GW CSPRI Newsletter

December 9, 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

-Dec. 9, 5:30 p.m. - 8:00 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. 4350 Fair Lakes Court, Fairfax, 22033. More information.

-Dec. 10, 2:00 p.m. - 5:00 p.m., **Risk Does Not Equal Threat** - Join Cylance's Chief Knowledge Officer, Dr. Shane Shook, along with industry experts Bob Bigman (President of 2BSecure and former CSO for the CIA) and Ulf Lindqvist (Program Director at SRI International) for a round-table discussion on how organizations can better distinguish between cyber threats and risks. SRI International, 1100 Wilson Blvd., 28th Floor, Arlington, VA 22209 More information.

-Dec. 11, 9:30 a.m., **Who's Watching Little Brother? Local Surveillance, National Concerns** - A panel discussion with leading scholars on privacy and national security. The discussion will seek answers to the following questions: Does federal support for fusion centers and suspicious activity reporting make sense? What can be done to mitigate the risks they pose to civil liberties, to prevent waste, and to improve oversight? Speakers will include Mike German, Senior Policy Counsel, American Civil Liberties Union; Eileen Larence, Director of Homeland Security and Justice Issues, Government Accountability Office; Michael Price, Counsel, Liberty & National

Security Program, Brennan Center for Justice; and Jim Harper, Director of Information Policy Studies, Cato Institute. Cato Institute, 1000 Massachusetts Ave, NW, Hayek Auditorium. The event also will be webcast live, at www.cato.org/live. More information.

-Dec. 11, 11:00 a.m. - 4:00 p.m., **ISACA CM Meetup: Supply Chain Risk Management** - Chapter meetings are usually held nine times per year (no meetings in June, July or August). The meetings are normally held on the second Wednesday of the month at various times (e.g., breakfast, lunch, and dinner meetings). Snyders Willow Grove Restaurant, 841 North Hammonds Ferry Road, Linthicum, MD, 21090. More information.

-Dec. 11, 1:00 p.m., **Ernst & Young's 2013 Global Information Security Survey: More money, More Problems?** - Financial institutions continue to increase their investment in cybersecurity, with 47% reporting an increase of at least 5% over the last year. But with greater scrutiny from the board, regulators and other stakeholders, the real measure is the return on those investments, a figure that proves elusive for even the most sophisticated organizations. When it comes to cybersecurity, there is no magic number and more money doesn't always mean less problems. This webinar will discuss ways to re-evaluate and reallocate investments to better meet today's threats. More information.

-Dec. 11, 2:00 p.m., **Continued Oversight of U.S. Government Surveillance Authorities** - The Senate Judiciary Committee will hold a hearing. The witnesses will include Keith B. Alexander, director National Security Agency; James Cole, deputy attorney general, Department of Justice; Robert S. Litt, general counsel, Office of the Director of National Intelligence; Edward Black, president & CEO, Computer & Communications Industry Association; Julian Sanchez, research fellow, Cato Institute; Carrie F. Cordero, adjunct professor of law, Georgetown Law, director, National Security Studies at Georgetown University Law Center. Dirksen Senate Office Bldg., Room 226. More information.

-Dec. 11, 5:00 p.m. - 7:00 p.m., **ISSA Baltimore Meetup** - The primary goal of the Information Systems Security Association, Inc. (ISSA) is to promote management practices that will ensure the confidentiality, integrity and availability of organizational information resources. The Baltimore Chapter is a local resource to be used by members and non-members alike. Chapter meetings are normally held on the fourth Wednesday of every month. Cybercore Technologies, 6605 Business Parkway, Elkridge, MD, 21075. More information.

-Dec. 11-12, **Law Enforcement, Homeland Security Forum and Technology Expo** - This conference will feature several talks on cybersecurity. The speakers will include Joseph Demarest, assistant director, FBI, Cyber Division; Daniel Gerstein, assistant undersecretary, Department of Homeland Security, Science and Technology; and David Aucsmith, senior director, Institute for Advanced Technology in Governments, Microsoft Corporation. National Reconnaissance Office (NRO), J.D. Hill Conference Center, 14675 Lee Road, Chantilly, VA 20151-1715 More information.

-Dec. 12, 3:30 p.m. - 4:30 p.m., **National Cyberwatch Center's Cybersecurity Education Solutions for the Nation** - Headquartered on the Largo campus of Prince George's Community College, the National CyberWatch Center is focused on leading and supporting collaborative

efforts to advance cybersecurity education and strengthen the national cybersecurity workforce. The 120-member cybersecurity consortium, which is funded by a grant from the National Science Foundation (NSF), along with a list of industry and government partners, will celebrate its expansion into a national program on Thursday. Center for Advanced Technology building, Room 110, 301 Largo Rd, Kettering, MD 20774. More information.

-Dec. 16, 6:00 p.m. - 9:00 p.m., **The Role of Circumvention Tools in Internet Filtering Countries** - Countries throughout the world filter Internet content, including Iran, China, Cuba, and Vietnam, among others. Find out why users adopt different censorship circumvention tools, and the impact and role they play in their respective countries. 1899 L Street, N.W., Suite 400. More information.

-Dec. 17, 6:30 p.m. - 8:30 p.m., **ISSA DC Chapter: DNS Security** - Matt Bianco of InfoBlox will take a look at how mobile device proliferation is adding to the strenuous task of maintaining and allowing access to the network, and how adding security at that layer can aid in incident response. Government Printing Office, 732 North Capitol Street, Washington, DC, 20401. More information.

-Dec. 18, 2:00 p.m. - 3:00 p.m., **State of the Hack** - Mandiant's Chief Security Officer Richard Bejtlich will be joined by Kelly Jackson Higgins, senior editor at DarkReading and Kristen Verderame, chief executive officer at Pondera International to share highlights from the past twelve months. The Webinar discussion will center around high profile security events of 2013, thoughts on what's working in security and what needs improvement, and what to expect in 2014. More information.

