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

GW CSPRI Newsletter

April 25, 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

-Apr. 26, 9:00 a.m. - 4:30 p.m.: The National Institute of Standards and Technology's Voluntary Laboratory Accreditation Program (NVLAP) will host a one day workshop regarding the NIST Information Technology Laboratory, the Department of Health and Human Services, NVLAP accreditation of laboratories to perform testing of health information technology, and electronic health record technology. Location: Gaithersburg Marriott Washingtonian Center, 9751 Washingtonian Boulevard, Gaithersburg, MD. More information.

-Apr. 26, 8:00 - 11:15 a.m., **Securing the Virtualized Data Center** Advanced targeted attacks have been are growing in frequency and sophistication. At the same time, business demands to use consumer products, social networks, and cloud computing are

creating new vulnerabilities. Security defenses need to evolve in many areas to deal with both consumerization and the advanced persistent threat. This presentation will provide Gartner's projection of the most critical current and future threats and highlight key approaches for security evolution to deal with those threats. Gartner Federal Offices, 4501 Fairfax Drive, 7th Floor, Arlington, VA. More information.

-Apr. 27, 9:00 a.m. - 1:00 p.m., **Social Networking, Cloud Computing, Hacking Mitigation to Address Threats to Your Business and Personal Data** - The Washington County Chamber of Commerce and Rep. Roscoe G. Bartlett (R-Dist. 6) will hold a cybersecurity seminar and expo. Hagerstown Community College, 11400 Robinwood Drive. Free. Registration: 301-694-3030 or bartlett.house.gov.

-May 4-5, **Industry Control Systems Security and Looking at Cyber for Nuclear Power Plants** - This event, the Maryland Cybersecurity Center's first workshop, focuses on the critical infrastructure and the commercial nuclear power industry. Academic leaders at the university together with individuals from the Nuclear Regulatory Commission, the commercial nuclear power industry, and other research institutions will explore new regulatory and industry-led initiatives to protect nuclear power plants from cyber-based threats. More information.

-May 5, 7:30 a.m. - 4:30 p.m., **Government IT Leadership Forum** - Chief information officers from civilian, defense, and intelligence agencies will discuss cybersecurity, open government, cloud computing, data center consolidation, and more. Newseum, Knight Conference Center 555 Pennsylvania Ave NW. More information.

Legislative Lowdown

-The House will be in recess the week of Monday, April 18 through Friday, April 22, and the week of Monday, April 25 through Friday, April 29. The House will return at 2:00 PM on Monday, May 2. The Senate will be in recess the week of Monday, April 18 through Friday, April 22, and the week of Monday, April 25 through Friday, April 29. The Senate returns at 2:00 PM on Monday, May 2.

Cyber Security Policy News

-Both iPhones and Android phones regularly transmit their locations to Apple and Google, including unique telephone identifiers, new research shows. The revelations came to light after researchers **Alasdair Allan** and **Pete Warden** found that ever since Apple released iOS4, iPhones have been storing a long list of locations and time stamps, using the GPS location tracking capability built into the iPhone. The two found that the data is recorded and stored on the phones multiple times per hour, although there is no indication that the data is being transmitted from iPhones to Apple or anyone else, apart from being synched to the machine on which users back up their phones. Nevertheless, several lawmakers on Capitol Hill are now demanding answers from Apple. **Sen. Al**

Franken (D-Minn.) sent a letter to Apple CEO Steve Jobs with a series of questions. Meanwhile, **Rep. Edward Markey** (D-Mass.) is calling for a congressional investigation into the privacy practices of Apple and Google following the revelations.

At the same time, the U.S. Justice Department is asking the Supreme Court to reverse a lower court ruling on warrantless GPS tracking. Wired.com writes that the Obama administration is urging the high court to allow the government, without a court warrant, to affix GPS devices on suspects' vehicles to track their every move. The DOJ is asking the court to overturn a 2010 lower court ruling that reversed the conviction of a drug dealer that was based on warrants to search and find drugs in the locations where the defendant had traveled. Wired's David Kravets reports that the government told the justices that GPS devices have become a common tool in crime fighting. "An officer shooting a dart can affix them to moving vehicles, and recently, a student in California found a tracking device attached to the underside of his car, which the FBI later demanded back," Kravets wrote.

A case in Michigan shows how the law has failed to keep up with new technologies and the ways that authorities may be using them. A story by a libertarian blogger reported that the Michigan state police have been using a high-tech device that enables them to extract information from the cell phones of motorists stopped for routine traffic violations. The device, the "CelleBrite UFED," is capable of grabbing photos, video, and GPS data from an iPhone in as little as 90 seconds. It is compatible with 3000 different models of phone and can even circumvent password protection. The Michigan State Police denied the charge in a statement issued the following day that also blasted the ACLU. An ABC News piece by Diane Sawyer the following day seems to be the most even-handed treatment to date.

-The number of financial and confidential records compromised as a result of data breaches in 2010 fell dramatically compared to previous years, a decrease that cybercrime investigators attribute to a sea-change in the motives and tactics used by criminals to steal information, according to the fourth annual Data Breach Investigations Report released by **Verizon Business**. At the same time, the 74-page report (PDF) found that organizations of all sizes are dealing with more frequent and smaller breaches than ever before, and most data thefts continue to result from security weaknesses that are relatively unsophisticated and easy to prevent.

-Extortion and distributed denial of service (DDoS) attacks against computer systems at companies that run elements of the nation's critical power and electric infrastructure are on the rise, according to a report (PDF) released last week by **McAfee** and the **Center for Strategic and International Studies** (CSIS). The report, "In the Dark: Crucial Industries Confront Cyberattacks," states that many infrastructure providers are deploying new technologies without taking adequate measures to protect their cyber assets from attack. A quarter of all respondents said their companies had been targeted by extortion attempts either through cyber attacks or with the threat of cyber attacks.

The McAfee/CSIS survey also notes that China has bumped the United States as the most feared nation in cyberspace, and that 30 percent of global IT security professionals view China as the biggest cyber threat, with Russia rising to number two. The United States was number one last year, but the number of IT pros who see the U.S. as a major threat fell dramatically - from 36 percent last year down to 12 percent this year.

-Classified information regarding the nation's nuclear stockpile, management of nuclear nonproliferation activities and operation of the naval reactor programs stored on computers at the government's Lawrence Livermore National Laboratory in California are at risk, the Energy Department's inspector general warns in a new audit. According to the IG report, contractor officials made security-significant changes to national security systems that potentially increased the risk to those systems, without first obtaining approval from the federal authorizing official, the person ultimately responsible for accepting risks posed by changes to information systems.

The report comes as the Energy Department is still reeling from a hacker attack that shut down email systems and Internet access at the Oak Ridge National Laboratory in Tennessee. Computerworld reports that the attackers appear to have been trying to steal technical data, and that investigators believe that the attackers stole less than 1 GB of data before the break-in was discovered. Investigators say the attackers broke in with the help of a malware-laced "spear-phishing" email that was designed to look like it had come from the internal HR department, and that more than 10 percent of the employees who received the message said they clicked the link.

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.