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

Follow Us

Follow us on Twitter:
@gwCSPRI

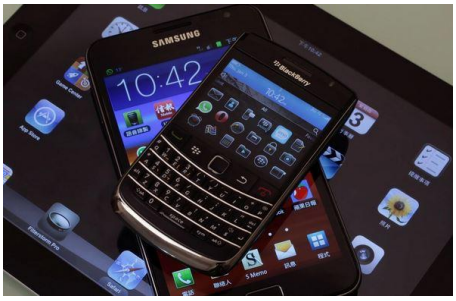
Follow CSPRI Director, Lance Hoffman:
@lancehoffman1

Follow CSPRI Associate Director, Costis Toregas:
@DrCostisToregas

August 3, 2015

Four (4) events scheduled in the Greater Washington Area in the next few weeks.

A different opinion on encryption



Over the past several weeks, we have kept our readers up-to-date on the debate surrounding data encryption. While the discussion is largely focused on national security, less attention is shed on the role of private industry.

This Washington Post op-ed suggests, "that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring."

Events

August 5
Cybersecurity, Governance, and Network 2015 Conference

August 7
2600 Arlington Meetup

August 11
NSA R&E Psyber Symposium

August 12-14
USENIX Security 2015

Click here for detailed descriptions

Of note, in addition to the argument itself, is who the authors are. Mike McConnell is a former director of the National Security Agency and director of national intelligence. Michael Chertoff is a former homeland security secretary and is executive chairman of the Chertoff Group, a security and risk management advisory firm with clients in the technology sector. William Lynn is a former deputy defense secretary and is chief executive of Finmeccanica North America and DRS Technologies. Their argument appears to clash with **that** of FBI Director James Comey.

Click **here** for the article.

Legislative Lowdown

-Legislation aimed to toughen cybersecurity at federal government civilian agencies by requiring the implementation of state-of-the-art tools has passed the Senate Homeland Security and Governmental Affairs Committee, GovInfoSecurityreports. "The bill, known as the Federal Cybersecurity Enhancement Act of 2015, would accelerate the deployment and adoption of the Department of Homeland Security's federal intrusion detection and prevention program known as Einstein and would require civilian agencies to participate in it. The panel approved the measure unanimously on July 29, just two days after it was introduced."

-Politico reports that it's anybody's guess whether the Cybersecurity Information Sharing Act of 2015 will make it to the Senate floor before the August recess. "The on-again, off-again bill has seesawed from indefinitely postponed to imminent proposition over the past few days," Politico reports on its Morning Cybersecurity roundup. "On Thursdayafternoon, Senate Majority Leader Mitch McConnell said the Senate's first priority Monday will be a measure to defund Planned Parenthood. The Planned Parenthood procedural measure requires 60 votes to advance and Democrats are vowing to block it - this seems to suggest CISA will be the main show after all." This summary of the bill at the Electronic Frontier Foundation does a good job of explaining why the legislation remains so controversial for security and privacy advocates.

Cyber Security Policy News

Heartbleed for Mobile

-A major security flaw in Android lets an attacker take control of a phone simply by sending a text message - and for the vast majority of Google Android users, there's no fix available yet. As The Guardian reports, even the small number of people using Google's own line of Android phones, sold under the Nexus brand,

are vulnerable to some of the effects of the bug,according to Joshua Drake, the researcher who discovered the flaw.

US Department of Commerce to revise regulations on hacking software

-The U.S. Commerce Department is proposing revised changes to regulations intended to restrict the export of software that can used to break into computers and smart phones. The move comes after a number of prominent security experts said the earlier proposed rules would stifle security research and were so broad that they could easily bar the easy sale of standard tools used to test electronic security. As Joseph Menn writes for Reuters, "the step had been expected after the avalanche of objections from major technology companies as well as security specialists. Even some activists who applauded the idea of cracking down on the sale of tools to despotic regimes that spy on dissidents said the draft had been clumsy."

Chinese cyber attacks on US

-NBC News last week published a secret map produced by the National Security Agency (NSA) which the publication saiddepicts the Chinese government's massive cyber assault on all sectors of the U.S economy, including major firms like Google and Lockheed Martin, as well as the U.S. government and military.

Google and the Right to be Forgotten

-Google has indicated that it does not intend to comply with a judgment of the high court in Europe after earlier losing its appeal in a fight over the Right to be Forgotten law in Europe. As the Electronic Privacy Information Center (EPIC) reports, earlier this year, the French Data Protection agency, consistent with the landmark decision of the European Court of Justice,instructed Google to delist certain links in all domains in which the search company operates. "A recently leaked version of a Google transparency report found that the vast majority of requests for delisting concern private matters of private individuals," EPIC notes. "Support for the "right to be forgotten"continues to grow around the world with courts in Japan, Canada, and the United States acknowledging similar claims."

New rules coming for government contractors?

-The White House wants to establish strict, consistent rules for how government contractors should lock down sensitive data. According to The Hill, The White House thinks part of the problem is inconsistency in the data-security standards of federal contracts. Multiple agencies have issued varying guidelines that have further complicated things. 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
Tompkins Hall, Suite 106
725 23rd Street NW
Washington DC, DC 20052