GW CSPRI Newsletter

October 21, 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.

New in CSPRI's blog, The CSPRI Byte:
Corrie Becker, *The Tallinn Manual: Legal Aspects of Cyber Warfare*

Contents

Events

(Access the CSPRI Events calendar here.)

*Events in blue are CSPRI related.

-Oct. 21, 5:30 p.m. - 8:30 p.m., **NoVa Hackers Association Meetup** - This informal group of security professionals from around the NoVA/DC area coordinates one or two monthly events – an evening meetup with presentations on the second Monday of the month and various lunch or bar meetups. SRA International, 4300 Fair Lakes Ct., Fairfax, 22033. More information.

-Oct. 22, 4:00 p.m., **Cyber Security Strategy: Why We're Losing and What's Needed to Win** - Backed by powerful, real-world examples of threat actor tactics, this presentation will help managers develop a better understanding of how their current security approach is most likely to succeed or fail over time, and what strategies are the most likely to shift the advantage to the good guys. The speaker, Steve Chabinsky, recently returned to the private sector after a distinguished career with the FBI, where he served most recently as Deputy Assistant Director of the Cyber Division. At CrowdStrike, he is chief risk Officer and Senior Vice President of Legal Affairs. He also serves as an adjunct faculty member of George Washington University. Capitol College's Avrum Gudelsky Memorial Auditorium, 11301 Springfield Road, Laurel, MD 20708. More information.

-Oct. 23, 3:00 p.m., **Cyber Risk Wednesday** - This event brings cyber experts from government and industry together with policymakers to examine topics at the core of the Cyber Statecraft Initiative's study of interrelated cyber hazards and underlying concentration of risks. The series is designed to expose stakeholders from the technology, policy, and risk management communities to vibrant new cyber topics and provide a venue for the exchange of ideas. This event will introduce the joint effort by the Atlantic Council and Zurich Insurance to understand how global aggregation of cyber risks could cause systemic shocks and ways, such as insurance and resilience, to mitigate them. A moderated discussion will analyze systemic cyber risks and explore their implications on the future of the internet. The panel will feature Larry Castro, managing director at The Chertoff Group, whose prior government service includes over four decades at the National Security Agency. 1030 15th Street, NW, 12th Floor. More information.

-Oct. 23, 12 noon - 1:30 p.m., **Big Surveillance: What the NSA is Doing, Why it Matters, and How to Address It** - GW Professor and CSPRI researcher Daniel Solove will address recent revelations about NSA surveillance and the legality of these activities, as well as how the debate between privacy and national security is often focused on wrong assumptions, faulty premises, and false trade-offs. Jacob Burns Moot Court Room, Burns Hall 1st Floor, 716 20th Street NW.

-Oct. 23, 8:30 a.m. - 10:00 a.m., **Cybersecurity** - The Center for Strategic and International Studies (CSIS) will host an on site and Webcast panel discussion. The speakers will be Rep. Mike Rogers (R-Mich.), Michael Chertoff, chairman and co-founder, Chertoff Group; James Lewis (CSIS); and Tim Pawlenty, president, Financial Services Roundatable. Registration to attend on site has closed. This event will be Webcast. CSIS, 212-C Concourse Level, 1616 Rhode Island Ave., NW. More information.

-Oct. 23, 12:00 noon - 1:00 p.m., **Advertising, Consumer Protection, & Privacy Law: An Emerging Practice with Exciting Career Opportunities** - The American Bar Association will host an on site and teleconferenced panel discussion. The speakers will be David Conway, Venable; Andi Arias; FTC's Division of Privacy & Identity Protection; Donnelly McDowell, Kelley Drye; Ella Krainsky, FTC's Division of Advertising Practices; and Mona Thakkar, Volkswagen Group. George Washington University Law School, Lisner Hall, Room 201, 2023 G St., NW. More information.

-Oct. 24, 10:00 a.m., **NSA Programs** - The House Intelligence Committee (HIC) will hold a hearing. Rayburn House Office Bldg. Room 2167. More information.

-Oct. 24, 6:00 pm, **Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet** will be presented in a special open class session of CSci 6534, Cybersecurity and Governance. The speaker will be Prof. Steven Bellovin of the Computer Science Department at Columbia, one of the creators of Netnews (most commonly known as Usenet) and until Chief Technologist for the Federal Trade Commission. GW Rome Hall Room 352, 801 22nd St. NW.

-Oct. 25, 12 noon - 1:00 p.m., **The NSA Internet Surveillance System: Who Has Oversight and How Transparent is the Program?** - Who's watching the watchers? And are programs like the NSA massive data collection programs transparent enough for those with oversight authority to be able to understand the scope of the system? This expert panel will discuss the oversight and transparency aspects of the growing controversy over the NSA's surveillance system. Rayburn House Office Bldg., Room 2226. More information.

