

GW CSPRI Newsletter

November 5, 2012

From the **Cyber Security Policy and Research Institute of The George Washington University**, www.cspri.seas.gwu.edu.

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.

Faculty and student readers of this newsletter with new and important cyber security research to report (especially new papers or results by GW faculty and students) are encouraged to send notifications of this to cspriaa@gwu.edu. A short (up to three sentences) description of why you think the research is important is required.

Contents

[Events](#)

[Announcements](#)

[Legislative Lowdown](#)

[Cyber Security Policy News](#)

Events

-Nov. 5, 12 noon - 1:00 p.m., **Cyber Security & Transformational Technologies: Keeping Systems and Data Safe** - This webcast will explore the results of the research, including how government is managing cyber security priorities and where they are investing limited funds to keep their systems and data safe while serving the needs of their agencies. [More information](#).

-Nov. 7, 6:00 p.m. - 8:00 p.m., **National Laboratories and Their Role in National Security** - Dr. Penrose (Parney) Albright, director of the Lawrence Livermore National Laboratory, will discuss the role of national laboratories in the critical function of national security and technical innovation at the GWU's Virginia Science and Technology Campus (VSTC). Dr. Albright is the inaugural presenter for the Dean's Speakers Series, hosted by Dr. Ali Eskandarian, dean of GW's VSTC. Exploration Hall 20101 Academic Way, Ashburn, VA. [More information](#).

-Nov. 7, 6:30 p.m. - 9:30 p.m., **CapSec DC Meetup** - Cap Sec DC is a subset of the CitySec movement, a group of information security professionals in the Washington DC Metropolitan area who get together about once a month to socialize. 808 7th Street, NW. [More information](#).

-Nov. 7, 7:15 a.m. - 6:30 p.m., **No Boundaries: Global, Connected, Secure** - This all day conference by Symantec will cover cyber security intelligence, tactical security, compliance and consolidation, as well as continuous monitoring, virtualization, and cloud data security. Walter E. Washington Convention Center, 801 Mount Vernon Place, NW. [More information](#).

-Nov. 12, 5:30 p.m. - 8:30 p.m., **NoVa Hackers Association Meetup** - This informal group of security professionals from around the NoVA/DC area coordinates one or two monthly events – an evening meetup with presentations on the second Monday of the month and various lunch or bar meetups. 11091 Sunset Hills Road, Reston, VA. [More information](#).

-Nov. 14, ISACA CM Meetup: Security Issues From Your Wired to Wireless Network - The ISACA – Central Maryland (CM) chapter is based in Baltimore, MD. Chapter meetings are usually held nine times per year. The Conference Center at the Maritime Institute, 692 Maritime Boulevard, Linthicum, MD. [More information](#).

-Nov. 15, 7:30 a.m. - 4:30 p.m., **FedCyber.com Cyber Security Summit** - Talks at this year's conference will focus on three key areas: threat intelligence, adversary characterization, and information sharing; cyber workforce challenges; and emerging technologies that will change the cyber security landscape. Ronald Reagan Building, 1300 Pennsylvania Ave. NW. [More information](#).

Announcements

-On October 31, CSPRI co-hosted a WashingtonPostLive event that featured remarks by DHS Secretary Janet Napolitano on cyber vulnerabilities, Gen. James Cartwright, former Vice Chairman to the Joint Chiefs, joining a group of subject area experts in a cyber attack simulation, and William Lynn III, former Deputy Secretary of the Defense Department, highlighting the need for enhanced public-private cooperation during a cyber attack. Video highlights are available [here](#).

Legislative Lowdown

-Senate Majority Leader Harry Reid hopes to reintroduce cyber security legislation opposed by business groups once lawmakers return after Tuesday's election, a Senate aide said, adding that

a White House executive order might pave the way for a compromise on the bill, the Associated Press [reports](#). Senator Joe Lieberman, one of the authors of the bill, would consider dropping a provision aimed at shoring up protection of critical infrastructure that had raised concerns among Senate Republicans, if that issue could be addressed in an executive order, Jeffrey Ratner, senior adviser for cybersecurity on the Senate Homeland Security Committee, said last week.

