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

GW CSPRI Newsletter

March 14, 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. 14, 9:00 a.m., **Federal Communications Commission's Security, Reliability and Interoperability Council Meeting** - Members will submit final reports that detail recommendations to the Commission on topics including cybersecurity best practices, media security and reliability best practices, transition to Next Generation 9-1-1, technical options for E9-1-1 location accuracy, and best practices implementation. The Council may take action on these final reports. The meeting is open to the general public, and also will be streamed over the Internet from this FCC Web page Room TW-C305, 445 12th St., SW. 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, 10:00 a.m., **Examining the Cyber Threat to Critical Infrastructure and the American Economy** - The House Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies will hold this hearing. 311 Cannon House Office Building. More information.

-Mar. 16, 10:00 a.m., **The State of Consumer Online Privacy** - Wednesday's hearing by the Senate Committee on Commerce, Science & Transportation will examine commercial practices that involve collecting, maintaining, using, and disseminating large amounts of consumer information, some of it potentially very sensitive and private in nature. It comes on the heels of two new reports by the Federal Trade Commission and the U.S. Department of Commerce calling for greater privacy protections for Americans online. Room 253, Russell Senate Building. 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.

Legislative Lowdown

-Four Democratic senators are asking Facebook to reverse a plan that would allow application developers to request users' phone numbers and addresses, reports The Hill. The senators cited Facebook's response last month to a letter from **Reps. Edward Markey** (D-Mass.) and **Joe Barton** (R-Texas) acknowledging the social network plans to allow application developers to request users' contact information.

-Sens. John McCain (R-Ariz.) and **John Kerry** (D-Mass.) are circulating a bill to create an online privacy bill of rights, a sign of bipartisan support for efforts to curb the Internet-tracking industry, The Wall Street Journal reports. The measure publication says the bill would require companies to seek a person's permission to share data about him with outsiders. It would also give people the right to see the data collected on them. The bill is expected to be introduced ahead of a Senate Commerce Committee hearing next Wednesday on online privacy.

-Federal News Radio reports that several cybersecurity bills are stalled in the Senate. Now one Senator is pressing the Obama administration to help un-jam things. Rhode Island Democrat **Sheldon Whitehouse** says it's up to the President's minions to tell Congress exactly what they want in a cyber bill before legislation can start moving again.

Meanwhile, NextGov reports that Whitehouse secured a promise from Homeland Security Secretary Janet Napolitano to establish a negotiating deadline.

Cyber Security Policy News

-Google has removed dozens of apps for Android-based devices from its apps store after they were found to be infected with malicious software known as DroidDream. The search giant also deployed a "remote removal function" to purge infected apps from Android devices running versions prior to 2.2.2. Google also deployed an app called "Android Market Security Tool," designed to undo the side effects from a previous malware attack against its mobile user base. The security tool was pushed to devices of users who had downloaded and installed infected applications. According to Symantec, cyber crooks responded by deploying a identically-named but compromised copy of the security tool designed to steal text messages from infected phones.

-South Korean government and commercial websites were the targets of recent cyber attacks. Over the weekend, at least 29 sites were hit with distributed denial-of-service (DDoS) attacks, assaults in which large numbers of "zombie" computers try to connect to a site at the same time in an attempt to overwhelm the server, the Associated Press reports. The attack follows a series of DDoS assaults last Thursday and Friday that hit the same number of sites.

-The French Finance Ministry is the latest victim of cyber attacks that appear to have emanated from China. Hackers infiltrated some 150 computers in the French Finance Ministry and pilfered data related to the G20 Summit, which France hosted last month, Voice of America reported. The attacks began in December 2010; only G20 data were affected.

-Microsoft is starting to actively discourage people from using Internet Explorer 6, a browser that first shipped with Windows XP more than a decade ago. CNET writes that the company has launched an official IE6 Countdown Site with graphics showing the percentage of market share IE6 holds in countries around the world; Microsoft hopes to see IE6 usage drop to less than one percent worldwide.

-The average organizational cost of a data breach jumped seven percent in 2010 to $7.2 million, or roughly $214 per lost record, says a new study from the Ponemon Institute. The survey, which examined the data breach experiences of 51 US companies from 15 industry sectors, found that in 2010, 43% of companies notified victims within one month of discovering a data breach, up from 36% in 2009. Quick responders had a per-record cost of $268 in 2010, up 22% from 2009; companies that took longer paid $174 per record, down 11%, the survey notes.

-A new academic research paper suggests that it is possible to break into newer-model cars' computer systems through Bluetooth and cellular network systems, and through diagnostic tools used by mechanics. The researchers, from the University of California,

San Diego and the University of Washington, followed up on a previous study they released last year describing how they were able to shut off a car's engine, lock the doors, turn off the brakes and falsify odometer readings.

-The U.S. Naval Academy has added cybersecurity classes to the core curriculum required of students, according to InformationWeek. The changes come as the Navy also is aiming to construct a facility for its Center for Cyber Security Studies (CCSS), which it created in December 2009 to increase cybersecurity education at the academy. Navy officials have said the service will spend up to $100 million for the new building, part of the Navy's push to promote the study of cybersecurity among its recruits and personnel.

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.