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](#)

Scholarship applications dueJanuary 31, 2015

Cybersecurity is increasingly seen as an interdisciplinary field.

The CyberCorps Scholarship includes**full tuition and fees coverage, a living stipend for**

January 12, 2015

Nine (9) Cyber security Events are scheduled in the Greater Washington Area in the next few weeks.

CSPRI has moved!

The CSPRI office has moved.
We are now located in Tompkins Hall:

725 23rd Street NW
Suite 106
Washington, DC 20052

Legislative Lowdown

-President Obama on Monday called for federal legislation intended to force American companies to be more forthcoming when credit card data and other consumer information is lost in an online breach like the kind that hit Sony, Target and Home Depot last year, the New York Times reports. "The Personal Data Notification and Protection Act would demand a single, national standard requiring companies to inform their customers within 30 days of discovering their data has been hacked,"[wrote](#) Michael D. Shear and Natasha Singer. In a speech today at the Federal Trade Commission, Mr. Obama said that the current patchwork of state laws does not protect Americans and is a burden for companies that do business across the country.

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

the academic year, a book allowance, and a professional development fund.

For more information on the program, click **here.**

-Sen. Ron Wyden (D-Ore.) is reintroducing legislation that bars the government from requiring technology companies to build so-called "backdoor" security vulnerabilities into their devices to allow access to their data, according to The Hill. "Wyden first introduced the bill last December after FBI director James Comey criticized moves by some phone companies to encrypt devices to prevent anyone from accessing their data without permission, even law enforcement," writes Mario Trujillo. "A law already governs law enforcement's ability to tap landline phones, but it does not extend to data from mobile devices. The FBI has pressed for an update as mobile companies like Apple and Google build stronger encryption on their devices."

The Hill covers another measure introduced by Rep. Dutch Ruppersberger (D-Md.) last week that would make it easier for private companies to share information about possible hackers and lines of attack with each other and the government. "Backers say it's a critical step to ensure there are no blind spots on the country's networks," reports Julian Hattem. "Privacy advocates, however, fear it would allow companies to send personal and identifying information about everyday users to the government, including agencies such as the NSA. Ruppersberger's bill has come up twice before in Congress, but failed to reach the finish line. President Obama has pledged to veto previous versions, on the grounds that it does not do enough to protect privacy."

Cyber Security Policy News

Smart gadgets: a threat to privacy?
-The head of the U.S. Federal Trade Commission said last week that the "internet of things" - the global mesh of Internet-connected devices from smart watches to net-aware appliances - presents "significant" privacy challenges for consumers. Edith Ramirez said a future full of smart gadgets that watch what we do posed a threat to privacy," writes the BBC, covering Ramirez's appearance and speech at last week's Consumer Electronics Show. "The collated data could create a false impression if given to employers, universities or companies, she said. Ms Ramirez urged tech firms to make sure gadgets gathered the minimum data needed to fulfill their function."

The Internet of Things
The Internet of Things also extends to devices that are fairly "dumb" in that they're extremely challenging to update with security fixes and frequently left unsecured. That fact is highlighted in a discovery posted last week by security journalist Brian Krebs, who learned that the

attacks which knocked tens of millions of people off Sony and Microsoft's online gaming networks on Christmas Day were powered by a botnet built on top of hacked consumer-grade Internet routers. "In addition to turning the infected host into attack zombies, the malicious code uses the infected system to scan the Internet for additional devices that also allow access via factory default credentials, such as 'admin/admin,' or 'root/12345'", Krebs writes of the malware used to build the attack machine. "In this way, each infected host is constantly trying to spread the infection to new home routers and other devices accepting incoming connections (via telnet) with default credentials," The botnet is not made entirely of home routers; some of the infected hosts appear to be commercial routers at universities and companies, and there are undoubtedly other devices involved. The preponderance of routers represented in the botnet probably has to do with the way that the botnet spreads and scans for new potential hosts."

Stingrays Update

-The Federal Bureau of Investigation is taking the position that court warrants are not required when deploying cell-site simulators in public places. Nicknamed "stingrays," the devices are decoy cell towers that capture locations and identities of mobile phone users and can intercept calls and texts, according to Ars Technica. "The FBI made its position known during private briefings with staff members of Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.) and Sen. Chuck Grassley (R-Iowa)," writes David Kravets. "In response, the two lawmakers wrote Attorney General Eric Holder and Homeland Security chief Jeh Johnson, maintaining they were 'concerned about whether the FBI and other law enforcement agencies have adequately considered the privacy interests' of Americans."

That position comes amid disclosures that the FBI is giving the National Security Agency a run for its money in terms of the law enforcement agency's desire for more powerful surveillance capabilities, The New York Times reports. "In 2008, according to the report, the F.B.I. assumed the power to review email accounts the N.S.A. wanted to collect through the 'Prism' system, which collects emails of foreigners from providers like Yahoo and Google," writesCharlie Savage. "The bureau's top lawyer, Valerie E. Caproni, who is now a Federal District Court judge, developed procedures to make sure no such accounts belonged to Americans. Then, in October 2009, the F.B.I. started retaining copies of unprocessed communications gathered without a warrant to analyze for its own purposes. And in April 2012, the bureau began nominating new email accounts and phone numbers belonging to foreigners for collection, including through the N.S.A.'s 'upstream' system, which collects communications transiting network switches." Read more here.

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