THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE
Thoughtful Analysis of Cyber Security Issues

GW CSPRI Newsletter

March 7, 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

-Mar. 7, Beyond the Beltway - This conference, now in its 6th year, is a market briefing on the $92 billion state and local government technology marketplace, and includes keynotes and roundtables from CTOs and CIOs from state and local governments. Ritz-Carlton – Tysons Corner 1700 Tysons Boulevard, McLean, VA. More information.

-Mar. 8, 9:00 a.m. - 4:00 p.m., **The SOCIALEX 2011** - The Social Media Legal Conference focuses on how to identify and manage legal risk associated with the use of social media, including: employment, privacy, copyright, intellectual property, anti-trust, defamation, marketing, terms of use, and trade secrets. University Club of Washington DC, 1123 16th St NW. More information.

-Mar. 8-9, **IANS Mid-Atlantic Information Security Forum** - The IANS Forums were inspired by the Harvard Business School method of teaching through case studies. Topics

of discussion at this conference include "Information Protection in the Age of Wikileaks," "Security Architecture 2.0," "Legal and Security Implications in the Cloud," JW Marriott Washington DC, 1331 Pennsylvania Ave NW. More information.

-Mar. 9, 2:00 - 3:00 p.m., **GovWin Cybersecurity Webinar** - Speakers from prime government contractors will explore the government's cybersecurity initiatives for 2011. Audience questions also will be taken prior to the event in the GovWin Q&A Forum, as well as during the Webinar. Speakers include **Tiffany Jones**, director of public sector strategy and programs, Symantec; **Mike Saintcross**, director of federal and mid-Atlantic sales, Agiliance; and **Stefen Smith**, chief security officer, SecureForce. More information.

-Mar. 9, 12 noon, **Investigating Cybersecurity Threats: Exploring National Security and Law Enforcement Perspectives** - GWU Professor Federic Lemieux, from the College of Professional Studies, will speak about how federal agencies define success in computer crime investigations, and how they can facilitate the development and refinement of law enforcement strategy for addressing cyber threats. Through interviews with experienced computer crime investigators from the Federal Bureau of Investigation, the U.S. Secret Service, and the Air Force Office of Special Investigations, this project aims to identify how federal agencies conduct investigations related to cyber security and how they define operational success. Room 302, Marvin Center, 800 21st St. NW. Full abstract (PDF).

-Mar. 9-11, **International Association of Privacy Professionals Summit** - Join privacy, security and data protection experts from around the globe for three days to discuss privacy challenges, debate the latest privacy issues, and get the answers you need. Washington Marriott Wardman Park, 2660 Woodley Rd., NW. More information.

-Mar. 15-17, **24th Annual Federal Information Security Educators' Association Conference** - This year's theme, “Bridging to the Future – Emerging Trends in Cybersecurity” was chosen to solicit presentations that reflect current projects, trends, and initiatives that will provide pathways to future solutions.National Institute of Standards and Technology (NIST), Administration Building (101), Green Auditorium, Lecture Room B, 100 Bureau Drive, Gaithersburg, Md. More information.

-Mar. 16, 8:00 a.m. - 3:45 p.m., **Symantec Government Technology Summit 2011** - This seminar will outline the steps federal, state and local government agencies should take to build a solid IT infrastructure. It provides an in-depth look at Symantec’s portfolio including Mobile Management and Security, Symantec Endpoint Protection, Data Loss Prevention. Grand Hyatt Washington, 1000 H St NW. More information.

-Mar. 16, 5:00 p.m., **Cyber Security East** - This conference brings together senior level military, government and industry experts in cyber security and computer network defense to examine the way forward for interagency cooperation, the latest DoD and government cyber security plans, initiatives and strategies, and what is being done to

protect critical infrastructure from cyber and other related threats. Holiday Inn Rosslyn, 1900 North Fort Myer Drive, Arlington, VA. More information.

Recent Appearances

CSPRI Assistant Director Costis Toregas is taking the cybersecurity message to the radio cyberwaves! Appearing on the Ajay Gupta "Technology Today" show broadcast on Internet radio on March 3, he spoke on a variety of themes, including the challenges posed by cybersecurity and the lack of an adequate pipeline of cyber workers emerging from universities and colleges. The entire hour long interview is posted here. Dr. Toregas' remarks, which include his views on the use of information technology to reduce the cost of government programs and enhance citizen services, begin at minute 16:20.

