Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

The Weekly Newsletter of The George Washington University Cyber Security Policy and Research Institute

Quick Links

About CSPRI

Contact Us

Newsletter Archive

Blog: The CSPRI Byte

Learn more about CSPRI

Read more about CSPRI's education, research, and service projects with our new, interactive project wheel.

Click here.

May 18, 2015

Fifteen (15) Cyber security events are scheduled in the Greater Washington Area in the next few weeks.

CyberCorps Grads Enter Workforce

Five CyberCorps graduates were given certificates of completion on Friday, May 15 in the SEH Lehman Auditorium as their programs of study came to an end this academic year. Four will be returning after their summer internships, to be joined by at least four new scholarship recipients entering the program in September. Some of the graduating and returning students have already started their jobs or internships at the Naval Research Laboratory, the Inspector General's Office at the U. S. Postal Service, MITRE Corporation, the Department of Justice, the Federal Reserve, and two agencies within the intelligence community.

Events

See Upcoming Events at a Glance

Click here for detailed descriptions

Follow Us

Follow us on Twitter: @gwCSPRI

Follow CSPRI Director, Lance Hoffman: @lancehoffman1

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

Legislative Lowdown

- The House of Representatives last week overwhelmingly approved legislation to end the federal government's bulk collection of phone records, The New York Times reports. The move puts strong pressure on Senator Mitch McConnell of Kentucky, the Senate majority leader, who insists that dragnet sweeps continue in defiance of many of those in his Republican Party. "Under the bipartisan bill, which passed 338 to 88, the Patriot Act would be changed to prohibit bulk collection by the National Security Agency of metadata charting telephone calls made by Americans," the Times notes. "However, while the House version of the bill would take the government out of the collection business, it would not deny it access to the information. It would be in the hands of the private sector - almost certainly telecommunications companies like AT&T, Verizon and Sprint, which already keep the records for billing purposes and hold on to them from 18 months to five years." According to The Hill, the White House 'strongly supports' measures to reform the NSA's practices.

Feeling the pressure, Sen. McConnell introduced a bill that would offer a simple, short extension to Patriot Act as it currently stands. The National Journal notes that McConnell introduced fast-track legislation that would extend without changes the expiring surveillance authorities of the Patriot Act until July 31 of this year. "McConnell also invoked the so-called fast-track procedure on a reform measure that passed the House this week," Dustin Volz writes. "Both bills will be eligible for consideration on the Senate floor when the chamber returns" this week.

-Florida has a new law prohibiting the use of drones to intentionally record images of people on private property if a reasonable expectation of privacy exists, according to a briefby the Electronic Privacy Information Center (EPIC). "The law applies to law enforcement and private individuals, and provides for civil damages and injunctive relief," EPIC notes. "The law follows Florida's 2013 law requiring that police obtain a warrant to use drones to collect evidence. Many states are considering similar legislation and EPIC's State Policy Projectis monitoring bills nationwide."

Cyber Security Policy News

Felton appointed as deputy chief technology offier

-The Obama Administration has appointed Ed Felton, one of the country's toughest critics against the National Security Agency as its deputy chief technology officer. Felton, a Princeton University computer science professor, has been an outspoken critic of the NSA's domestic surveillance activities.

"After ex-NSA contractor Edward Snowden disclosed Verizon was providing call records on U.S. citizens to the intelligence agency, Felten filed a declaration in support of an American Civil Liberties Union lawsuit against 'mass call-tracking,' writes Aliya Sternstein for NextGov. "Felten's research interests include demonstrating how personal behavior can be inferred from large data sets and how to block NSA from seeing thetracking data companies collect on consumers online."

Russia & China sign no-hacking pact
-Russia and China have signed a pact in an agreement not to hack each others' networks, according to The Wall Street Journal. "According to the text of the agreement posted on the Russian government's website on Wednesday, Russia and China agree to not conduct cyber-attacks against each other, as well as jointly counteract technology that may 'destabilize the internal political and socio-economic atmosphere,' 'disturb public order' or 'interfere with the internal affairs of the state,'" the Journal wrote. "The two countries agreed to exchange information between law enforcement agencies, exchange technologies and ensure security of information infrastructure, the document says."

Former federal employee charged in spear phishing attack
-A former U.S. Department of Energy (DOE) and U.S. Nuclear Regulatory Commission (NRC) employee was charged last week with an attempted spear phishing attack aimed at sabotaging sensitive systems. According to SC Magazine, "Charles Harvey Eccleston, 62, allegedly sent dozens of spear phishing emails in January 2015 to DOE employees' emails, the Department of Justice (DOJ) wrote in a press release. He faces four felony offenses, including three counts of crimes involving unauthorized access of computers and a wire fraud charge. Eccelston allegedly wanted to cause damage to the department's network and infect it with a virus that would extract nuclear weapons information for a foreign country." Read more at the FBI's press release.

Ars Technica reports about a setback for prosecutors pursuing people for cross-border theft of trade secrets. "The US government's prosecution of a South Korean businessman accused of illegally selling technology used in aircraft and missiles to Iran was dealt a devastating blow by a federal judge," Ars wrote. "The judge ruled Friday that the authorities illegally seized the businessman's computer at Los Angeles International Airport as he was to board a flight home." Read more here.

Security researcher hacks aircraft's WiFi - and tweets about it
In other law cyber enforcement news, the FBI has stated that a security researcher who was pulled off

of a plane last month after tweeting that he had hacked the plane's wireless network had in fact gotten access to control systems on board the aircraft and managed to affect the trajectory of the aircraft. CNet News reports about a story that first appeared in a Canadian publication, in which an FBI agent Mark Hurley describes an interview with researcher Chris Roberts on April 15 at Syracuse airport, after he'd been detained. "Hurley claims that Roberts 'exploited/gained access to, or 'hacked' the [in-flight entertainment] system," CNet writes. "He stated that he then overwrote code on the airplane's Thrust Management Computer while aboard a flight. He stated that he successfully commanded the system he had accessed to issue the climb command. He stated that he thereby caused one of the airplane engines to climb resulting in a lateral or sideways movement of the plane during one of these flights. He also stated that he used Vortex software after compromising/exploiting or "hacking" the airplane's networks. He used the software to monitor traffic from the cockpit system." Roberts told reporters that the FBI agent took his comments out of context.

About this Newsletter

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. It is published by the Cyber Security Policy and Research Institute (CSPRI) of the George Washington University. CSPRI is a center for GW and the Washington area that promotes technical research and policy analysis of topics in or related to cybersecurity. More information is available at our website, http://www.cspri.seas.gwu.edu

CSPRI

202 994 5613. cspri@gwu.edu
Tompkins Hall, Suite 106
725 23rd Street NW
Washington DC, DC 20052