GW CSPRI Newsletter

July 9, 2012

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

Events

-July 7-15, **SANSFIRE** - In addition to a week's worth of security training, each evening the SANS Internet Storm Center handlers share talks on their most interesting experiences and newest cyber hazards. Hilton Washington & Towers, 1919 Connecticut Avenue NW. More information.

-July 9, 3:00 p.m. - 5:00 p.m., **Cybersecurity and American Power: Addressing New Threats to America's Economy and Military** - The American Enterprise Institute will host a speech by NSA Director Keith Alexander. The AEI notice states that this event will focus on "Chinese hackers". AEI, 12th floor, 1150, 17th St. NW. More information.

-July 10, 10:00 a.m., **Developing the Framework for Safe and Efficient Mobile Payments, Part 2** - The Senate Banking Committee will hold a hearing. Room 538, Senate Dirksen Office Building. More information.

-July 10, 1:00 p.m. - 2:00 p.m., **Privacy & Information Security Update** - The American Bar Association will host a webcast presentation. The speakers will include Aryeh Friedman, of Dun & Bradstreet; and Edward McNicholas and Elisa Jillson, both from Sidley Austin. To register, email jawelch@vorys.com.

-July 10-11, **U.S. Cyber Command Intelligence Support to Cyber** - Organized by the United States Cyber Command (USCYBERCOM), this conference will cover a range of cybersecurity issues, from creating a unifying intel strategy, to building shared situational awareness of the cyber threat to the Department of Defense, to developing a common understanding of current US adversaries' cyber capabilities policy and cyber challenges. NSA Headquarters, Ft. Meade, Md., OPS 1 Cafeteria Party Room. More information.

July 11-13, **Symposium On Usable Privacy and Security** - The eighth Symposium on Usable Privacy and Security (SOUPS), sponsored by Carnegie Mellon CyLab, will bring together an interdisciplinary group of researchers and practitioners in human computer interaction, security, and privacy. AAAS building in Washington, 1200 New York Ave., NW. More information.

Announcements

-Diana Burley, GW Associate Professor of Human and Organizational Learning and a Senior Research Scientist at CSPRI, has been appointed to the Cybersecurity Advisory Committee of the Virginia Joint Commission on Technology and Science.

Legislative Lowdown

-Senators are set to tackle legislation to protect the nation’s computer system when the upper chamber returns from its July 4th recess, but the efforts are being hampered by disagreements over the government’s role in overseeing cybersecurity standards, The Hill reports. Lawmakers of both parties worry that hackers are stealing America's business secrets and that an attack on a vital computer system could cause thousands of deaths. But sharp differences remain. Senate Democrats are still trying to round up the necessary 60 votes to bring their preferred bill to the floor. The House passed its own bill, the Cyber Intelligence Sharing and Protect Act (CISPA), in April. President Obama has threatened to veto CISPA, saying it would undermine privacy and would fail to protect the nation's critical infrastructure. The White House and Senate Democratic leaders have instead endorsed the Cybersecurity Act, sponsored by Sens. Joe Lieberman (I-Conn.) and Susan Collins (R-Maine).

Cyber Security Policy News

-Companies that operate critical infrastructure systems have reported a sharp rise in cybersecurity incidents over a three-year period, according to a new report from an arm of the Department of Homeland Security, Federal News Radio writes. In 2011, companies reported 198 cyber incidents to the Homeland Security Department — a nearly 383 percent increase above 2010, according to a June 28 report from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Companies reported nine such incidents in 2009., when DHS opened ICE-CERT to help protect private-sector operators critical infrastructure from "emerging" cyber threats. Water facilities claimed the lion's share of reported incidents, about 41 percent. ICS-CERT also logged reports from energy, nuclear and chemical facilities.

-Hundreds of thousands of computer users around the world -- and about 64,000 in the United States -- are in for a rude awakening today. Today is the date when systems still infected with the now-dormant DNSChanger Trojan will be blocked from accessing the Internet. In a bid to help users clean up infections, security experts won court approval last year to seize control of the infrastructure that powered the search-hijacking Trojan. But a court-imposed deadline to power down that infrastructure will sever Internet access for PCs that are not rid of the malware by July 9. According to security firm Internet Identity, 12 percent of all Fortune 500 companies and four percent of “major” U.S. federal agencies are still infected. PC World has published a guide to help you make sure your PC isn't among the unlucky.

-A decision handed down by a federal appeals court this week may make it easier for small businesses owners victimized by cyberheists to successfully recover stolen funds by suing their bank. The U.S. Federal Court of Appeals for the First Circuit has reversed a decision from Aug. 2011, which held that Ocean Bank (now People’s United) was not at fault for a $588,000 cyberheist in 2009 against one of its customers — Sanford, Me. based Patco Construction Co. The appeals court in Boston sent specific aspects of the earlier decision back to the lower court for review, but it encouraged both parties to settle the matter out of court. The appeals panel called the bank’s security systems “commercially unreasonable,” reversing a lower court ruling that Ocean Bank’s reliance on passwords and secret questions was in line with guidance set out by federal banking regulators. A copy of the decision is here (PDF).

-A car theft gang in the United Kingdom allegedly hacked into the computers of pricey cars, cloned their electronic keys and disabled their remote locking features, and then surreptitiously installed GPS devices to learn the best time and place to heist the cars, authorities there allege, according to The Telegraph. Alan Watkins, 42, created false identities for over 150 stolen cars worth up to £3.5m to sell them on in Cyprus. He particularly targeted models of BMWs, Audis and Range Rovers. Watkins had details of over 500 vehicles and had all the required documentation to create false registrations for over 300 stolen luxury cars - a practice known as 'ringing'.

-The Defense Advanced Research Projects Agency (DARPA) says it has developed prototype "disinformation technology," which is designed to identify insiders who leak information. Called "fog computing" in a playful nod to the burgeoning cloud computing industry, the technology involves identifying how suspected leakers search for data, then planting false but believable information and tracking its access and misuse, Wired's Noah Shachtman reports. The plan presents a couple of problems: first, the techniques resemble spammers' methods, and second, it could undermine trust at the very agencies where trust is critical to effective operations. The plan involves planting real valuable data in among large quantities of useless information, so if the data were to be leaked, those with the information would have a hard time distinguishing the truth from the phony data. The decoy documents would then be tracked as they cross the firewall. The Fog Computing project is part of a broader assault on so-called “insider threats,” launched by DARPA in 2010 after the WikiLeaks imbroglio.

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.