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

GW CSPRI Newsletter

September 6, 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

-Sept. 7, 8:30 a.m., **CDT's Congressional Agenda** - The Center for Democracy and Technology (CDT) will host an onsite and teleconferenced event to discuss the top ten issues on its congressional agenda, including the PROTECT IP Act, consumer privacy, data retention, cybersecurity, location privacy, data breach bills, and HIPAA privacy rules. The call in number is 1-800-377-8846. The password is 92713123. CDT, 1634 Eye St., NW.

-Sept. 7, 10.a.m., **Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats** - The Senate Judiciary Committee will hold a hearing that was rescheduled from Aug. 3. The witnesses will be James Baker, associate deputy attorney general, Department of Justice; Pablo Martinez, deputy special agent in charge, U.S.

Secret Service. This hearing will be Webcast. Dirksen Senate Office Building, Room 226. More information.

-Sept. 7, noon - 1:00 p.m., **Cyber Governance and Instability** - Paul Twomey, former president and CEO of the Internet Corporation for Assigned Names and Numbers (ICANN), will discuss the challenges posed by the present state of global cyber instability for governance at both the corporate and international levels. Council on Foreign Relations, 1777 F St, NW.

- Sept. 7, 1:00 p.m., **Health Care Information, HITECH Breach Notification and HIPAA Privacy & Security: Can you Demonstrate a Good Faith Effort?** - John Steiner, Chief Compliance Officer for Cancer Treatment Centers of America (CTCA), and Stephen Molen, Director of Solutions for EthicsPoint, co-host this Webcast to provide an overview of key principles in the HIPAA Privacy and Security Rules. More information.

-Sept 7, **Defense Systems Summit** - A full-day event focusing on military and defense data/network protection. The conference is free for all military and government personnel. Crystal City Marriott, 1999 Jefferson Davis Hwy., Arlington, Va. More information.

Legislative Lowdown

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

Cyber Security Policy News

-The hacking of a Dutch Web site security firm is apparently related to efforts to spy on Iranian Internet users. In July 2011, hackers used certificate authority Digitnotar's systems to issue dozens -- and potentially hundreds -- of fraudulent SSL certificates for some of the Web's most popular destinations, including google.com, android.com, microsoft.com, mozilla.org, skype.com, windowsupdate.com and wordpress.com. Security experts believe the fake certificates may have been used by the Iranian government to spy on citizens.

-Some 30 million customers of a top South Korean bank were unable to use ATMs or online services for several days earlier this year, thanks to a massive denial-of-service attack that is thought to have been waged by North Korea, The Washington Post writes. Western analysts who studied the incident agreed that the aggressor was probably North Korea, and described it as the first publicly reported case of computer sabotage by one nation against a financial institution in another country.

-Multiple servers used to maintain and distribute the Linux operating system were infected with malware that gained root access, modified system software, and logged passwords and transactions of the people who used them, according to a disclosure from the official Linux Kernel Organization. The infection occurred no later than August 12 and wasn't detected for another 17 days. The Register reports that a Trojan horse program was found on the personal machine of kernel developer Peter Anvin and later on kernel.org servers. A secure shell client

used to remotely access servers was modified, and passwords and user interactions were logged during the compromise. The maintainers said they believed the repositories used to store Linux source code were unaffected by the breach, although they said they were in the process of verifying its security.

-The military's war-fighting commands are unsure how to handle cyberspace activities, but a strategy that could alleviate the confusion is months from completion, Government Accountability Office analysts concluded in a report released last week. The Hill writes that the auditors found no consensus across the Defense Department as to what constitutes a cyber force. "Conflicting statements have led to confusion among the combatant commands about command and control over cyber operations," the publication quotes GAO officials as saying of the DoD's cyber strategy.

-Scam artists and fraudsters have been capitalizing on the public release of tens of thousands of email addresses and passwords for military personnel that were posted online earlier this summer, the FBI's Internet Crime Complaint Center (IC3) warns. On July 11, 2011, the hacker group Anonymous posted 90,000 email addresses and passwords, and a number of online merchants have begun reporting fraudulent orders from many of these email addresses within the last 30 days, the IC3 said.

-A 32-year-old paraplegic was sentenced to six years in prison for infecting more than 100 computers in a quest for financial information, nude photographs and thrill, ComputerWorld reports. Luis Mijangos worked as a freelance computer consultant in Santa Ana, California, earning about $1,000 per week writing programs and building websites. But he lived a double life, also earning as much as $3,000 per day hacking and stealing financial information from his victims.

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.