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

GW CSPRI Newsletter

May 31, 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

-June 1, 9:30 a.m. - 11:30 a.m., **Cybersecurity: Assessing The Nation's Ability To Address The Growing Cyber Threat** - The House Oversight and Government Reform Committee will hold a hearing. Room 2154, Rayburn House Office Building. This hearing will be Webcast at this link.

June 2, 8:00 a.m. - 4:00 p.m., **Techstorm** - This event is exclusively focused on matching innovative technologies developed at universities and federal labs with entrepreneurs, industry professionals and investors looking for startup and licensing opportunities. The Mason Inn Conerence Center & Hotel, 4352 Mason Pond Drive, Fairfax, VA.

June 2, **Cyber Security Conference & Expo** - This free government cyber security event will review government and industry best practices for protecting data, strengthening identity and authentication procedures, and keeping systems tightly locked. Speakers will include **Stephen Elky**, deputy director for IT services, Library of Congress; **Patrick Howard**, director/chief information security officer, Nuclear Regulatory Commission; **Michele Iversen**, chief information system security officer, Department of Education; **John Kropf**, deputy chief privacy officer, Department of Homeland Security; **Chuck McGann**, corporate information security officer, U.S. Postal Service. Ronald Reagan Building, The Pavilion Room, 1300 Pennsylvania Ave., NW. More information.

June 2, 9:00 a.m., **Sony and Epsilon: Lessons for Data Security Legislation** - The House Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade will hold a hearing. Room 2123, Rayburn Building. More information.

June 2, 10:00 a.m. - 11:30 a.m.: The Executive Office of the President's National Security Telecommunications Advisory Committee (NSTAC) will hold a meeting that is open to the public. The agenda includes government use of cloud computing, the Federal Emergency Management Agency's (FEMA) national security and emergency preparedness communications, communications resiliency, and commercial satellite mission assurance. U.S. Chamber of Commerce, 1615 H St., NW. More information.

June 2, 12:30 p.m. - 2:30 p.m., **IRS E-File and Identity Theft** - The House Oversight and Government Reform Committee's Subcommittee on Government Organization will hold a hearing. Room 2247, Rayburn House Office Building. More information.

Announcements

-There is a new monthly seminar series at the National Science Foundation: the Washington Area Trustworthy Computing Hour (WATCH). The series will meet at NSF at noon on the first Thursday of each month, starting **June 2, 2011**. These talks will be held in Stafford I, Room 110, (4201 Wilson Boulevard, Arlington, VA) and the public is invited; no badges required.

The inaugural speaker is **Prof. Fred B. Schneider** of Cornell, who will speak on "Cybersecurity Doctrine: Towards Public Cybersecurity." Abstract: With increasing dependence on networked computing systems comes increasing vulnerability. The vulnerabilities are mostly technical in origin, but their remediation is not. Only by coupling technical insights with public policy do we stand a good chance to create a safer and more secure cyberspace. This talk will survey the landscape, discuss why past doctrines have failed, and propose a new doctrine of Public Cybersecurity. This is joint work with **Deirdre Mulligan**, a professor of law at the UC Berkeley School of Information and a Faculty Director of the Berkeley Center for Law and Technology.

Legislative Lowdown

The Senate Judiciary Committee last week unanimously approved a bill offered by Chairman Patrick Leahy (D-Vt.) that would grant new powers to the U.S. Justice Department in cracking down on piracy online. The Hill writes that the Protect IP act would empower the Justice Department to seek a court order against any infringing websites either domestic or foreign that can then be served on third parties, including Internet service providers, search engines and payment processors, to force them to cut off access to the site. Copyright holders can also file for a court order that would force payment processors to cut off payments to infringing sites. But opponents including Public Knowledge say the law will only spur criminals to create technological workarounds that will allow piracy to continue.

