GW CSPRI Newsletter

September 24, 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

-Sept. 24, 6:00 p.m. - 8:00 p.m., **Cybersecurity: Workforce Industry Building Learning Series Kickoff** - The Northern Virginia Community College's Workforce Industry Building Learning Series kickoff event about cybersecurity. Dr. Ronald Ross, one of the top 50 information technology decision-makers in government, will present about integrating cybersecurity requirements into mainstream organizational mission and business processes. The event is free to attend. All attendees will receive a complimentary dinner. Space is limited, so RSVP quickly. Ernst Cultural Center, Northern Virginia Community College, 8333 Little River Turnpike, Annandale, VA. To register, email camolinari@nvcc.edu or call 703-323-3281 or 703-323-3102.

-Sept. 26, 12:00 noon. The World Wide Web Consortium's (W3C) Tracking Protection Working Group will meet by teleconference. The call in number is 1-617-761-6200. The passcode is TRACK (87225).

-Sept. 27, **3rd Annual Billington Cybersecurity Summit** - A cross-section of over 25 confirmed federal, international and industry cyber experts will discuss late-breaking developments surrounding increasingly sophisticated threats to critical infrastructure. John Streufert, director, National Cybersecurity Division, DHS and Roberta Stempfley, deputy assistant secretary for cybersecurity, DHS, will be participating. National Press Club, 529 14th Street, NW. More information.

-Sept. 27, 5:00 p.m., **The State of the Hack** - The University of Maryland's Cyber Security Center will host a presentation by Kevin Mandia, CEO of Mandiant. This event is free, and open to the public, but registration is required. UM, Kim Engineering Building Lecture Hall, Room 1110, College Park, MD. More information.

-Sept. 27, 6:00 - 8:15 p.m., **An Evening with a Hacker** - The Federal Communications Bar Association will host an event a panel discussion. Confirmed speakers include Peter V. Roman, trial attorney, U.S. Department of Justice, criminal division, computer crime & intellectual property section; Amie Stepanovich, associate litigation counsel, Electronic Privacy Information Center; Stephen L. Surdu, vice president of professional services, Mandiant; Amy S. Mushahwar, associate, Reed Smith LLP. The deadline for registrations and cancellations is 12:00 noon on September 26, 2012. Bingham & McCutcheon, 2020 K St., NW. More information.

-Oct 1-3, **Military Cyber Security Conference** - This conference brings together the senior level military, government and industry experts who are defining the requirements and shaping the solutions in cyber security and computer network defense. The conference will examine the role and status of new defense organizations, the latest threats, and emerging tools/techniques for continuous risk monitoring and management. Sheraton Pentagon City, 900 South Orme Street, Arlington, VA. More information.

-Oct. 3, 1:00 p.m. - 2:30 p.m., **Complex Catastrophes: Improving Resilience of the Nation's Electric Grid** - The George Washington University's Homeland Security Policy Institute will host an event featuring the Honorable Paul Stockton, Assistant Secretary for Defense for Homeland Defense and Americas' Security Affairs. Assistant Secretary Stockton will discuss how to best address vulnerabilities of the electric power grid from physical and cyber threats. Elliott School of International Affairs, 7th floor, City View Room, 1957 E. St. NW. More information.

-Oct. 4, 7:30 a.m. - 11:45 a.m., **Cybersecurity 2013** - Federal Computer Week hosts a seminar on how to extend the principles of FISMA to devices and processes beyond traditional network perimeters, and methods to mitigate and manage malware. Speakers include Parmy Olson, London bureau chief, Forbes; and Ron Ross, computer scientist and NIST fellow, computer security division, National Institute of Standards and Technology. The Willard InterContinental Hotel, 1401 Pennsylvania Avenue NW. More information.

Legislative Lowdown

-A bill to require a police warrant for email snooping advanced in the Senate last week. The Senate Judiciary Committee on Thursday unanimously adopted an amendment that would require police to obtain a warrant before reading people's emails, Facebook messages or other forms of electronic communication. The Hill's Brendan Sasso writes that committee Chairman Patrick Leahy (D-Vt.) authored the amendment, which was added to a House bill, H.R. 2471, that loosens video privacy regulations. Under the Electronic Communications Privacy Act (ECPA) of 1986, police only need an administrative subpoena, issued without a judge's approval, to read emails that have been opened or that are more than 180 days old. Police simply swear an email is relevant to an investigation, and then obtain a subpoena to force an Internet company to turn it over.

