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

GW CSPRI Newsletter

August 15, 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

-Aug. 15, 11:00 a.m. - 12:30 p.m., **National EMP Recognition Day: The Threat That Can't Be Ignored** - A discussion of the cyber and physical threat from weapons and various natural events that emit an unusually strong electromagnetic pulse (EMP) capable of irreparably destroying electronic circuits. Heritage Foundation, 214 Massachusetts Ave., NE. More information.

-Aug. 18, 7:45 a.m. - 5:00 p.m., **CISO Executive Summi**t - A one day private peer to peer security event built "by CISOs for CISOs," allowing the top level security professionals from the region's largest enterprise company the opportunity to come together for a full day of collaboration, networking and best practices by their peers. Washington Marriott, 1221 22nd St. NW. More information.

-Aug. 18, 1:00 p.m., **Navigating the Rising Tide of Cyber Crime** - The U.S. Telecom Association will host a free Webinar. The speaker will be Tom Dotson, chief information officer at SureWest. More information.

-Aug. 19, 1:00 p.m. - 2:30 p.m., Ownership of Digital Media and Electronic Privacy - The American Bar Association will host a webcast panel discussion. More information.

Legislative Lowdown

-The House and Senate are in recess until Sept. 6 and 7, respectively.

Cyber Security Policy News

-Police in the U.K. and the United States took or contemplated taking unusually stringent methods to crack down on disruptive protesters. In response to a threatened protest in its subway system, San Francisco authorities temporarily shut down mobile phone service in the underground stations of the Bay Area Rapid Transit District, known locally as BART. Across the pond, the BBC reports that the government of U.K. Prime Minister David Cameron said authorities were exploring whether to turn off social networks or stop people from texting during times of social unrest. Texting and Blackberry Messenger are said to have been used by some during last week's riots in Britain.

-The FBI last week launched its very first app for the iPhone. Called "Child ID," the app is being billed as a convenient place to electronically store photos and vital information about your children so that it’s literally right at hand if you need it. "You can show the pictures and provide physical identifiers such as height and weight to security or police officers on the spot," the FBI said in a statement on its Web site advertising the new app. "Using a special tab on the app, you can also quickly and easily e-mail the information to authorities with a few clicks. The app also includes tips on keeping children safe as well as specific guidance on what to do in those first few crucial hours after a child goes missing."

-US regulators have warned electricity utilities to protect themselves from hacking attacks involving a simpler variation of the Stuxnet program that damaged Iran’s nuclear infrastructure last year. According to the Financial Times, the North American Electric Reliability Corporation (Nerc) issued an alert hours before a security researcher showed at the Black Hat security conference in Las Vegas last week that he could break into programmable logic controllers – computers that control automated processes – made by Siemens, even if they were protected by passwords. Other researchers at the conference said criminals and intelligence agencies would be able to use the Internet to hack into controllers made by other companies as well. Researcher Dillon Beresford of NSS Labs warned of widespread vulnerabilities in machines that are installed in tens of thousands of utilities and other industries. Siemens has fixed some of the issues – though it is up to customers to install the patches – and has begun work on others.

-A US District Court judge in Maine has approved a pending decision recommended by a magistrate stating that a commercial bank which protected customers' accounts with minimal authentication is in compliance with federal online banking security requirements. KrebsOnSecurity.com reports that Patco Construction had sued Ocean Bank following a series of fraudulent funds transfers totaling US $588,000. Part of Patco's argument rested on Ocean Bank's allowing the transactions to go through without taking adequate steps to verify their legitimacy. In late May, the magistrate ruled in the bank's favor, and on August 4 a judge made the ruling official. Patco has not decided whether it will appeal the decision. Similar suits are being tried in various federal district courts, but none qualifies as binding case law, which requires a ruling from an appellate court. For a decision to set a national precedent, a decision would be required from the US Supreme Court. A copy of the decision is available here (PDF).

-From Florida to Texas, more reports of pay-at-the-pump card-skimming scams are pouring in to law enforcement agencies, GovInfoSecurity writes. Last week, the National Association of Convenience Stores issued a statement about skimming trends in Tampa, Fla., saying the theft of debit and credit card numbers at pay-at-the-pump gas terminals has become nearly epidemic. And on Thursday, a detective with the Euless, Texas, Police Department said a months-long investigation into skimming at gas pumps throughout northern Texas has finally come to a close, after local authorities arrested and charged a 51-year-old fraudster for his role in masterminding the scheme.

-Rep. Mary Bono Mack (R-Calif.), the chairwoman of the House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade requested a briefing last week from security firm McAfee about a massive cyber-attack that the company identified last week, The Hill reports. The attack, dubbed Operation Shady RAT, targeted more than 70 government organizations and corporations in 14 countries. The United Nations, the Department of Energy and numerous defense contractors were all affected by the data breach.

-A US man charged with sending more than 27 million spam messages to Facebook users has turned himself in. Sanford Wallace, who is known as the "Spam King," surrendered to FBI agents in California. Prosecutors allege he developed a program that breached Facebook spam filters and lured users to submit their account details. Facebook sued Wallace in 2009 and a federal judge ordered him not to access Facebook's computer network. However, prosecutors say he repeatedly violated that order earlier this year. Wallace also lost a civil case brought against him by MySpace in 2008 over junk messages sent to members of the social networking site.