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

July 27, 2015

Six (6) events scheduled in the Greater Washington Area in the next few weeks.

Michael Chertoff disagrees with the "going dark" stance on encryption

Speaking at the Aspen Security Forum this week, Third Circuit Judge and ex-Secretary of Homeland Security Michael Chertoff surprised many by disagreeing with FBI Comey's "going dark" stance on encryption. The one-hour video can be found **here**. Chertoff quotes from around 15:50:

"We do not historically organize our society to make it maximally easy for law enforcement even with court orders to get information"; "we're not quite as dark sometimes as we fear we are"; "requiring people to build a vulnerability may be a strategic mistake".

Legislative Lowdown

-A Senate committee last week approved a measure that would give current and former federal employees and contractors affected by the hack at the Office of Personnel Management ID theft protection for three

Events

July 28
Cybersecurity Best Practices

July 29
Internet of Things

Cyber RiskWednesday

July 30
Cyber Montgomery

World Wide Cyber Threats

CharmSec Meetup

Click here for detailed descriptions

times longer than the OPM originally offered. "The amendment would provide hack victims with 10 years of credit monitoring services and it would offer $5 million in liability protection to hack victims," writes Eric Katz at Government Executive. "OPM offered the 21.5 million federal employees, contractors, applicants and family members affected by the breach involving security clearance files three years of a 'suite of services,' including full service identity restoration support and victim recovery assistance, identity theft insurance, identity monitoring for minor children, continuing credit monitoring and fraud monitoring services beyond credit files."

-Senate Homeland Security lawmakers are prepping a bill that would cement into law use of a DHS intrusion-blocker called EINSTEIN, according to NextGov. As Aliya Sternstein reports, DHS has had trouble convincing agencies it was legal to let the department scan their Internet traffic for threats. "The new legislation would require that EINSTEIN incorporate cutting-edge commercial security technologies, provide full coverage across civilian agencies and bake in privacy protections," Sternstein writes. Read more here.

Cyber Security Policy News

Jeep Cherokee - Hackable
-In a gripping story that reads like science fiction, Wired.com carries a piece examining methods that researchers worked out to remotely hack into a late-model Jeep Cherokee through the car's entertainment system, and control everything from the brakes to the ignition itself. The story tracks a reporter's firsthand experience in a vehicle on the highway as the researchers toyed with the car and showed how they could -- remotely, over the Internet -- seize control over virtually all of its features.

Cybersecurity standards for vehicles
The research, to be detailed in a popular hacker convention held next month in Las Vegas, has prompted calls from lawmakers for stricter car security standards. Wired reports that U.S. Senators plan to offer a bill that would require cars sold in the United States to meet specific cybersecurity standards, and calls on the National Highway Safety Administration and the Federal Trade Commission to promulgate those standards.

The Wired story comes amid reports that Fiat Chrysler has issued a recall affecting 1.4 million cars to patch a security flaw in the software used by some cars' radio systems. The car maker said the recall was directly related to the findings of the researchers. CNBC has more here.

NSA update
-The nation's top spy agency is taking steps to revive

a program to track Americans' phone records, according to The Hill. "After President Obama signed legislation last week to end the controversial program, the Justice Department submitted a legal memorandum to the secretive federal court justifying authorization for the NSA collection for another six months, as the new law allows," writes Julian Hattem. "The legal analysis was submitted on Tuesday, less than an hour after the White House announced that the president had signed the USA Freedom Act into law. The memo was not revealed to the public until Monday. Until the passage of the USA Freedom Act last week, the Foreign Intelligence Surveillance Court (FISC) routinely granted the NSA the ability to collect "metadata" about millions of Americans' phone calls, including the numbers people dial and the length of their calls, but not their actual conversations."

AshleyMadison.com hack update

-Last week featured news of several high-profile cyberattacks affecting tens of millions of people. KrebsOnSecurity broke the news that hackers had broken into the networks and internal data of AshleyMadison.com, an online dating service that caters to married people looking to set up extramarital affairs. The attacker in that case released the account information of several thousand of AshleyMadison's 37 million users, and threatened to leak the entire user database unless the company voluntarily agreed to shut down. AshleyMadison's chief executive told reporter Brian Krebs that the company believes it has identified an suspect who formerly had access to the organizations network. As of this date, the hacker or hackers had not yet followed through on their threat to release the entire database.

JP Morgan Chase: plot to change stock prices

Also last week, the Justice Department announced arrests in connection with the high-profile intrusion at JP Morgan Chase last year that jeopardized the personal data on more than 70 million people. According to investigators, the attack was part of a complex plot to manipulate the stock prices of specific companies in a scam known as a "pump-and-dump" scheme. Read the complete report on the investigation at Bloomberg.

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