GW CSPRI Newsletter

July 14, 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

Announcement 1
Events 1
Legislative Lowdown 3
Cyber Security Policy News 3

Announcement

CSPRI Director Lance Hoffman presented a keynote address on the Internet of Things at the IoT Privacy Summit in Silicon Valley last week. Catch his remarks here.

Events

-July 15, 2:30 p.m. – 3:30 p.m., **Securing the U.S. Electrical Grid** - The event will feature a panel made up of project co-chairs, Mack McLarty and Tom Ridge, as well as House Permanent Select Committee on Intelligence Chairman Mike Rogers (R-Mich.), and Ranking Member Dutch Ruppersberger (D-Md.). Hyatt Regency Capitol Hill, 400 New Jersey Ave. NW. Please RSVP to Hurst.Renner@thePresidency.org.

-July 15, 2:30 p.m., **Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks** – Dirksen Senate Office Bldg., Room 226. More information.

-July 15, 6:30 p.m. – 8:00 p.m., **ISSA DC Chapter: Social Media and the Insider Threat** – This talk will be given by Terry Gudaitis, currently the owner of Mindstar Security & Profiling, LLC. Center for American Progress, 1333 H Street, NW. More information.

-July 16, 12:30 p.m. – 2:00 p.m., **Protecting Our Data: A Conversation about Credit Card Security & Online Transactions** - Senator Richard Blumenthal (D-Conn.) will host a discussion about how many flows through the financial system. The event will also feature Maarten Bron, international data security and electronic transactions expert with Underwriters Laboratories. Senate Russell Bldg., Room 385.

-July 16, 6:00 p.m. – 9:00 p.m., **NovaInfosec West Meetup** – If you are in the IT security business, like the idea of meeting to discuss the foibles of the industry, demo your recent discovery and conquest, or just drink a beer with like minded folks, then this meeting is for you. Lost Rhino Brewing Co., 21730 Red Rum Dr # 142, Ashburn, VA. More information.

-July 17, 5:30 p.m. – 8:30 p.m., **A Primer on Cyber Threat Intelligence** - It's the latest trend and marketing phrase. How is it really new or different? How is it distinct from threat feeds? How does the IT security organization use intelligence to defense and be proactive? This talk will be an operations level discussion of how an end to end cyber threat intelligence program works. And how cyber threat intelligence flows across the enterprise. Lockheed Martin, 13560 Dulles Technology Drive, Herndon, VA. More information.

-July 21, 4:00 p.m. – 5:30 p.m., **Living With Cyber Insecurity: Reducing the National Security Risks of America's Cyber Dependencies** – This event will feature a panel discussion of proposals for U.S. government responses to cyber insecurity by the Honorable Richard Danzig and the rollout of a major new report from the Center for New American Security: "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies." Abelson/Haskins Conference Room, American Association for the Advancement of Science, 1200 New York Avenue NW. More information.

-July 21, 5:30 p.m. – 8:00 p.m., **NoVA Hackers Association Meetup** – SRA International, 4350 Fair Lakes Court, Fairfax, VA, 22033. More information.

Legislative Lowdown

-The Senate Select Committee on Intelligence last week approved the Cybersecurity Information Sharing Act of 2014, largely without alteration even though it has drawn severe criticism from privacy and civil liberties groups. As Forbes reports, the bill is intended to help companies and the government thwart hackers and other cyber-intrusions. "Civil liberties advocates have opposed CISA, arguing that it fails to adequately shield Americans' privacy," Forbes writes. "Proponents of the bill say it will help stop attacks by encouraging data-sharing between businesses and the government."

Cyber Security Policy News

-A four-month investigation by The Washington Post reveals that ordinary Americans – foreigners and native-born citizens – are equally likely to be caught up in surveillance dragnets run by the National Security Agency (NSA). "Nine of 10 account holders found in a large cache of intercepted conversations, which former NSA contractor Edward Snowden provided in full to The Post, were not the intended surveillance targets but were caught in a net the agency had cast for somebody else," The Post wrote on July 5.

"Many of them were Americans. Nearly half of the surveillance files, a strikingly high proportion, contained names, e-mail addresses or other details that the NSA marked as belonging to U.S. citizens or residents. NSA analysts masked, or "minimized," more than 65,000 such references to protect Americans' privacy, but The Post found nearly 900 additional e-mail addresses, unmasked in the files, that could be strongly linked to U.S. citizens or U.S. residents."

In a follow-up piece published last Friday, The Post sought to clarify criticisms of its reporting, which called the piece alarmist and stating the obvious. The Post responded by breaking down the story into bite-sized chunks, and by retracing its steps in its reporting. "We found about 11,400 unique online accounts. Among them, about 1,200 were designated by the NSA as foreign targets. The remaining 10,000-plus were akin to digital bystanders. Some of them knew the NSA targets and conversed with them. Others fell into the pile by joining a chat room, regardless of subject, or using an online service hosted on a server that a target used for something else entirely."

-Chinese hackers earlier this year March broke into the computer networks of the United States government agency that houses the personal information of all federal employees, according to senior American officials, The New York Times revealed last week. "They appeared to be targeting the files on tens of thousands of employees who have applied for top-secret security clearances. The hackers gained access to some of the databases of the Office of Personnel Management before the federal authorities detected the threat and blocked them from the network, according to the officials. It is not yet clear how far the

hackers penetrated the agency's systems, in which applicants for security clearances list their foreign contacts, previous jobs and personal information like past drug use."

-Malicious software has been discovered on tools at seven shipping and logistics companies across the globe that pulled the firms' financial, customer and operational data into a Chinese botnet, according to MarketWatch. "San Mateo, Calif.-based TrapX first detected the malware in the scanner software about six months ago while doing security testing for one shipping company, finding that 16 of the initial customer's 48 scanners from a Chinese manufacturer located near the schoolhouse were infected. In the last six months, the security company reached out to other customers of the scanner manufacturer and realized their scanners had the same malware. TrapX also informed the manufacturer, who denied any knowledge of the malware."

-A law being proposed in Russia would require citizens to store their data at data centers exclusively inside of the country. As the BBC reports, Russia's lower house of parliament passed a law requiring internet companies to store Russian citizens' personal data inside the country. "The Kremlin says the move is for data protection but critics fear it is aimed at muzzling social networks like Twitter and Facebook. The Russian government is thought to be seeking greater access to user data."

-In the latest reminder of what the "Internet of Things" has in store for us security-wise, researchers have discovered that a cryptography weakness in certain "smart LED" lightbulbs can expose the passwords of wireless networks to which they are connected. As Ars Technica writes, the attack works against LIFX smart lightbulbs, which can be turned on and off and adjusted using iOS- and Android-based devices. "Ars Senior Reviews Editor Lee Hutchinson gave a good overview here of the Philips Hue lights, which are programmable, controllable LED-powered bulbs that compete with LIFX. The bulbs are part of a growing trend in which manufacturers add computing and networking capabilities to appliances so people can manipulate them remotely using smartphones, computers, and other network-connected devices. A 2012 Kickstarter campaign raised more than $1.3 million for LIFX, more than 13 times the original goal of $100,000."

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.