THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE

Thoughtful Analysis of Cyber Security Issues

GW CSPRI Newsletter

December 5, 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.

Contents

Upcoming Events

-Dec. 5, 10:00 a.m., Draft Legislative Proposal on Cybersecurity - The House Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies will hold a hearing. Room 311, Cannon House Office Building. More information.

-Dec. 6-8, **Federal Cyber Security Conference** - Threats to and emerging solutions for cyber security in the energy grid, interstate commerce, law enforcement, counterterrorism, banking, nuclear safety, telecommunications, electronic health records and many more potentially key

cyber targets will be examined during this three day program. Hilton Crystal City, 2399 Jefferson Davis Hwy., Arlington, VA. More information.

-Dec. 7, 9:30 a.m. - 2:00 p.m., **Second Annual Netezza Cyber Security Summit** - This conference will feature talks from retired General Michael Hayden, Jerry Derrick, Wayne Wheeles and Matt Stern who will discuss the growing threat of "Cyber War" and how agencies can stop reacting to the threat and instead start predicting the next attack. Ritz Carlton, 1700 Tysons Blvd., McLean, VA. More information.

-Dec 7-8, **Intrusion and Log Analysis Summit** - Talks at this conference will concentrate on network-centric and host-centric methods to detect intruders that work in the real world. The event will also focus on which logging configurations capture the history of a hacker's activity on a machine, from the establishment of unauthorized accounts to the installation of back-doors, enabling attendees to quickly isolate and repair affected systems after an intrusion. Embassy Suites Washington D.C. - Convention Center, 900 10th Street NW. 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.

-Dec. 9, 10:00 a.m. - 11:30 a.m., **Hacktivism, Vigilantism and Collective Action in a Digital Age** - The Center for Technology Innovation at Brookings will host a discussion exploring the impact of “hactivism” and vigilantism in a digital age. Panelists will examine the environment in which it emerged, implications for developing an effective cybersecurity agenda and how public policies can help deter particularly malicious behavior without quashing internet freedom. Speakers include CSPRI's Prof. Paul Rosenzweig (GW Law School), Prof. Gabriella Coleman, NYU, and Allan Friedman, the moderator for the Brookings Institution. To RSVP for this event, please call the Brookings Office of Communications at 202.797.6105 or click here.

Announcements

-Following CSPRI's debate Resolved: Cell Phone and Internet Blackouts by Government Agencies are Unconstitutional and Illegal, Absent a Declared National Emergency that took place November 16 at GW and that arose from the BART shutdown of mobile service, we can now report (thanks to Eric Burger, one of our commentators that day) that only under

extraordinary circumstances will BART now shut down mobile service. See http://www.bart.gov/news/articles/2011/news20111201.aspx for more details.

-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 is now open 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 the contest among current and former CyberCorps students to produce the ad. It features a cartoon from the webcomic website xkcd.com and appeared in the Hatchet on December 1. The ad will also be featured in an animated sequence on the Hatchet website periodically throughout December and January and can be seen at http://www.seas.gwu.edu/cybercorps/Hatchett%20Print%20Ad%20Dec%201%202011.pdf.

Legislative Lowdown

-The House Intelligence Committee approved a sweeping new cybersecurity bill last week, after the panel's chairman and ranking Democrat agreed to changes to address concerns of the White House, civil liberties advocates, and liberal Democrats. Politico writes that the measure would allow the government and private companies to share information about electronic threats and attacks. Private entities would participate on a voluntary basis and would receive significant liability protections in return. The White House and Democrats on the committee had expressed concerns about the possibility that information sharing could lead to invasions of privacy on matters unrelated to protecting the nation. The ACLU charged that the bill, in its original form, did not limit the type of information companies could share with the government. Others expressed fear that the bill could also concentrate private citizens' information in the hands of the National Security Agency, without restrictions on how the government could use the data.