But any major progress on the overall privacy reform measure will probably have to wait until after Congress returns from the November election, according to The National Journal. Leahy said he wanted to give members more time to work through some of the concerns they have with the legislation and a substitute amendment he offered to the bill that also would make changes to the 1986 Electronic Communications Privacy Act, which deals with government access to electronic communications. A broad coalition of tech companies and groups and privacy and

civil-liberties advocates have been pushing lawmakers to update the ECPA, saying that its protections are woefully out of date given the explosion of new technologies since it was first enacted.

Cyber Security Policy News

-A White House executive order on cybersecurity is “close to completion,” but Congress will still need to act to ensure security for American networks, Homeland Security Secretary Janet Napolitano said on Wednesday. NextGov reports that the draft order is being reviewed at the "highest levels" and some issues still need to be ironed out, she said. President Obama has yet to review it. If he decides to move forward, an executive order would likely establish a system of voluntary standards to be followed by certain critical companies, such as those that control chemical plants or power grids. The administration reportedly came under pressure to draft the order after Congress failed to reach an agreement to reconcile competing bills designed to shore up cybersecurity standards for the nation's most critical information networks.

-The Obama administration gets relatively poor marks for progress on cybersecurity reform, although there is plenty of blame to go around, according to a lengthy analysis published last week by Federal News Radio. FNR's Jason Miller compares the then and now clash of ideas versus reality. "Obama team came in knowing what needed to be done in 2009. And almost from the start set high expectations for themselves. In his 2008 campaign, Barack Obama reveled in being called the "Tech President." He issued a cyberspace policy review within 60 days of taking office and named the first White House position to focus solely on cybersecurity. The President laid out his vision for improving cybersecurity in a May 2009 speech, the first by a President on this topic." Sure, there were the inevitable turf battles over which branch of bureaucracy would take the lead in spearheading the proposed changes. But Miller argues that in the end, the regulation versus cost debate was one of the main reasons the administration's signature effort to get comprehensive legislation passed by both houses of Congress has failed so far. Others, such as the Internet Security Alliance's Larry Clinton say the White House approach to the legislation was doomed from the start. Sen. Susan Collins (R-Maine), one of the principal authors of the bill, put the blame at the feet of her fellow lawmakers. "I know of no area where the threat is greater and where we have done less," FNR quotes Collins as saying.

-With Congress failing to pass legislation strengthening the nation’s cybersecurity, leaders at the agency overseeing much of U.S. critical infrastructure are taking matters into their own hands, writes Amber Corrin for Federal Computer Week. Officials at the Federal Energy Regulatory Commission on Sept. 20 announced the creation of the agency’s new Office of Energy Infrastructure Security, which will work to reduce threats to the electric grid and other energy facilities. The goal is for the office to help FERC, as well as other agencies and private companies, better identify potential dangers and solutions. According to FERC, the OEIS will focus on developing recommendations for identifying, communicating and mitigating cyber and physical threats and vulnerabilities; providing assistance and expertise to other government organizations; participating in collaborative, interagency efforts; and conducting outreach to the private sector.

-Despite several years of escalating diplomacy and warnings, the U.S. is making little headway in its efforts to tamp down aggressive Chinese cyberattacks against American companies

and the government, the Associated Press reports. U.S. Defense Secretary Leon Panetta, who recently wrapped up three days of meetings with military and civilian leaders, said he has brought the issue up at every session and come away with little more than agreements to talk again. Meanwhile, cybersecurity analysts say the computer-based attacks emanating from China continue unabated, and in fact are expanding and focusing more intently on critical American oil, gas and other energy companies.

-Government auditors warned last week that agencies are not doing enough to sound the alarm nationwide about taking security precautions when using mobile devices. In a report that charted a steep rise in mobile malware, the Government Accountability Office called on federal agencies and telecommunications companies to step up efforts to implement baseline security measures for mobile devices and to do more to educate consumers on the need to protect their devices. The report (PDF) said the number of malware strains targeting mobile devices has nearly tripled in less than a year.

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.