GW CSPRI Newsletter

August 26, 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.

Announcement: CSPRI's blog, The CSPRI Byte, has gone live! Our blog is student-and-alumni-run on all things cybersecurity. Check out our articles written by CSPRI affiliates to find out how cybersecurity plays a role in intelligence, diplomacy, business, healthcare, education, and more!

Contents

Events

-Aug. 27, 2:00 p.m. - 3:00 p.m., **Ensuring Application Security in a Mobile World** - As mobility becomes a top priority on the federal technologist's agenda, many agencies are developing mobile apps to better serve their customers. However, security concerns can slow agency momentum toward mobile computing. This Webcast will highlight the major security areas are for mobile applications; the difference between device and application security; and how to secure mobile applications and support BYOD as an option for partners, contractors, and customers. Speakers will include Pam Hird, senior project manager and CAPI program manager, National Agriculture Statistics Service, U.S. Department of Agriculture; Tom Suder, president, Mobilegov; and Tom Voshell, senior director, solutions engineering, SAP Regulated Industries. More information.

-Aug. 28, 1:00 p.m., **Winning the War on Account Takeover Fraud: A Global Top 500 Bank's Journey** - A discussion of how Entersekt and Nedbank defeated cybercriminals. More information.

-Aug. 29, 7:00 p.m. - 10:00 p.m., **CharmSec Meetup** - Part of the CitySec movement, this is a monthly informal meetup of information security professionals in Baltimore. Heavy Seas Alehouse, 1300 Bank Street, Baltimore, MD, 21231. More information.

-Sept. 5, 6:00 p.m. - 7:45 p.m., **Mindforge Meetup** - As a follow up to its previous primer on lockpicking and physical security, this meetup will feature a full lockpick village. Deviant Ollam of The Open Organization of Lockpickers will be there along with Tenacity Director Shane Lawson to teach, demonstrate, and train attendees in basic and more advanced techniques. Bechtel Conference Center, 1801 Alexander Bell Drive, Reston, VA, 20191. More information.

-September 7, 5:30 p.m. – 8:00 p.m. "**The Lives of Others". Free Movie Screening and Panel Discussion** – CSPRI will kick-off the fall semester with a screening of the German film ***The Lives of Others***, which won the 2006 Academy Award for Best Foreign Language Film and is a political thriller and human drama about life in a surveillance state Right after the film, there will be a short multidisciplinary panel discussion on cybersecurity, privacy in the age of Big Data, and state and commercial surveillance. The panelists will include Prof. Peter Hayes of the Elliot School of International Affairs, Prof. Lance Hoffman, CSPRI Director, and Evan Sills, a recent GW Law grad who has just finished a study of cybersecurity for the American Bar Association. This event is supported by the Office of the Vice President for Research Centers and Institutes Facilitating Fund and should appeal to students (and faculty) watching with interest the current surveillance revelations Betts Theater, Marvin Center, 800 21st St NW.

-Sept. 8-14, **2013 ASE/IEEE International Conference on Privacy, Security, Risk and Trust** - The goal of this week-long conference is to provide an international forum for information privacy, risk, trust, and security researchers and practitioners to explore solutions to profound challenges on privacy, risk, trust, and security issues and exchange recent progresses.. Hilton Alexandria Mark Center, 5000 Seminary Road, Alexandria, Va. 22311. More information.

Legislative Lowdown

The House and Senate are in August recess.

Cyber Security Policy News

-The field of cybersecurity has experienced rapid growth in recent years. But one thing that seems to be lagging behind is diversity in its workforce. Carrie Madren reports that universities across the country are beginning to offer degrees in cybersecurity, as well as related scholarships, and researchers are suggesting policy options to improve diversity. Educators hope that more women and minorities will establish a presence within the field.

- Bloomberg reported last week that NSA analysts have “deliberately ignored restrictions on their authority to spy on Americans multiple times in the past decade.” The disclosure comes despite claims by government officials that Americans need not worry about NSA surveillance because of a lack of cases in which the system was willfully abused. According to Bloomberg, an average of one case of intentional abuse per year has been documented in internal reports. The incidents, chronicled by the NSA’s inspector general, provide additional evidence that U.S. intelligence agencies sometimes have violated the legal and administrative restrictions on domestic spying, and may add to the pressure to bolster laws that govern intelligence activities.

