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

GW CSPRI Newsletter

March 21, 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

-Mar. 22, **Assumption Buster Workshop: Defense-in-Depth is a Smart Investment for Cyber Security** - This event is hosted by the National Coordination Office for the Networking and Information Technology Research and Development program. The NCO, on behalf of the Special Cyber Operations Research and Engineering (SCORE) Committee, an interagency working group that coordinates cyber security research activities in support of national security systems, is seeking expert participants in a day-long workshop on the pros and cons of the Defense-in-Depth strategy for cyber security. More information.

-Mar. 30, 7:30 - 9:30 a.m., **GovExec: WikiLeaks: Lessons Learned** - A complimentary discussion of what lessons the WikiLeaks incident has offered about information-sharing and cybersecurity. Ronald Reagan Building, The Rotunda, 8th Floor (North Tower), 1300 Pennsylvania Avenue, NW. More information.

-Mar. 30, 12:00-1:30, **Security and Privacy: Clinical Case Studies** - Dr. Neal Sikka, of the GW School of Medicine and Health Sciences, will be the featured speaker in the next CSPRI Cyber Security and Privacy Multidisciplinary Research Problems Seminar. All are welcome for the talk, but only a limited number of lunches can be provided, so if you plan to attend and also stay for lunch, please RSVP to the CSPRI Administrative Assistant at cspriaa@gwu.edu with a brief email by Thursday, March 24 so that we can reserve a lunch for you. GW's Marvin Center, 800 21st St. NW, Washington, DC, Room 302.

Announcements

This year's **Computers, Freedom and Privacy Conference**, June 14-16 at the Georgetown University Law Center in Washington, will feature a research showcase in the form of a research poster session on June 16 as well as a research panel that includes the authors of the best research posters. CFP focuses on topics such as freedom of speech, privacy, intellectual property, cyber security, telecommunications, electronic democracy, digital rights and responsibilities, and the future of technologies and their implications. Researchers who work in any of these areas are invited to submit research abstracts at the submission site. The deadline is April 3.

Legislative Lowdown

- **Rep. James Langevin** (D-RI) has introduced legislation to replace the paper-intensive compliance requirements of the Federal Information Security Management Act (FISMA) with automated, continuous monitoring, GovInfoSecurity reports. The bill, "The Executive Cyberspace Coordination Act," would create a National Office of Cyberspace in the White House, and would increase the Department of Homeland Security's authority over private networks that are part of the country's critical infrastructure.

-For the first time, the Obama administration is calling for legislation to protect consumers' privacy, USA Today reports. **Larry Strickling**, the head of the telecom arm of the Commerce Department, said during a Senate Commerce hearing on Wednesday that "the administration now recommeds that Congress enact legislation" after a lengthy study of privacy and after issuing a paper on the topic. Meanwhile in the Senate, John Kerry is trying to draft a privacy bill of rights with the across-the-aisle support of John McCain. Consumer groups are warning that Obama's privacy law is likely to be dominated by industry.

Cyber Security Policy News

-The chairman of security provider RSA -- a division of EMC Corp. - issued an "urgent" message to customers last week, warning that an "extremely sophisticated cyber attack against RSA" may have compromised the security of its SecurID two-factor authentication products. RSA's **Art Coviello** said digital information relating to SecurID tokens was stolen from RSA systems. Beyond that he offered few details about the attack, other than to say it was of a similar sophistication and precision to those constantly leveled against defense contractors and the U.S. government. An estimated 40 million SecurID tokens are currently in use. The devices most often are used to conduct financial transactions and at government agencies. The lack of detail provided so far has lead to broad speculation about the extent of the company's exposure, leading many experts to consider whether the security firm may have lost special processes or information needed to generate secret keys or tokens for the SecurID devices.

A top Senate Republican said called the attack on RSA an “urgent” sign for Congress to pass comprehensive cyber security legislation. **Sen. Susan Collins** (R-Maine), the ranking member on the Senate Homeland Security and Governmental Affairs Committee, stressed that the federal government was as equally prone to cyber attacks as the private sector and that Congress should act now before it's too late, The Hill reports.

-The Rustock botnet, a collection of hacked computers that at one point was responsible for as much as half of all spam worldwide, was knocked offline last week. Computers infected with Rustock stopped sending out spam on March 16, and initially researchers were not certain what caused the outage. On Thursday, The Wall Street Journal reported that Microsoft and a civil lawsuit were principally responsible for the takedown. Microsoft employed a novel legal tactic to seize control over servers and Internet addresses at more than a half-dozen hosting providers around the United States, in a bid to learn more about the Rustock author(s) and to prevent the giant botnet from resurrecting.

-The number of attacks on federal government networks increased 40 percent last year, according to a new White House report on cybersecurity, The Hill writes. Federal agencies reported 41,776 attacks in fiscal 2010 after seeing 30,000 the previous year, according to the Office of Management and Budget's annual report on implementation of the Federal Information Security Management Act (FISMA).

-The US Internal Revenue Service (IRS) has made some progress in improving the security of taxpayer information, but the agency still needs to work on preventing unauthorized access to systems, a report (PDF) issued last week by the Government Accountability Office (GAO) contends. FederalComputerWeek writes that the two-year audit found that 74 percent of the IRS’ previous information security weaknesses (65 of 88) had not been resolved. The report focused on a range of problems, including failure to restrict users' access to only the information necessary to do their jobs. The GAO also identified 37 new security issues in the audit.

-Research in Motion (RIM) is urging BlackBerry users to disable JavaScript in the smartphone's browser to block exploits from a security vulnerability showcased at a hacking contest in Canada last week, ZDNet reports. The vulnerability, which exists in the open source WebKit browser engine provided in BlackBerry Device Software version 6.0 and later, was exploited to hack into a BlackBerry Torch 9800 smart phone to steal the contact list and image database. In response to the hack, RIM issued a security advisory to acknowledge the flaw and suggest a temporary mitigation until a comprehensive patch is issued.

-The rogue hacking group known as "Anonymous" has released email messages that they say demonstrate fraud at Bank of America. The information, posted at Bankofamericasucks.com, appears to have been leaked by a former employee of Balboa Insurance, which used to be owned by the major financial institution. The former employee accuses Balboa Insurance of knowingly charging customers overinflated insurance premiums in the documents released. He also claims the firm has been falsifying loan documentation to proceed with foreclosures and that incorrect volumes have been reported to all lenders and federal auditors to avoid fines for falling behind on loan modifications.

-The National Institute of Standards and Technology's Computer Security Division released its draft "Personal Identity Verification of Federal Employees and Contractors" (PDF). The deadline to submit comments is June 6, 2011.

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.