Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

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

In This Issue

[Quick Links](#)

[Announcements](#)

[Legislative Lowdown](#)

[Cyber Security Policy News](#)

[Events](#)

Quick Links

About CSPRI

Contact Us

Newsletter Archive

Blog: The CSPRI Byte

November 17, 2014

Ten (10) Cyber security Events are scheduled in the Greater Washington Area in the next few weeks.

Event Announcement

Cybersecurity scholarships information session in person and online Thursday e vening

Are you or is someone you know a U. S. citizen interested in becoming a full-time student at GW, studying cybersecurity, and working for a government agency after graduation? The CyberCorps program offers scholarships with full tuition and a living stipend. Possible majors include cybersecurity in computer science, other engineering majors, public policy, business, and more. Law students with a computer science bachelor's degree would also qualify if they will graduate in May 2016 and have enough free slots in their third year schedule for the right cybersecurity and privacy courses.

Events

Click here for descriptions of the upcoming events!

Click the Calendar to See Upcoming Events at a Glance!

Follow Us

Follow us on Twitter: @gwCSPRI

Follow CSPRI Director, Lance Hoffman: @lancehoffman1

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

Follow CSPRI Research Scientist, Allan Friedman: @allanfriedman

An information session is available by webcast and in-person on campus this Thursday, November 20, starting at5:30 pm. Details at http://www.cspri.seas.gwu.edu/scholarships.

Legislative Lowdown

-Last week, Senate Majority Leader Harry Reid moved to advance a bill that would usher in comprehensive reforms to the government's most controversial domestic-spying program, more than a year after Edward Snowden's leaks exposed it publicly, the National Journal writes. "The bill, the USA Freedom Act, would effectively end the government's bulk collection of metadata-the numbers and time stamps of phone calls but not their actual content. Phone companies such as Verizon would instead retain those records, which intelligence agencies could obtain only after being granted approval from the Foreign Intelligence Surveillance Court. The bill would also usher in a host of additional privacy and transparency measures, including a more precise definition of what can be considered a surveillance target."

Cyber Security Policy News

Cybersecurity ranked at the No. 1 threat to the US

-The Associated Press carried last week perhaps the most damning condemnation of the U.S. government's efforts thus far to secure its networks from attack. The AP story, through multiple Freedom of Information Act requests, depicts a pattern of missteps and miscues by cybersecurity personnel at all levels of the government over the past several years. "At a time when intelligence officials say cybersecurity now trumps terrorism as the No. 1 threat to the U.S., an AP review of the $10 billion-a-year federal effort to protect sensitive data shows that the government struggles to close holes without the knowledge, staff or systems to keep pace with increasing attacks by an ever-evolving and determined foe," writes Martha Mendoza for the AP. "While breaches at businesses such as Home Depot and Target focus attention on data security, the federal government isn't required to publicize its own data losses, with news of breaches emerging sporadically."

The Justice Department: Backtracking on Federal Appeals Court

-The Justice Department acknowledged it misled a federal Appeals Court during oral arguments last month in a case reviewing whether the government should be able to secretly conduct electronic surveillance of Americans without a warrant, the National Journal reports. "In a newly

unsealed letter, a Justice Department lawyer told the U.S. Court of Appeals for the 9th Circuit that it spoke erroneously when describing the disclosure restrictions placed upon the FBI's use of so-called national security letters," writes Dustin Volz. "NSLs, as they are often referred, can compel companies to hand over communications data or financial records of certain users to authorities conducting a national security investigation."

AT&T moves away from "permacookie"
-AT&T has decided to back away from a controversial tracking program that keeps tabs on its users' mobile device app and Internet activity. "The method - which the digital advocate Electronic Frontier Foundation dubbed the "permacookie" - is meant to cover the shortcomings of the traditional tracking cookie, which can be easily erased or blocked," The Hill's Cory Bennett writes. "Verizon conceded the tracking number could not be deleted, but explained it didn't use the information to create individual customer profiles."

-In the realm of spooky government activity comes a report from The Wall Street Journal, which indicates that the U.S. government is scooping up data from thousands of mobile phones through devices deployed on airplanes that mimic cellphone towers, a high-tech hunt for criminal suspects that is snagging a large number of innocent Americans. "The U.S. Marshals Service program, which became fully functional around 2007, operates Cessna aircraft from at least five metropolitan-area airports, with a flying range covering most of the U.S. population, according to people familiar with the program," the Journal reports.

Government data becoming harder to protect
-A $10 billion-a-year effort to protect sensitive government data -- from military secrets to social security numbers --is struggling to keep pace with an increasing number of cyberattacks and is unwittingly being undermined by federal employees and contractors," according to The Guardian. "Workers scattered across more than a dozen agencies, from the defense and education departments to the National Weather Service, are responsible for at least half of the federal cyberincidents reported each year since 2010, according to an Associated Press analysis of records."

Cyber attack allows emails to go without encryption
-Privacy advocates are making their case against a US-based ISP suspected of performing encryption downgrade attacks that caused customers' e-mail to remain in plaintext as it passed over the Internet, reports Ars Techica.

"The attacks, according to researchers, were carried out by AT&T subsidiary Cricket and prevented e-mail from being protected by STARTTLS, a technology that uses the secure sockets layer or transport layer security protocols to encrypt plaintext communications," Dan Goodin reports. "The attacks worked by removing the STARTTLS flag that causes e-mail to be encrypted as it passes from the sending server to the receiving server. After the tampering came to light late last month it was reported by *The Washington Post* andTechDirt."

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
304 Staughton Hall
707 22nd St., NW
Washington DC, DC 20052