Meanwhile, The Wall Street Journal wrote last week that NSA officers on several occasions have channeled their agency’s enormous eavesdropping power to spy on love interests. The practice is not frequent — one official estimated a handful of cases in the last decade — but it is common enough to garner its own spycraft label: LOVEINT. Spy agencies often refer to their various types of intelligence collection with the suffix of “INT,” such as “SIGINT” for collecting signals intelligence, or communications; and “HUMINT” for human intelligence, or spying. According to The Journal, the “LOVEINT” examples constitute most episodes of willful misconduct by NSA employees.

Across the pond in Germany, Der Spiegel reported that the NSA successfully cracked the encryption code protecting the United Nations’ internal videoconferencing system. According to documents unearthed by Der Spiegel, the United States was not just busy spying on the European Union, but had its surveillance apparatus trained on the international body as well. The publication reported that the electronic breaching of the UN, which is headquartered in New York, occurred in the summer of 2012. Within three weeks of initially gaining access to the UN system, the NSA had increased the number of such decrypted communications from 12 to 458.

The Obama administration is pointing to the revelations about NSA missteps as evidence that "all these safeguards, checks, audits," in effect, worked as designed. In an interview with CNN, Obama expressed confidence that no one at the spy agency would use its surveillance abilities to spy on Americans. "This latest revelation that was made, what was learned was that NSA had inadvertently, accidentally pulled the emails of some Americans in violation of their own rules because of technical problems that they didn't realize," Obama told CNN's "New Day" in an interview that aired last week.

At the same time, a group of veteran security experts and former White House officials has been selected to conduct a full review of U.S. surveillance programs and other secret government efforts disclosed over recent months, ABC News reports. The recent acting head of the CIA, Michael Morell, will be among what President Obama called a "high-level group of outside experts" scrutinizing the controversial programs. Joining Morell on the panel will be former White House officials Richard Clarke, Cass Sunstein, and Peter Swire. An announcement is expected Thursday, a source told ABC News’ Jon Karl. The group will "consider how we can maintain the trust of the people [and] how we can make sure that there absolutely is no abuse," President Obama said two weeks ago when announcing the group’s formation, without identifying who would be on the panel.

-The Department of Homeland Security last week awarded more than $6 billion in contracts to 17 vendors for a variety of cybersecurity tools and services, The Federal Times writes. Most large civilian agencies have agreed to use the contract, which will provide diagnostic tools for agencies to quickly identify and fix the most serious cyber risks in their networks. The year-long contract has four option years, and DHS has committed $185 million this fiscal year to launch the first of three phases under the Continuous Diagnostic and Mitigation Program. The General Services Administration awarded the blanket purchase agreement on behalf of DHS, and GSA will charge agencies a 2 percent fee to use the contract.

All of this cyber acquisition by DHS has The Washington Times' Andrew Scarpitta wondering what has become of American ingenuity in the cybersecurity space. The Times notes that DHS's just-announced integration of IBM software into its Continuous Diagnostics and Mitigation (CDM) program comes a day after IBM's announcement that it has acquired the Israeli cyber defense powerhouse company, Trusteer. The programs DHS will use from IBM will help transform the nation's security networks from an antiquated system to a system that focuses on combatting attacks in real-time. "Trusteer, an Israel company, currently serves as the main cyber security provider to 7 of the top ten American banks and nine of the top ten UK firms. It specializes in defending against financial fraud and advanced security threats, two things that both Israel and the US experience all too often," Scarpitta writes. "But how does a nation of 7.8 million people with the world's 49th largest GDP which experiences 100,000 cyber-attacks a day outproduce a country of 313 million with the world's largest GDP where the National Nuclear Security Administration faces up to 10 million Cyber-attacks daily?"

-A new report from the Pew Research Center's Internet & American Life Project finds that more than half of American teens have opted not to install a mobile app due to worries about privacy. Dark Reading reports that while nearly 60 percent of American teenagers between the ages of 12 and 17 have downloaded an app on their smartphones or tablets, it appears many of them actually do pay attention to how much information they have to share in return. Some 26 percent uninstalled an app after discovering it was collecting some of their personal information, and 46 percent say they have disabled location-tracking on their devices due to privacy concerns. Girls lead the anti-location tracking trend, with 59 percent of teen girls turning off the feature, versus 37 percent of boys. According to the report, the teens are avoiding location-tracking due to concerns that companies would be able to access information on their phones.

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.