Cyber Security Policy News

-Rep. Ed Markey (D-Mass.) urged the Federal Trade Commission (FTC) on Friday to investigate reports that mobile phone software developer Carrier IQ software tracks nearly everything that consumers do on their smartphones, The Hill reports. Trevor Eckhart, a systems administrator in Connecticut, posted a video earlier this week claiming to show that Carrier IQ, which is embedded in millions of Android, BlackBerry and Nokia phones, tracks users' every key stroke.

Sen. Al Franken also has demanded answers from Carrier IQ. Amid a media firestorm over the controversy, the company has repeatedly disputed that it is doing anything nefarious, and that it merely collects data about customer usage habits that is shared with the handset makers on request. Additional research on the company's technology indicates that many of the initial claims of nefarious activity by Carrier IQ may have been overblown.

-The hackers behind the Duqu botnet have shut down their snooping operation, writes ComputerWorld. The 12 known command-and-control servers for Duqu were scrubbed of all files on Oct. 20, 2011, according to Moscow-based Kaspersky Lab. That was just two days after rival antivirus firm Symantec went public with its analysis of Duqu, a Trojan horse-based botnet that many security experts believe shared common code and characteristics with Stuxnet, the super-sophisticated worm that last year sabotaged Iran's nuclear program.

-A cyber security expert has linked the Stuxnet worm to the indefatigable Conficker worm, drawing on similarities between the two sophisticated contagions. John Bumgarner, a retired U.S. Army special-operations veteran and former intelligence officer, told Reuters that Conficker was used to open back doors into computers in Iran, then infect them with Stuxnet. "Conficker was a door kicker," said Bumgarner, chief technology officer for the U.S. Cyber Consequences Unit, a non-profit group that studies the impact of cyber threats. "It built out an elaborate smoke screen around the whole world to mask the real operation, which was to deliver Stuxnet." Many within the security research community who have studied both worms extensively, however, strongly disagreed with Bumgarner's assessment, saying there was no link between the two worms.

-The FBI is warning that computer crooks have begun launching debilitating cyber attacks against banks and their customers as part of a smoke screen to prevent victims from noticing simultaneous high-dollar cyber heists, KrebsOnSecurity.com reports. The bureau says the attacks coincide with corporate account takeovers perpetrated by thieves who are using a modified version of the ZeuS Trojan called “Gameover.” The rash of thefts come after a series of heavy spam campaigns aimed at deploying the malware, which arrives disguised as an email from the National Automated Clearing House Association (NACHA), a not-for-profit group that develops operating rules for organizations that handle electronic payments. The ZeuS variant steals passwords and gives attackers direct access to the victim’s PC and network. In several recent attacks, as soon as thieves wired money out of a victim organization’s account, the victim’s public-facing Internet address was targeted by a network attack, leaving employees at the organization unable to browse the Web.

-A security protocol named 3 Domain Secure and adopted by Visa and MasterCard to cut down on online credit card fraud is being poorly and insecurely implemented by many banks, essentially negating the security value of the offering, new research suggests. Visa introduced the program in 2001, branding it “Verified by Visa,” and MasterCard has a similar program in place called “SecureCode.” Cardholders who chose to participate in the programs can register their card by entering the card number, filling in their ZIP code and birth date, and picking a passcode. When a cardholder makes a purchase at a site that uses 3DS, he enters the code, which is verified by the issuing bank and is never shared with the merchant site. Experts at Trend Micro wrote last week that a number of banks in the United States allow users to reset their passwords using little

more than the information on the card and the customer's ZIP code. As it happens, crooks have known about and been abusing this weakness for several years now.

-The National Institute of Standards and Technology is offering a free online HIPAA Security Rule Toolkit, a self-assessment tool that's designed to help healthcare organizations and their business associates comply with the rule, writes GovInfoSecurity. The stand-alone application, available for Windows, Mac and Linux, presents a series of questions in groups related to each of the Health Insurance Portability and Accountability Act's Security Rule standards and implementations specifications. It follows the established HIPAA structure of administrative, physical and technical safeguards; organizational requirements; and policies, procedures and documentation requirements.

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.