Legislative Lowdown

-**Sen. Charles Schumer** (D-NY) is urging major public Web sites in the United States to change their default Web addresses from the standard http:// connection to secure and encrypted pages (https://), following reports that hackers were able to access users' private information through insecure wireless networks found at coffee shops and bookstores around the nation, The New New Internet reports. In a letter to major Web providers, Schumer said these gathering spots online have a "responsibility to protect individuals who use their sites and submit private information." Once a complicated and sophisticated process, tapping into someone's computer has become an effortless task thanks to easy-to-use programs such as Firesheep. Through the insecure HTTP extension, hackers can get to the user's web browsing history and perform functions on websites as if they were the individuals who were hacked.

-The Senate Commerce Committee has scheduled a nomination hearing this Thursday for **Philip Coyle**, the White House's pick to become associate director of the Office of Science and Technology Policy (OSTP), TheHill.com reports.

Cyber Security Policy News

-**Bradley Manning**, the soldier believed to have leaked classified cables to Wikileaks, has been charged by the U.S. government with 22 new counts. One of the counts -- wrongfully causing intelligence to be published on the Internet knowing it would be accessible to the enemy -- is punishable by execution. Wired.com writes that while the government's prosecution team says it does not plan to seek the death penalty, the final decision of whether or not to impose that punishment rests with the convening authority.

-Friendly hackers and other computer whizzes who could help bolster government's cyber defenses often are unable to collaborate with the Homeland Security Department because

of outdated policies that Congress and the White House must reform, former DHS Secretary Tom Ridge said on Tuesday. Despite recruitment efforts through the higher education community, members of the hacker community remain wary of working with the government. They know how to find network weaknesses, but might be leery of sharing such talents, if lending a hand requires navigating through too much red tape. Ridge said Congress should revisit rules that restrict engaging private individuals in partnerships with the federal government.

-Funding for cybersecurity projects appears to be getting the axe in the major bill to keep the government operating through March 18, as the Republican-controlled House and Democratic-led Senate began negotiations on further cuts for the rest of the fiscal year ending in September, according to NextGov. Congress agreed to eliminate $20 million for network security programs in the major bill to keep the government operating through March 18, as the Republican-controlled House and Democratic-led Senate began negotiations on further cuts for the rest of the fiscal year ending in September. "The short-term continuing resolution signed into law on Wednesday will trim the Homeland Security Department account that safeguards critical networks and facilities far less than the $60 million cut House appropriators had proposed last month, reporter **Aliya Sternstein** wrote. "The stopgap bill deleted earmarks -- monies requested by individual lawmakers -- for the DHS infrastructure protection and information security program."

-Google was forced to pull more than 50 infected apps from its Android marketplace, after security researchers discovered that the mobile phone applications contained secret code designed to allow attackers to completely and remotely control the devices. Computerworld reports that the apps were available for about four days on the Android Market, Google's official app store. According to San Francisco-based smartphone security firm Lookout, between 50,000 and 200,000 copies of the apps were downloaded by users.

-Morgan Stanley experienced a “very sensitive” break-in to its network by the same China-based hackers who attacked Google Inc.’s computers more than a year ago, according to leaked e-mails from a cyber-security company working for the bank. **Michael Riley** reports for Bloomberg that the e-mails, from the Sacramento, California-based computer security firm HBGary Inc., which identify the first financial institution targeted in the series of attacks, said the bank considered details of the intrusion a closely guarded secret.

-Yeah, there's an app for that: The Federal Aviation Administration has approved Apple's iPad as an alternative to paper aeronautical charts for all phases of a flight, NextGov reports. "FAA-approved iPad applications were developed by Englewood, Colo.-based Jeppesen, and are being used by Executive Jet Management, a wholly-owned subsidiary of NetJets, which provides worldwide charter and aircraft management services," the story notes. "The iPad and the apps underwent testing on more than 250 flights with 55 pilots on 10 different aircraft models and had to be approved by FAA."

-A new report puts the term "Cyberwar" in a more provincial perspective, with the finding that most cyber skirmishes over the years appear to have stemmed from local or regional conflicts. Scott Borg, director and chief economist at the US Cyber Consequences Unit, a nonprofit research institute that investigates the dangers of cyberattacks, examined some 20 "significant" cyber conflicts since 1998, and found that most were not the work of nation-states, but rather of informal and loosely organized civilian groups - "cyber militias" -- sometimes aided by organized crime.

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.