THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE

Thoughtful Analysis of Cyber Security Issues

GW CSPRI Newsletter

November 28, 2011

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

Upcoming Events

- December 5, 9:00 a.m. Personal Information: The Benefits and Risks of De-Identification. The Future of Privacy Forum, with CSPRI as its academic co-sponsor, is hosting leading academics, advocates, Chief Privacy Officers, legal experts and policymakers as they discuss and debate the benefits and risks of de-identification, the definition of personal information and whether anonymization still matters. Location: The National Press Club, Murrow Room, 529 14th Street, NW, Washington, DC 20045. More information.

-Dec. 6, 8:30 a.m. - 5:00 p.m., **Securing Supply Chains in the Cyber Domain** - Speakers include Brett B. Lambert, deputy assistant secretary of defense, manufacturing and industrial base policy, Department of Defense; Larry Clinton, president and CEO, Internet Security Alliance; Steven R. Chabinsky, deputy assistant director, Cyber Division, Federal Bureau of Investigation; Jeffrey W. Irvine, deputy assistant director, Office of Investigations, US Secret Service. The Ritz-Carlton Pentagon City, 1250 South Hayes Street, Arlington, VA. More information.

-Dec. 8, 7:30 a.m. - 9:30 a.m., **Cyber Security: A Global Effort** - In 2007, Estonia was the victim of the first full-fledged cyber war, launched by Russia. At that time, Marina Kaljurand was serving as Estonia's Ambassador to the United States. Ambassador Kaljurand will join Government Executive on December 8 to share Estonia's experiences in weathering a cyber attack and what the future of international cyber cooperation might look like. Ronald Reagan Building, The Rotunda, 8th Floor (North Tower), 1300 Pennsylvania Avenue, NW. More information.

-Dec. 8-9, **12th Annual Cyber Security Expo** - Keynote speakers include Shawn Henry, executive assistant director of the Criminal, Cyber, Response and Services Branch at the FBI, and Edward Amoroso, senior vice president and chief security officer, AT&T Services Inc. The Walter E. Washington Convention Center, 801 Mount Vernon Place NW. More information.

Announcements

Each fall, approximately a dozen students pursue their bachelor's, master's, and doctoral degrees with federal funding from the National Science Foundation, the Defense Department, and the Department of Homeland Security. Federal funding provides two-year full scholarships (tuition, books, stipend, and in most cases room and board) for students to study computer security and information assurance at GW or a partner university. After completing their coursework, students will help protect the nation's information infrastructure by working as security experts in a government agency for two years. Since 2002, 56 students have graduated with help from this program, earning degrees in computer science, electrical engineering, engineering management, forensic sciences, business administration, and public policy. They have gone on to work at 36 governmental organizations.

The competition opens December 1 for scholarships starting in Summer or Fall 2012. Each year, CSPRI places an advertisement in the GW Hatchet to announce the scholarships. This year, Kathryn Neugent, a Computer Science graduate student, won a Kindle for her entry in a contest among current and former CyberCorps students to produce the ad. It features a cartoon from the webcomic website xkcd.com and will appear in the Hatchet on December 1 and in an animated sequence on the Hatchet website throughout December and January. View her winning ad here.

Legislative Lowdown

-House Intelligence Committee Chairman Mike Rogers (R-Mich.) will discuss his upcoming bipartisan cybersecurity legislation at an event sponsored by telecom industry groups on Nov. 30. According to The Hill, Rogers decried the growing threat of "cyber espionage" from Chinese hackers intent on stealing U.S. firms' trade secrets. Rogers announced the committee would be launching an investigation into Chinese telecom firms such as Huawei that operate in the U.S.

-Congress' failure to enact comprehensive cybersecurity legislation over the past half decade doesn't mean lawmakers haven't influenced IT security policy, says one of the House's leading authorities on cyber legislation. Jacob Olcott, who spent years on Capitol Hill as a top staffer on cybersecurity matters, told GovInfoSecurity, discusses how different cultures in the House and Senate affect how lawmakers approach cybersecurity legislation, and why, despite challenges, Congress will enact comprehensive cybersecurity legislation in an election year.

Cyber Security Policy News

-The U.S. Department of Homeland Security last week took aim at widespread media reports about a hacking incident that led to an equipment failure at a water system in Illinois, noting there was scant evidence to support any of the key details in those stories — including involvement by Russian hackers or that the outage at the facility was the result of a cyber incident. The Washington Post cites anonymous sources saying the water pump failure was in fact caused by a plant contractor traveling in Russia.

-Congress will pay the FBI an additional $18.6 million to better investigate computer hacking cases, following a federal study that found a third of bureau agents probing breaches significant to national security lacked the necessary networking and counterintelligence skills, according to NexGov. A spending package passed Nov. 17 to fund many federal agencies through September 2012 includes President Obama's full request for $166.5 million to tackle computer crimes, an 11.2 percent increase over last year's appropriations. The bureau must use the money to hire an additional 42 computer security professionals, including 14 special agents, according to a report accompanying the legislation.

-AT&T Inc., the largest U.S. telephone company, notified customers of an effort by hackers to collect online account information. The Associated Press reports that the company believes the perpetrators were unable to obtain access to customer online accounts or any of the information contained in them. AT&T said the hacking attempt used so-called auto script technology to “determine whether AT&T telephone numbers were linked to online AT&T accounts,” company spokesman Mark Siegel wrote in an e-mail. In a telephone interview, Siegel said that less than 1 percent of the Dallas-based company’s customers were affected.

In an apparently unrelated crime against the telephone giant, four people in the Philippines hacked into the accounts of AT&T business customers in the United States and diverted money to a group that financed terrorist attacks across Asia, authorities in the region told The New York

Times. The Federal Bureau of Investigations said on Saturday that it was working with the police in the Philippines on the investigation into the telephone hacking effort, which apparently began as early as 2009. The suspects remotely gained access to the telephone operating systems of an unspecified number of AT&T clients and used them to call telephone numbers that passed on revenues to the suspects, The Times reported.

-Former House Speaker and current Republican Presidential candidate Newt Gingrich said last week that if elected president, he would use cyber warfare to bring about regime change in Iran and would use military force to destroy its nuclear weapons. Gingrich told the New Hampshire Union Leader that electronic warfare should be used not only to attack Iran's nuclear development program, but also its economic system as a way to "break them down."

-US authorities have initiated the largest round of domain name seizures yet, as part of their continued crackdown on counterfeit and piracy-related websites, file-sharing news site TorrentFreak reports. In an action timed to coincide with "Cyber Monday," more than 100 domain names have been taken over by the Justice Department to protect the commercial interests of US companies. The Justice Department's National Intellectual Property Rights Coordination Center is expected to reveal further details about the takedowns in a press briefing.

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.