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

CSPRI in the News

July 8: CSPRI Associate Director Costis Toregas speaks to CTV about the NYSE and United Airlines technical system failures. Click **here** for the clip.

July 9: CSPRI Senior Research Associate Trey Herr blogs for The Hill about preparing for data breaches. Click**here** for the piece.

Follow Us

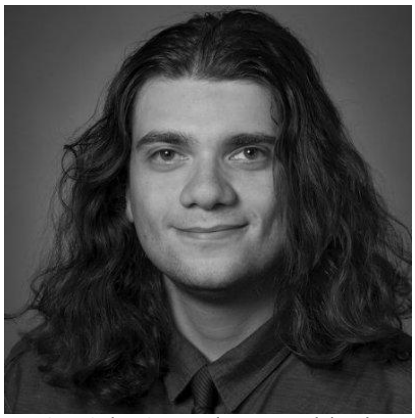
Follow us on Twitter:
@gwCSPRI

Follow CSPRI Director, Lance Hoffman:
@lancehoffman1

July 13, 2015

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

GW CyberCorps alumnus among experts in encryption debate



GW CyberCorps alumnus, Michael Specter.

Michael Specter is a 2010 graduate of GW's CyberCorps program, holding degrees in Computer Science and International Affairs. Following graduation, he accepted a position at position with MIT's Lincoln Lab, a Federally

Events

July 14
Hearing: Department of Homeland Security

July 15
Cybersecurity: Department of the Interior

NovaInfoSec Meetup West

July 16
Internet Governance Forum USA 2015 (IGF-USA)

National Insider Threat Special Interest Group

National Cybersecurity Center of Excellence Speaker Series

ISSA NoVA Meetup

July 21
ISSA DC Meetup

Click here for detailed descriptions

Follow CSPRI Associate Director, Costis Toregas: @DrCostisToregas

Funded Research and Development Center (FFRDC) where he specialized in reverse engineering. He returned to GW in 2013, as a speaker to the (then) current CyberCorps students to give a talk on his work. How important is this work? **See below** to read about the report,Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications. Or, click **here** to read the full report.

Legislative Lowdown

-Lawmakers are debating whether to strip the Office of Personnel Management (OPM) of its control over security clearances after hackers made off with nearly 20 million background check forms housed at the agency, according to The Hill. "Reps. Ted Lieu (D-Calif.) and Steve Russell (R-Okla.), who both likely had their security clearance details taken in the breach, are prepping a bill that would move the security clearance database away from the OPM, perhaps back to the Defense Department (DOD), where it was housed until 2004," reports Cory Bennett.

Cyber Security Policy News

OPM breach update

-The massive breach at the Office of Personnel Management just got more massive. At one of several congressional hearings on the breach last week, OPM leaders acknowledged that the breach jeopardized the personal information - including Social Security numbers and some fingerprints -- on more than 22 million people. This was a significantly higher number than the agency had disclosed previously. "The agency said hackers stole 'sensitive information,' including addresses, health and financial history, and other private details, from 19.7 million people who had been subjected to a government background check, as well as 1.8 million others, including their spouses and friends," writes Julie Hirschfeld Davis for The New York Times. "The theft was separate from, but related to, a breach revealed last month that compromised the personnel data of 4.2 million federal employees."

OPM Director Katherine Archuleta resigns

The disclosure was the final straw for OPM Director Katherine Archuleta, who announced she was resigning shortly after news of the expanded breach hit the press. The Obama administration praised Archuleta for work that uncovered the breach. "White House Press Secretary Josh Earnest credited Archuleta for beginning a process of upgrading cybersecurity at OPM," GovInfoSecurity reports. "It's precisely because of some of the reforms that she initiated, that this particular cyber-breach was

detected in the first place,' Earnest said. 'But given the urgent and significant challenges that are facing OPM right now, a new manager with a specialized set of skills and experiences is needed.'"

Meanwhile, OPM still hasn't decided how it is going to provide identity theft protection services to the 22 million-plus people affected by the breach. The agency selected a company called CSID to offer 18 months of credit monitoring services for the 4.2 million individuals originally thought to have been the totality of those impacted in the break-in. That contract cost more than $20 million, according to National Journal. "The overlap between the individuals affected by the two data breaches is very large: 3.6 million of the 4.2 million people affected by the smaller hack were also affected by the larger one," writes Kaveh Waddell. "Given that CSID charged upwards of $20 million to provide notifications and 18 months of services to 4.2 million people, the price tag for notifying 21.5 million people and serving them for at least three years could potentially be much, much higher."

TerraCom and YourTel America

Poor grades for its own security haven't stopped the federal government from fining private sector companies for theirs. Two sister mobile and telecom service providers will pay a combined $3.5 million after the U.S. Federal Communications Commission found that they were storing customers' personal data on unprotected servers accessible over the Internet," according to Grant Gross of Computerworld. "TerraCom and YourTel America failed to adequately protect the personal information of more than 300,000 customers," Gross reports. "The settlement stems from a 2013 incident when an investigative reporter found customer records from the companies' low-income Lifeline programs online, the agency said in an October 2014 proposal to fine the companies."

Experts respond to the threat of "Going Dark"

Last week's hearing on the threat of "Going Dark" -- or a future in which thieves, cyberspies and terrorists are all using uncrackable encryption that thwarts law enforcement ability to track them - generated a healthy debate on the merits of purposefully building backdoors into technology for investigators. FBI Director James Comey went to Capitol Hill last week to argue for a requirement that technology makers like Apple and Google weaken the encryption on their devices to allow investigators to access customer devices when authorized by a court. In response, more than a dozen experts in computer security published a report called "Keys Under Doormats: Mandating Insecurity By Requiring Government Access to All Data and Communications," which seeks to explain how doing so would weaken security for everyone.

Not that the government really needs this kind of

access: As noted computer security pioneer Peter C. Neumann quipped to The New York Times, "there are more vulnerabilities than ever" that could be exploited through access to encrypted communications.

Nevertheless, the powers-that-be will likely search for a middle ground, according to technology Ray Ozzie. "Ozzie shepherded the development of Lotus Notes collaboration and email software and had to navigate a tricky course between offering the most secure software possible - with 64-bit encryption - and laws that forbid the export of that technology outside the U.S. because it was *too* secure," writes Barb Darrow for Gigaom. "A compromise was struck that allowed Lotus to offer a version of Notes that was more secure than other commercial offerings but met government export restrictions."

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