Cyber Security Policy News

-Lockheed Martin, the Pentagon's No. 1 supplier, experienced a major disruption to its computer systems last week that could be related to a problem with network security, Reuters reported last week. Reuters quoted the notable and pseudonymous blogger Robert Cringely as saying the slowdown began on Sunday after security experts for the company detected an intrusion to the network, according to technology blogger Robert Cringely. He said it involved the use of SecurID tokens that employees use to access Lockheed's internal network from outside its firewall. In March, RSA said it had sustained a data breach that could have compromised some of its security products, including its SecurID tokens. Its announcement shocked computer security experts, particularly because its systems are widely used. Shortly after RSA announced that breach, Lockheed, like many other large companies, said it had added an additional password to the process employees used to connect to its system from remote locations. One Lockheed executive, who spoke to The New York Times on the condition of anonymity because of security issues, said on Sunday that investigators “cannot rule out” a connection between the attacks on the RSA and Lockheed networks. EMC said in a statement on Sunday that it was “premature to speculate” on the cause of the Lockheed attack.

-Spam might not be such a problem if activists, banks and law enforcement took action to target the pressure points of these criminal enterprises: Specifically, the relatively few financial institutions abroad and at home that help process credit card payments for products advertised in junk e-mail, according to a paper (PDF) released last week by a research team from the University of California, San Diego, the University of California, Berkeley, The International Computer Science Institute and Budapest University. "It is the banking component of the spam value chain that is both the least studied and, we believe, the most critical," researchers state in the paper. "Without an effective mechanism to transfer consumer payments, it would be difficult to finance the rest of the spam ecosystem. The research notes that "only a small number of banks are willing to knowingly process what the industry calls high-risk transactions. In fact, just three banks, which are located in Azerbaijan, Denmark and the Caribbean island of Nevis, provided the payment servicing for over 95 percent of the spam-advertised goods in the study."

-The U.S. Chamber of Commerce criticized a new proposal by the Obama administration to help protect America's computer networks from cyber attacks, calling it "regulatory overreach," The Wall Street Journal wrote last week. The criticism comes as a blow to the White House, where officials thought they had secured the influential business group's support. The Chamber's stance could threaten the prospects for the administration's approach, cybersecurity specialists said.

-Instead of imposing mandatory new legal restrictions on publication of sensitive information, the nation would be better off if scientists, journalists and others adopted an ethic of self-restraint in what they choose to publish, a provocative new paper (PDF) suggests. The plan, described in the Naval Postgraduate School Homeland Security Affairs journal, is to promote self-censorship as a 'civic duty'. **Steven Aftergood**, director of the Federation of American Scientists' Project on Government Secrecy, said that overall, the Boyd paper tends to reinforce the "soft consensus" that new legal restrictions on dissemination of information are to be avoided. But he added that in most cases, those who are likely to be receptive to the appeal of voluntary self-restraint on publication of sensitive data probably have already embraced it. "News for Nerds" site Slashdot continues the discussion, asking: Who needs to censor themselves? According to the paper, "Amateur enthusiasts who describe satellite orbits, scientists who describe threats to the food supply, graduate students mapping the internet, the Government Accountability Office, which publishes failure reports on the TSA, the US Geologic Survey, which publishes surface water information, newspapers (the New York Times), TV shows, journalism websites, anti-secrecy websites, and even security author Bruce Schneier, to name a few."

-Federal investigators said last week that they have broken up a "sophisticated scheme to import and sell counterfeit Cisco-branded computer networking equipment" in the USA. The scheme was masterminded by a Virginia woman who made millions from the scam. Chun-Yu Zhao, of Centreville in Virginia and Donald H Cone, of Frederick in Maryland, were convicted by a federal jury on 24 May. Zhao was convicted on 16 counts, including conspiracy, importation fraud, trafficking in counterfeit goods and labels, false statements to law enforcement, false statements in naturalization and money laundering.

-India and the US are likely to give a boost to cyber-security cooperation, with a deal between the CERT-IN and US-CERT—the lead agencies in the respective countries to respond to cyber attacks. The CERT-IN (Indian Computer Emergency Response Team) and its American counterpart US-CERT are likely to sign a Memorandum of Understanding for sharing of expertise in artifact analysis (study of traces of virus and worm), network traffic analysis and exchange of information, The Deccan Herald writes.

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.