-Oct. 25, 1:00 p.m. - 2:30 p.m., **Am I Competent? The Ethical Use of Evolving Technologies** - The American Bar Association will host a Webcast panel discussion. The speakers will address acting competently when using new technologies, such as social media, smartphones and cloud computing services. The speakers will be Daniel Crothers, Justice of the Supreme Court of North Dakota; Andrew Perlman, Suffolk Law School; and Ellyn Rosen, ABA. More information.

Legislative Lowdown

-At 9:00 a.m. on Oct. 24, the House Homeland Security Committee will meet to mark up several bills, including HR 3107, "Homeland Security Cybersecurity Boots on the Ground Act;" and HR 2952, the "Critical Infrastructure Research and Development Advancement Act of 2013". This markup will be Webast. Rayburn House Office Bldg., Room 311. More information.

Cyber Security Policy News

-"An identity theft service that sold Social Security and drivers license numbers — as well as bank account and credit card data on millions of Americans — purchased much of its data from **Experian**, one of the three major credit bureaus, according to a lengthy investigation by KrebsOnSecurity", just released today.

-Europe's crime fighting agency says the internet is being used to facilitate the international drug trafficking business. As the BBC writes, Europol Direcotr Rob Wainwright said that drug traffickers recruited hackers to break into IT systems that controlled the movement and location of containers. According to the BBC, "the attack on the port of Antwerp is thought to have taken place over a two-year period from June 2011. Prosecutors say a Dutch-based trafficking group hid cocaine and heroin among legitimate cargoes, including timber and bananas shipped in containers from South

America. The organized crime group allegedly used hackers based in Belgium to infiltrate computer networks in at least two companies operating in the port of Antwerp. The breach allowed hackers to access secure data giving them the location and security details of containers, meaning the traffickers could send in lorry drivers to steal the cargo before the legitimate owner arrived."

-Last week was a doozy for cybercrime security researchers and prognosticators. Researchers have discovered more than two dozen security holes in software and hardware powering critical infrastructure systems that could allow attackers to crack or hijack servers controlling sensitive national assets, including electric substations and water systems. The New York Times writes that the advisories concern vulnerabilities in the communication protocol used by power and water utilities to remotely monitor control stations around the country. "Using those vulnerabilities, an attacker at a single, unmanned power substation could inflict a widespread power outage," The Times writes. "Still, the two engineers who discovered the vulnerability say little is being done."

According to reporting from Wired.com, the vulnerabilities are found in devices that are used for serial and network communications between servers and substations. "These products have been largely overlooked as hacking risks because the security of power systems has focused only on IP communication, and hasn't considered serial communication an important or viable attack vector," Wired's Kim Zetter writes. "But the researchers say that breaching a power system through serial communication devices can actually be easier than attacking through the IP network since it doesn't require bypassing layers of firewalls. An intruder could exploit the vulnerabilities by gaining physical access to a substation — which generally are secured only with a fence and a webcam or motion-detection sensors — or by breaching the wireless radio network over which the communication passes to the server."

Meanwhile, an independent security expert has discovered that each mobile smartphone contains a tiny defect that can be used to uniquely identify the device. Security researcher Hristo Bojinov, a Ph.D. candidate in computer science at Stanford originally from Bulgaria, said his research shows that the tiniest defects in a mobile device's accelerometer — the sensor that detects movement — produces a unique set of numbers that advertisers could exploit to identify and track most smartphones. The San Francisco Chronicle has more on this story.

-New documents leaked by NSA whistleblower Edward Snowden suggest that the NSA has been systematically eavesdropping on the Mexican government for years. Der Spiegel features documents indicating that the NSA hacked into the president's public email account and gained insight on policymaking and the political system. According to Der Spiegel, the NSA has an entire division for particularly difficult missions known as "Tailored Access Operations" (TAO), which devises special methods for special targets.

The court that oversees NSA surveillance programs reauthorized the agency's collection of bulk telephone data despite legislative efforts to the contrary, saying that Congress had already approved the reauthorization of the program. The Hill writes that in a ruling declassified late last week, the Foreign Intelligence Surveillance (FISA) Court Judge Mary McLaughlin said she "supports a ruling from earlier in the year, reauthorizing Section 215 of the USA Patriot Act, which allows the National Security Agency to collect bulk telephone data. To justify her ruling, McLaughlin points to Congress' reenactment of Section 215 after receiving information about the government's ... interpretation of the statute."

-There is something to be said for security by obscurity. Just ask the justices on the nation's highest court: According an interview given by the high court's newest justice -- Elena Kagan -- the judges eschew email for old-fashioned paper and in-person communications. "And so we do a lot of our communicating by these, it looks, it's sort of 19th century," Kagan was quoted as saying in an interview at the Fortune Most Powerful Women Summit at the Mandarin Oriental Hotel in Washington, D.C. last week. "It's very heavy ivory paper—it looks like it came out of the 1800s or something. But it seems to work pretty well," she added. "And when you think about it, how many emails have you sent that you wished you could take back? So, so we're careful and deliberative."

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.