-Dec. 18, 3:00 p.m., **Cyber Risk Wednesday: Risks and Resilience of the Electrical Sector** - The third Cyber Risk Wednesday discussion will focus on cybersecurity challenges facing this important sector and methods of reducing the existing and future vulnerabilities. The panel will feature Gib Sorebo, the chief cybersecurity technologist at Leidos and Tom Parker, the chief technology officer of FusionX. Additional speakers will be announced. The Atlantic Council, 1030 15th Street NW, 12th Floor. More information.

-Dec. 19, 2:00 p.m., **BlackHat 2013 Infosec Year in Review** - Whichever metrics you choose to employ, 2013 was a bumper year for the information security industry: An unholy mix of advanced research and APT attacks. "Cyberwar" started the year strong but lost ground to "opsec" as the year's most overused (but least understood) terms. Speakers in this Webcast will include Haroon Meer, founder of Thinkst; Marco Slaviero, lead researcher at Thinkst; and Amit Yoran, senior vice president of unified products at RSA and former director of the National Cybersecurity Division and US-CERT at the Department of Homeland Security. More information.

-Dec. 19, 7:00 p.m. - 9:00 p.m., **CharmSec Meetup** - Part of the CitySec movement, this is a monthly informal meetup of information security professionals in Baltimore. Unlike other meetups, you aren't expected to pay dues, "join up", or present a zero-day exploit to attend. Heavy Seas Alehouse, 1300 Bank Street, Baltimore, MD, 21231. More information.

Cyber Security Policy News

-Fresh leaks from NSA whistleblower Edward Snowden indicate that the National Security Agency gathers location data on hundreds of millions of cell phones around the world, enabling the agency to track the movements of individuals — and map their relationships — in ways that would have been previously unimaginable, The Washington Post reports. According to The Post, the records "feed a vast database that stores information about the locations of at least hundreds of millions of devices, according to the officials and the documents, which were provided by former NSA contractor Edward Snowden. New projects created to analyze that data have provided the intelligence community with what amounts to a mass surveillance tool," Barton Gellman and Ashkan Soltani wrote. "The NSA does not target Americans' location data by design, but the agency acquires a substantial amount of information on the whereabouts of domestic cellphones "incidentally," a legal term that connotes a foreseeable but not deliberate result. "

While an official quoted by The Post told the publication that the mobile phone data gathered by the NSA are not covered by the Fourth Amendment -- meaning that a probable-cause warrant isn't required to get it -- that interpretation is far from grounded in established and clear legal precedent, according to Wired.com. "In reality, however, the case law on cell-site locational tracking — while generally favorable to the government — is far from clear, with federal courts and appellate courts offering mixed rulings on whether warrants are needed," writes Wired's David Kravets. "Warrantless cell-phone location tracking has become a de facto method to snoop on criminals in the wake of the Supreme Court's decision that probable-cause warrants from judges are generally needed to affix covert GPS devices to vehicles. Yet the mobile-phone location data issue has never been squarely addressed by the Supreme Court, and the dispute isn't likely to be heard by the justices any time soon. All of which means that the legality of the latest crime- or terror-fighting method of choice is equally up in the air."

-Computer scientists in Germany have proposed a groundbreaking, proof-of-concept strain of malicious software capable of infecting and spreading between computers that are not connected to networks. Ars Technica reports that the malware can spread from one computer to the next using audio signals that are beyond the range of human hearing. "The proof-of-concept software—or malicious trojans that adopt the same high-frequency communication methods—could prove especially adept in penetrating highly sensitive environments that routinely place an "air gap" between computers and the outside world," writes Dan Goodin. "Using nothing more than the built-in microphones and speakers of standard computers, the researchers were able to transmit passwords and other small amounts of data from distances of almost 65 feet. The software can transfer data at much greater distances by employing an acoustical mesh network made up of attacker-controlled devices that repeat the audio signals." The publication notes that the discovery comes not long after an independent security consultant told Ars his computers were infected with a mysterious piece of malware that used high-frequency transmissions to jump air gaps.

-The Obama administration on Tuesday said it plans to review the privacy implications of facial recognition technology. The Hill's Kate Tummarello writes that some lawmakers and privacy

advocates are worried that tech companies and government agencies are using facial recognition technologies to track people, often without their knowledge. The Commerce Department said it recognizes those concerns and will work with tech groups, privacy advocates and online advertising trade associations to identify them.

At the same time, The Hill reports, titans of the technology industry are coming together in a campaign to lobby for wide-ranging reforms to the National Security Agency. "Google, Facebook, Twitter, Yahoo, Microsoft, Apple, LinkedIn and AOL are setting aside their business rivalries to demand that Congress and President Obama scale back the government's voracious surveillance," The Hill writes, citing bits from an open letter to The White House that appears in print newspapers nationwide today. "[T]his summer's revelations highlighted the urgent need to reform government surveillance practices worldwide," the letter reads. "The balance in many countries has tipped too far in favor of the state and away from the rights of the individual — rights that are enshrined in our Constitution. … It's time for change."

Mobile phones aren't just being used for spying; The Federal Trade Commission last week announced a privacy settlement with the makers of one of the most popular mobile apps for Android devices. According to the FTC, Goldenshores Technologies LLC, the company behind the "Brightest Flashlight Free," deceptively failed to disclose that the app transmitted users' precise location and unique device identifier to third parties, including advertising networks. In addition, the complaint alleges that the company deceived consumers by presenting them with an option to not share their information, even though it was shared automatically rendering the option meaningless.

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.