THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE

Thoughtful Analysis of Cyber Security Issues

GW CSPRI Newsletter

December 19, 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.

We wish all of you a happy holiday season. We will resume publication on January 16, 2012.

Contents

Announcements

The Systems & Security Group at The George Washington University Computer Science Department is looking for scholars with a desire to advance the field of computer security. It has funded PhD and postdoctoral positions available starting in Fall 2012. The successful applicant will work with Prof. Michael Clarkson and the large cybersecurity community in DC to advance the state of the art in the scientific foundations of computer security. See http://faculty.cs.gwu.edu/~clarkson/positions.php for more information.

Mark your calendar for the January 25 CSPRI-sponsored lunchtime debate "Resolved: It makes sense to use the Internet's Domain Name System (DNS) to control bad behavior such as copyright and trademark infringement." After a warmup introduction by Leslie Daigle of the Internet Society on "DNS addressing explained for non-techies", Paul Brigner of the Motion Picture Association of America and David Sohn of the Center for Democracy and Technology will debate the topic. Registration information is at http://debateinternetdns.eventbrite.com.

Legislative Lowdown

-Members of the House Homeland Security Committee introduced a cybersecurity bill last week that would establish a quasi-governmental entity to oversee information-sharing with the private sector, according to The Hill. The Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness (PrECISE Act) encourages private firms to share information on cyber threats but stops short of mandating new security standards for sectors deemed critical to national security. The bill would clearly delineate the cybersecurity functions of the Department of Homeland Security by requiring DHS to evaluate cybersecurity risks for critical infrastructure firms and determine the best way to mitigate them.

-Sen. Joseph Lieberman (I-Conn.) said last week that congressional staff is reviewing a draft of the changes to FISMA, the bill that measures how prepared federal agencies are to meet cybersecurity challenges, FederalNewsRadio reports. Senate lawmakers have been trying to update FISMA for the last three years. Sen. Tom Carper (D-Del.) introduced a bill to update the 2002 law in 2008 and held out hope each successive year, but couldn't get enough traction. Rep. Diane Watson (D-Calif.) introduced a version of the FISMA update in 2010, but again, it got nowhere. Watson also tried to add a FISMA update to the 2010 Defense Authorization bill. But the provisions were not included in the final law.

-The House Judiciary Committee plans to resume its markup of the controversial Stop Online Piracy Act on Wednesday. A notice went out to staff late Friday to prepare to resume the markup on Wednesday, provided the House is still in session. There had been talk of the session being postponed until the new year.

Cyber Security Policy News

-As few as 12 different Chinese groups, largely backed or directed by the government there, do the bulk of the China-based cyberattacks stealing critical data from U.S. companies and government agencies, the Associated Press reported last week. The aggressive, but stealthy attacks, which steal billions of dollars in intellectual property and data, often carry distinct signatures, allowing U.S. officials to link them to certain hacker teams. And, analysts say the U.S. often gives the attackers unique names or numbers, and at times can tell where the hackers are and even who they may be.

-Iran claims it caused the crash of the U.S. military's state-of-the-art stealth spy drone by remotely manipulating the craft's global positioning system technology. According to a story in the Christian Science Monitor, the Iranian government says it led the stealth drone to an intact landing inside hostile territory by exploiting a navigational weakness long-known to the US military.

Meanwhile, Tehran has embarked on an ambitious plan to boost its offensive and defensive cyber-warfare capabilities and is investing $1 billion in developing new technology and hiring new computer experts, the Jerusalem Post writes. Iran has been the victim of a number of cyber attacks in recent years, some attributed to Israel. The most famous attack was by a virus called Stuxnet which is believed, at its prime, to have destroyed 1,000 centrifuges at the Natanz fuel enrichment facility by sabotaging their motors.

-Ronald Marks, a senior fellow at the George Washington University Homeland Security Policy Institute and a former CIA official, was interviewed by Federal News Radio's Francis Rose last week to talk about what the intelligence community is doing to manage the cyber revolution. Marks said the government has made great strides recently, citing the standing up of U.S. Cyber Command as a positive development. But he also noted how fast cyber has revolutionized government operations, which can leave agencies in a perpetual state of catch-up.

-President Obama said privacy concerns are keeping his family off Facebook for the most part. In an interview with People magazine, Obama said, "Why would we want to have a whole bunch of people who we don't know knowing our business? That doesn't make much sense." But when the First Lady points out that Malia is only 13 and Sasha 10 right now, the President laughs and adds, "We'll see how they feel in four years."

-The Federal Trade Commission in a Friday letter urged the Internet Corporation for Assigned Names and Numbers (ICANN) to rethink its plan to allow for new domain-name endings, warning that the current plan could harm consumers and hamper law enforcement. ICANN, a nonprofit group that manages the Web's naming system, approved a plan in June to allow for new generic top-level domain names in addition to traditional domain endings such as ".com" or ".org." Beginning on Jan. 12, organizations can apply for new addresses ending in almost any word or phrase. But the FTC warned that the plan could make it easier for scammers to set up fake websites to trick consumers and evade law enforcement. The commission explained that under the plan, "ABC Bank" could have the website "ABC.com," but a scammer could set up "ABC.bank," and another scammer could set up "ABC.finance." The plan for new domains also got a chilly reception from lawmakers in the House, who held a hearing on the idea last week.

-Revised guidance from the National Institute of Standards and Technology could help organizations protect themselves from a growing threat to their information assets: the insider, reports GovInfoSecurity. NIST Special Publication 800-63-1: Electronic Authentication Guideline expands the options for government agencies and other organizations that must verify the identity of users of their Web-based services. SP 800-63-1 updates guidance originally issued in 2006, and recognizes how technologies have changed over the past half decade.

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.