THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY
AND RESEARCH INSTITUTE

Thoughtful Analysis of Cyber Security Issues

GW CSPRI Newsletter

November 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

-Nov. 7, 8:00 - 5:00 p.m., **Government Enterprise Architecture Conference** - Enterprise architecture (EA) practitioners will share strategies for applying EA methodologies to today's top government priorities, including cloud computing, information sharing, cybersecurity, and mobility. Ritz-Carlton Tysons Corner, 1700 Tysons Boulevard, Tysons Corner, Va. More information.

-Nov. 7, 9:00 a.m. - 2:00 p.m., **Cyber Defense: International Cooperation and Deterrence** - The Center for Strategic and International Studies hosts a discussion on the challenges and opportunities posed by the ideas of cyber deterrence and international cyber defense cooperation, their implications for the transatlantic security relationship, and their possible impact on relations between the alliance and non-NATO powers. CSIS, 1800 K St. NW. More information.

-Nov 8, 9:30 a.m., **Counterfeit Electronic Parts in the Department of Defense Supply Chain-** The Senate Armed Services Committee will hold a hearing. Dirksen Senate Office Bldg., Room SD-G50. More information.

-Nov. 8, 11:00 a.m. - 12 noon, **Cyber Threats 2011: Executive Guide for Law Enforcement -** In this webinar, Trustwave's Nicholas Percoco will address today's cyber security threats, including attacks against network devices, Web applications, mobile devices and social engineering scams. More information.

-Nov. 9, 2:30 p.m., **Your Health and Your Privacy: Protecting Health Information in a Digital World** - The Senate Judiciary Committee's Subcommittee on Privacy, Technology and the Law will hold a hearing, which will also be Webcast. Senate Dirksen Office Bldg., Room 226. More information.

-Nov. 10, **Deadline to Submit Comments on NIST Wireless and Bluetooth Security Guidelines** - This is the final day for submitting comments to the National Institute of Standards and Technology's Guidelines for Securing Wireless Local Area Networks (PDF), and NIST's Guide to Bluetooth Security (PDF).

Announcements

-On Nov. 16, CSPRI will host a debate on whether cell phone and Internet blackouts by government agencies are unconstitutional and illegal, absent a declared national emergency. Gregory T. Nojeim, senior counsel at the Center for Democracy & Technology and director of its Project on Freedom, will be arguing that such actions are unconstitutional and illegal. Taking the contrary stance will be Paul Rosenzweig, founder of Red Branch Law & Consulting, PLLC. Mr. Rozenzweig formerly served as deputy assistant secretary for policy in the Department of Homeland Security and twice as acting assistant secretary for international affairs. The debate begins at noon. Lunch will be provided at 1 p.m. to accompany a roundtable discussion with the debaters and with two additional experts, GW Prof. Amitai Etzioni, and Dr. Eric Burger, Georgetown University adjunct faculty member. Please RSVP to lunch and/or the seminar at https://csprieventblackouts.eventbrite.com. GW Marvin Center, 800 21st St. NW, Room 302.

-Adjunct GW Professor Mischel Kwon and former Cybercorps student P.J. Kelly were featured in last week's Bloomberg article about US Cybercorps programs, Students Trade Hacking Skills for US Scholarships.

Legislative Lowdown

-Sen. John Rockefeller (D-WV), chair of the Senate Commerce Committee, is still working to reach consensus on the data security bill that he and Sen. Mark Pryor (D-AR) introduced in June, writes Josephine Liu for InsidePrivacy.com. “A scheduled markup was canceled in September, and the committee decided not to consider the bill at yesterday’s executive session. Nonetheless, a spokesman for Sen. Pryor said Tuesday that lawmakers are ‘hoping to resolve any disagreements so the bill can be on a December markup,’” Liu reports. The bill, S. 1207, requires firms to establish information security policies for safeguarding personal information and to provide notice in the event of a security breach. Sens. Rockefeller and Pryor are reportedly reworking the bill in the hopes of securing bipartisan support.

