a declaration that the Mass Call Tracking is unlawful; to enjoin the government from continuing the Mass Call Tracking under the VBNS order or any successor thereto; and to require the government to purge from its databases all of the call records related to Plaintiffs' communications collected pursuant to the Mass Call Tracking."

The move by the DNI comes a week after the Obama administration said it was completely legal for the government to hoover up mountains full of call and email metadata from Americans. Wired.com writes that the administration for the first time responded to a Spygate lawsuit, telling a federal judge the wholesale vacuuming up of all phone-call metadata in the United States is in the "public interest," does not breach the constitutional rights of Americans and cannot be challenged in a court of law.

-Smartphone users may soon receive notices on their devices about the sorts of information their mobile apps are collecting on them. App developers and other business groups agreed last week to begin testing the notices, which would disclose the type of information an app is collecting, such as browsing history, location data, contacts, and text logs. The notices would also detail whether the information is being shared with third parties, such as advertisers. Politico writes that the groups supporting the code are "fairly extensive, including CDT, EFF, and ACLU on the privacy side, and AT&T, CTIA, and CCIA and the Internet Commerce Coalition from industry. But participants are expected to reconvene in some form a few months after testing, and that's when we'll learn more about who's actually going to put the policies in place."

A new report (pdf) from the Center for Strategic and International Studies (CSIS), a Washington think-tank, published in association with the software security firm McAfee attempts to estimate the annual losses of from cyber crime and cyber espionage. In it, writes Quartz, the authors tentatively suggested a wide variety of numbers and then attempt to contextualize each of them. One big problem with estimating losses is the number of factors involved. For example, it emerged last week that over $300 million was stolen by hackers from a variety of US companies between 2005 and 2012. As The Wall Street Journal notes, the study put the annual tally at $100 billion each year. Given that McAfee's prior estimates put the annual losses at 10 times that amount -- $1 trillion annually -- some might conclude that cybercrime has somehow become far less expensive for consumers and businesses. After all, The Journal notes, that $100 billion figure is 1% or less of U.S. gross domestic product and, for companies, puts cyber theft losses among a variety of costs incurred in the course of doing business.

Reuters writes that when asked if the No. 2 security software vendor would remove the trillion-dollar estimate from its website, McAfee Vice President of Government Relations Tom Gann said that was "a good question" but that he didn't know the answer. "This study here is newer, it's based on extra rigorous work, and once it's made public, this is clearly the one we're going to focus on," Gann said.

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.