-The United States argued that cybersecurity mandates should be excluded from an international telecommunications treaty in a new set of proposals sent to a United Nations agency last week. The Hill [writes](#) that some countries are pushing to include cybersecurity proposals in the treaty that could lead to online censorship or put one regulatory body in charge of cybersecurity mandates. U.S. Ambassador Terry Kramer argued that including such regulations would be a "dead end" because countries need to be agile enough to respond to cyberattacks on critical infrastructure. He acknowledged that the threat of cyberattacks is a problem, noting that 67,000 malware attacks occur each day — double the number from 2009.

Cyber Security Policy News

-Last week was a tough one for identity theft crimes and consumers worried about protecting their personal data. Cyberthieves broke into a bank employee's computer in September 2011 and stole the password for the bank's online account with Experian Plc, the credit reporting agency with data on more than 740 million consumers. The intruders then downloaded credit reports on 847 people, according to [Bloomberg](#). The attackers took Social Security numbers, birthdates and detailed financial data on people across the country who had never done business with Abilene Telco, which has two locations and serves a city of 117,000. Reuters's Jordan Robinson writes that the incident is one of 86 data breaches since 2006 that exposes flaws in the way credit-reporting agencies protect their databases. Increasingly, instead of directly targeting Experian, Equifax Inc. and TransUnion Corp., hackers are attacking affiliated businesses, such as banks, auto dealers and even a police department that rely on reporting agencies for background credit checks.

In other identity crisis news, Social Security Numbers belonging to about 3.6 million residents in South Carolina have been exposed in an intrusion into a computer at the state's Department of Revenue, ComputerWorld [writes](#). Another 387,000 credit and debit card numbers were also exposed in the September attack, the state Department of Revenue said in a statement Friday. However, out of that number only about 16,000 of the credit and debit cards were unencrypted, the department added. The SSNs, meanwhile, do not appear to have been encrypted. Anyone who has filed a South Carolina tax since 1998 has been impacted by the breach and will be offered one year of identity protection service from Experian.

- Peter G. Neumann, an applied-mathematics student at Harvard who once lunched with physicist Albert Einstein, is now an 80-year-old computer scientist at SRI International and

leading a team of researchers in an effort to completely rethink how to make computers and networks secure, according to [The New York Times](#). Neumann is working on a five-year project financed by the Pentagon's Defense Advanced Research Projects Agency, or Darpa, with Robert N. Watson, a computer security researcher at Cambridge University's Computer Laboratory. "I've been tilting at the same windmills for basically 40 years," said Dr. Neumann recently during a lunchtime interview at a Chinese restaurant near his art-filled home in Palo Alto, Calif. "And I get the impression that most of the folks who are responsible don't want to hear about complexity. They are interested in quick and dirty solutions."

-Nearly one-third of the companies participating in a Pentagon pilot program to boost cybersecurity by sharing classified threat information have dropped out, apparently because it was too onerous to participate, according to [NextGov](#). Five of the 17 companies in the Defense Industrial Base Enhanced Cybersecurity Services group "chose to withdraw and reallocate their resources to other corporate priorities," InsideDefense reported, citing a Pentagon spokesman.

Meanwhile, the Homeland Security Department increased its cyber workforce by 600 percent over the last few years, but it still has a ways to go. Secretary Janet Napolitano said today DHS and the rest of government have been moving at 80 mph over the last few years and need to move at 120 mph to deal with the ever-increasing cyber threat. "We have great and fabulous people, and they attract fabulous people like them," Napolitano said during a discussion in Washington sponsored by [Washington Post Live and GWU](#). "We are in the midst of hiring. We need cyber folks, analysts, IT specialists and people who are familiar with code and coding."

The Cyber Security Policy and Research Institute (CSPRI) is a center for GW and the Washington area to promote technical research and policy analysis of problems that have a significant computer security and information assurance component. More information is available at our website, <http://www.cspri.seas.gwu.edu>.