-In the House, lawmakers on the Energy and Commerce Committee met last week to discuss Rep. Mary Bono Mack's (R-Calif.) SAFE Data Act behind closed doors, according to The Hill. The legislation would establish a national standard for data-breach notification for companies in the event consumers' personal information is compromised by an attack. A spokesman for Bono Mack said the meeting is aimed at resolving some concerns among Republicans on provisions in the bill regarding liability, the pre-emption language and the timing of the breach notification. The spokesman said lawmakers have made progress in the last few weeks and that there is still flexibility to address the remaining concerns.

Cyber Security Policy News

-U.S. intelligence officials have accused China and Russia of systematically stealing American high-tech data for their own national economic gain, the Associated Press reports. It was the most forceful and detailed public airing of U.S. allegations after years of private complaints. U.S. officials and cybersecurity experts said the U.S. must openly confront China and Russia in a broad diplomatic push to combat cyberattacks that are on the rise and represent a “persistent threat to U.S. economic security.” The comments came in a report released last week in which U.S. intelligence agencies said “the governments of China and Russia will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace.” GovInfoSecurity notes that the report doesn't just focus on China: Russia is also a major player and is quite aggressive.

The head of the Senate Intelligence Committee is calling for an “aggressive” response to an unprecedented counterintelligence report that names -- specifically China and Russia -- in its allegations of cyberespionage, reports NextGov. Chairwoman Sen. Dianne Feinstein, D-Calif., said in response to the report, “If we are to avoid overt cyber hostilities between nations, we must work as an international community. Getting more nations to sign onto the Budapest Convention -- authored by the Council of Europe, the United States and other nations -- is a good first step, but more aggressive actions are needed.” The 2001 convention is a binding pact governing international cooperation on the prosecution of computer crimes.

For its part, China dismissed the findings of the report as “irresponsible,” and repeated Beijing's long-standing position that it wants to help. “Online attacks are notable for spanning national borders and being anonymous. Identifying the attackers without carrying out a comprehensive investigation and making inferences about the attackers is both unprofessional and irresponsible,” Hong told a daily news briefing, as reported by Reuters.

-The Associated Press ran a story last week that said the Central Intelligence Agency secretly tracks millions of Tweets, Facebook updates, and other open sources of data for intelligence. “From Arabic to Mandarin, from an angry tweet to a thoughtful blog, the analysts gather the information, often in a native tongue,” AP's Kimberly Dozier wrote. “They cross-reference it with a local newspaper or a clandestinely intercepted phone conversation. From there, they build a picture sought by the highest levels at the White House. There might be a real-time peek, for example, at the mood of a region after the Navy SEAL raid that killed Osama bin Laden, or perhaps a prediction of which Mideast nation seems ripe for revolt.”

-The U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) and the Federal Communications Commission (FCC) will conduct the first nationwide test of the Emergency Alert System (EAS) on Wednesday, Nov. 9, at 2 p.m. EST. The test, which may last up to three minutes, will be played for up to three minutes along with the familiar “this is a test” message. The message is likely to be heard and seen on most traditional public airwaves. Under the FCC's rules, radio and television broadcasters, cable operators, satellite digital audio radio service providers, direct broadcast satellite service providers and wireline video service providers are required to receive and transmit presidential EAS messages to the public. The DHS said a national test will help the federal partners and EAS participants determine the reliability of the system and its effectiveness in notifying the public of emergencies and potential dangers nationally and regionally.

-The U.S. Supreme Court is expected to hear arguments this week in the case of U.S. v. Jones, questioning whether the government's warrantless use of a global positioning system (GPS) device to track a defendant's car violated his rights under the 4th Amendment.

-The Department of Defense announced last week that the TRICARE® Management Activity (TMA) has directed Science Applications International Corp. (SAIC) to provide one year of credit monitoring and restoration services to patients who express concern about their credit as a result of a data breach that occurred in Texas in September. Approximately 4.9 million patients treated at military hospitals and clinics during the last 20 years may have been affected by the breach. Potentially affected patients are being notified by letter. The data involved in the breach may contain names, Social Security numbers, addresses and phone numbers, and some personal health data such as clinical notes, laboratory tests and prescriptions. There is no financial data, such as credit card or bank account information, on the information that was taken.

-The National Institute of Standards and Technology is helping to change the way your office obtains and uses electricity. NIST has released a new roadmap for building the Smart Grid, adding a new list of standards, cybersecurity guidance and product testing proposals, according to Federal News Radio.

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.