Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

Quick Links

About CSPRI

Contact Us

Newsletter Archive

Blog: The CSPRI Byte

Scholarship portal is open

The GW CyberCorps Program is accepting applications for the upcoming 2016 - 2017 academic year.

The scholarship includes fully funded tuition and fees, a living stipend, book allowance, and a professional development fund.

Completed scholarship packages are due byJanuary 31, 2016.

Click **here** for more information.

December 14, 2015

Five (5) events scheduled in the Greater Washington Area in the next few weeks.

Legislative Lowdown

-A House panel last week passed the Data Security Act of 2015, a bill that would establish minimum security protections at businesses as well as create a national requirement for data breach notifications. The measure would supplant 47 state laws with a single, national breach notification statute. Read more atGovInfoSecurity.

-Congressional negotiators are close to finishing a compromise cybersecurity bill, but there may not be time for a floor vote since lawmakers are expected to vote on an omnibus spending bill and a tax extenders package, according to Morning Consult. "The House passed two similar bills, one coming out of the Homeland Security Committee and one coming from the Intelligence Committee, that lawmakers have spent the past few months conferencing with the Senate measure," the publication notes. "The buzz around the Hill last week was that negotiations were almost done, and reports say House leaders are reviewing a final version of the bill. But the negotiations have seen some hiccups, and there might not be time for a vote on the bill with both an omnibus spending bill and a tax extender deal on the floor schedule."

Events

December 15
ISSA Baltimore Meetup

December 16
Crafting a National Strategy for the Internet of Things

December 16
NovaInfosec Meetup

December 17
CharmSec

December 18
International Norms in Cyberspace

Click here for detailed descriptions

The Hill reports that the Senate Intelligence Committee's top Democrat could soon introduce legislation that would require social media platforms, including Facebook, Twitter and YouTube, to alert federal officials about online terrorist activity. "Sen. Dianne Feinstein (D-Calif.) has been pushing for language that would address the growing use by extremist groups of social media to both spread propaganda and plot attacks around the world," reports Cory Bennett.

Cyber Security Policy News

Bitcoin creator found?
-Wired.com outed an Australian computer expert as the man who is most likely behind the pseudonym "Satoshi Nakamoto," the celebrated but anonymous persona linked to the creation of the virtual currency bitcoin. No sooner had Wired's article ran than dozens of federal agentsraided the house of the man named as the mastermind of bitcoin. Australian authorities claimed the raid was related to tax issues, not bitcoin, however the man is reputed to have one of the world's largest stashes of bitcoins.

Wyndham hotel update
-The Federal Trade Commission (FTC) last week settled a lawsuit with hotel chain Wyndham Worldwide that alleged the company's poor data security exposed customer data to hackers. Wyndham had challenged the FTC's authority, seeking to dismiss the lawsuit against it. But in August, a federal appeals court sided with the FTC, setting off negotiations that led to the settlement. Read more at The Hill.

France considering new bans on wifi to combat Tor
-According to leaked documents France's Ministry of Interior is considering two new proposals: a ban on free and shared Wi-Fi connections during a state of emergency, and measures to block the free anonymity service Tor being used inside France. Ars Technica writes about the revelations, first reported by the French newspaper *Le Monde*. "According to the paper, new bills could be presented to parliament as soon as January 2016," writes Sebastian Anthony. "These proposals are presumably in response to the attacks in Paris last month where 130 people were murdered."

FBI admits to using "zero-days"
-A top tech official with the FBI acknowledged that the agency uses "zero-days," unknown vulnerabilities in software and hardware that can be used in stealthy attacks or law enforcement investigations. The agency also revealed that it uses "Stingrays," devices that mimic cell phone towers in a bid to intercept cell phone communications. Check out this Washington Post story for more details.

OPM violated federal procedures by awarding contract to identify theft protection company
-A new government watchdog report says the Office of Personnel Management violated federal procedures when it awarded a $20 million contract to a company that is providing identity theft protection to millions of current and former federal workers who had their data stolen. The Washington Examiner has the full scoop.