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

November 16, 2015

Ten (10) events scheduled in the Greater Washington Area in the next few weeks.

CyberCorps Information Session

The application portal is now open for the GW CyberCorps Scholarship Program (2016-2017)!

Come join us on **Monday, November 23rd from 5:30 - 7:00 PM** to get an overview of the scholarship, its benefits, and its requirements. Complete application packages are due by **January 31, 2016.**

Events

November 17
Technical Tuesday: Hackproof Signal Processing for Wireless Communications

November 18
ISACA NCA Meetup: Conference on treads in mobile computing

November 18
The Internet of Cars

November 18
ISSA Baltimore Meetup: Advanced endpoint protection

November 18
Cybercon 2015

November 18
NovaInfosec Meetup West

November 18
OTA IoT Trust Framework Summit

November 19
Cyberpoint 2nd Annual Women in Cyber Security

Location:
The George Washington University
Science & Engineering Hall
800 22nd Street NW
Room 2000B
Washington, DC 20052

Click **here** for the CyberCorps webpage.

Legislative Lowdown

-A House panel last week approved two cybersecurity bills aimed at helping states and ports fight off hackers, reportsThe Hill. The first bill would direct the federal government to provide state and local officials with the technical know-how and strategies they are lacking in the fight against overseas cyberattacks. The second bill would help maritime ports share data on hacking threats in the hopes of staving off a destructive attack. "Ports have been increasing the amount of automation used to move cargo from ships to trucks and rail, which has raised fears about potential cyberattacks," writes Cory Bennett.

Cyber Security Policy News

Microsoft: international servers
Microsoft will store data for European cloud computing customers on servers run by a German company to reassure them that their data can't be accessed by U.S. authorities, reports The Hill. "It's an admission from the company that tech firms will need to find new ways to satisfy overseas customers' privacy concerns after a European Union court invalidated a key data safety pact," writes David McCabe. "Microsoft saidWednesday that it would offer customers the option of storing their data in two server farms in Germany, likely in 2016."

Cyber insurance on the rise
-More businesses are filing cyber insurance claims related to data breaches of late, according to a new study. "A recentWells Fargo survey of 100 U.S. middle-market and large companies found that 85 percent say they have purchased cyber and data privacy insurance, while 44 percent have already filed a claim as a result of a breach," reports James Eng for NBC News. "The report didn't look into the total cost of the claims but a recent study by NetDiligence pegged the average claim for a large company at $4.8 million."

2016 National Defense Authorization Act
-President Obama is set to sign a defense bill ordering the Pentagon to probe every major weapon system for hacker entryways. Among many passages dedicated to cybersecurity in the 2016 National Defense Authorization Act is a section on evaluating cyber

vulnerabilities in weaponry, according to NextGov. "An inspection last year of almost the entire Pentagon weapons program revealed 'significant vulnerabilities' in cybersecurity throughout in every system," Aliya Sternstein writes. "For the most part, the U.S. military never fathomed its weapons would be considered 'connected devices' one day, right along with refrigerators, cars and other data-driven machines in the Internet of Things."

Cybercrime: financial firm update
-Authorities in New York and Atlanta last week announced arrests and indictments in the case of a sophisticated organized cybercrime gang accused of stealing tens of millions of consumer records from top financial firms, including JPMorgan Chase, E*TRADE and Scottrade. Investigative reporter Brian Krebs writes about other unnamed victim companies buried in the charging documents: One company, identified in the indictments only as 'Victim #12,' is an entity that helps banks block transactions for dodgy goods advertised in spam. Turns out, the hackers targeted this company so that they could more easily push through payments for spam-advertised prescription drugs and fake antivirus schemes. Read more here.

Tor Project: update
The head of the Tor Project has accused the FBI of paying Carnegie Mellon computer security researchers at least $1 million to de-anonymize Tor users and reveal their IP addresses as part of a large criminal investigation, Ars Technica reports. "Neither Carnegie Mellon officials nor the FBI immediately responded to Ars' request for comment," Cyrus Farivar reports. "If true, it would represent a highly unusual collaboration between computer security researchers and federal authorities."