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]

March 9, 2015

Eight (8) Cyber security events are scheduled in the Greater Washington Area in the next few weeks.

Event thisThursday

CSPRI Director Dr. Lance Hoffman will speak on a panel at the ITIF event *Crypto Wars 2.0: Has the United States Abandoned the Policy of Secure by Design?*

The event is free, but registration is required. Click **here** for more information.

Legislative Lowdown

-A bill in the Senate to beef up cybersecurity and information sharing about new threats has stalled after pushback from the White House. As the Wall Street Journal reports, The White House and some congressional Democrats have raised privacy concerns about a cybersecurity bill drafted by top Senate Intelligence Committee lawmakers, stalling - at least temporarily - one of Congress's top priorities. "The general counsels of more than 30 different firms, including 3M Co. and Lockheed Martin Corp., sent a joint letter to lawmakers March 1 prodding officials to back legislation that promoted more information sharing, in part because of legal protections extended to companies in the bill," writes Damian Paletta. "But privacy advocates and at least one technology

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

firm immediately mobilized to try to quash the legislation, arguing that the way the 48-page draft was worded could make it easier for the government to use corporate data to spy or conduct surveillance on U.S. citizens."

Cyber Security Policy News

Security hole: FREAK
-Security experts are again warning of another serious security hole in the SSL/TLS technology used by most Web sites and browsers to encrypt communications. "This one goes by the clever acronym FREAK which stands for Factoring Attack on RSA-EXPORT Keys," writes Steve Weisman for USA Today. "This bug affects SSL/TLS protocols used to encrypt data as it is transmitted over the Internet and potentially puts at risk private information sent over the Internet including passwords, banking and credit card information. To better understand FREAK, it is necessary to go back to restrictions of a maximum of 512-bit code encryption from the early 1990s used in software to be sold abroad." Google, Apple and Microsoft are readying or pushing fixes. Read more here.

Clinton: In trouble over private email server
-Some Republican lawmakers are calling for inquiries over whether former Secretary of State Hillary Clinton's use of private email violated security rules. "A State Department review of Hillary Rodham Clinton's e-mails from her time leading the agency could reveal whether she violated security policies with her use of a private e-mail server," The Washington Post reports. "The official, requesting anonymity to discuss sensitive internal deliberations, said that Clinton's use of personal e-mail did not automatically break the rules, but the analysis could show whether work e-mails sent from her personal account included sensitive information that is typically required to be handled on a system that meets security protocols."

Apple Pay fraud
-Security experts are warning that fraudsters have latched onto Apple Pay, a relatively new form of payment that was initially touted as a more secure alternative to paying with a basic magnetic-stripe-powered credit card. "The fraud issue was brought to light by Cherian Abraham, a payment expert who works with banks and retailers on mobile-payment strategies, in a blog post in late February," The Wall Street Journal reports. "He said fraud 'is growing like a weed, and the bank is unable to tell friend from foe.' Abraham said it's not 'an anomaly' to see fraud accounting for about 6% of Apple Pay transactions, compared to about 0.1% of transactions using a plastic card to swipe.

He noted that fraud rates vary by issuing bank."

Wary of Beijing's new source code rule
-President Obama warned the Chinese government that its recently-announced new rules requiring tech firms to hand over the source code to their products as a condition of selling their products to businesses in China is a non-starter. In an interview with Reuters, Obama said he was concerned about Beijing's plans for a far-reaching counterterrorism law that would require technology firms to hand over encryption keys, the passcodes that help protect data, and install security "backdoors" in their systems to give Chinese authorities surveillance access. "This is something that I've raised directly with President Xi," Obama said. "We have made it very clear to them that this is something they are going to have to change if they are to do business with the United States." Meanwhile, a spokesperson for the Chinese foreign ministry addressed the president's concerns in a Q&A published on March 5.

Financial incentives are low for big companies to up their cybersecurity measures
-With all of the high-profile security breaches of the last year, one would think that it might become easier to make the business case for cybersecurity at the nation's top companies. But according to a provocative essay in Quartz, the math suggests otherwise. "When we examine the evidence, though, the actual expenses from the recent and high-profile breaches at Sony, Target and Home Depot amount to less than 1% of each company's annual revenues. After reimbursement from insurance and minus tax deductions, the losses are even less," writes Benjamin Dean for Quartz. "This indicates that the financial incentives for companies to invest in greater information security are low and suggests that government intervention might be needed."

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