GW CSPRI Newsletter

February 21, 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

-Feb. 21, 8:00 a.m. - 10:00 a.m., **Cybersecurity Legislation in Congress: Where Does it Stand?** - Broadband Census News will host a discussion with speakers Ari Schwartz, senior policy advisor to the secretary, Internet Policy Task Force, Department of Commerce; Larry Clinton, president of the Internet Security Alliance; Tommy Ross, senior intelligence and defense advisor, Sen. Harry Reid (D-Nev.); and Nick Rossi, minority staff director, Senate Homeland Security and Governmental Affairs Committee. Clyde's of Gallery Place, 707 7th Street NW. More information.

-Feb. 21, 4:00 p.m. - 5:30 p.m., **Information Visualization for Knowledge Discovery** - Virginia Tech is launching a series of seminars focusing on issues that lie at the intersection of science and technology. Speakers will discuss visualization and information theory, cybersecurity and the complexity of language. Tuesday's event features Ben Schneiderman, computer science professor and founding director of the Human-Computer Interaction Laboratory, University of Maryland, College Park, and member of the National Academy of Engineering, will present “Information Visualization for Knowledge Discovery,” a lecture on visualization as it applies to temporal event sequences such as electronic health records and social network data. Virginia Tech Research Center - Arlington, 900 N. Glebe Rd., 2nd Floor. More information.

-Feb. 22, 8:30 a.m. - 4:00 p.m., **Success Strategies for Meeting the 2012 FISMA Requirements** - This conference covers the challenges facing agencies that need to comply with the new information security rules mandated by the updated Federal Information Security Management Act. Speakers from the Department of Homeland Security and NIST will be providing information and guidance related to trends and the new FISMA reporting metrics, processes and standards. UVA/Virginia Tech Center, 7054 Haycock Rd., Falls Church, Va. More information.

-Feb. 23, 7:30 a.m. - 1:40 p.m., **2nd Annual MobileGov Summit** - This conference will bring government and industry IT leaders together to share current issues, trends and best practices on how to create the next generation of mobile government workforce. Included in this discussion will be discussions on teleworking and remote computing security. Hotel Monaco, 700 F St. NW. More information.

Legislative Lowdown

-Senate Majority Leader Harry Reid (D-Nev.) plans to bring a cybersecurity bill straight to the Senate floor in the coming weeks, skipping any committee markups, according to The Hill. The move ignores the pleas from seven GOP senators to slow down the process and allow for multiple committees to hold hearings and markups of the legislation. The current measure, which was introduced by Sen. Joe Lieberman (I-Conn.) last week, would give the Homeland Security Department regulatory authority over companies with computer systems crucial to the nation's economic and physical security. It would require that the companies take adequate precautions to safeguard their systems and would increase information-sharing about cyber threats between the private sector and the government.

Republican opponents of the measure, lead by Sen. John McCain (R-Ariz.) and joined by the U.S. Chamber of Commerce, charged that the bill calls for too much regulation by the Homeland Security Department of critical infrastructure owners and operators. They also say the bill calls for redundant oversight mechanisms. Meanwhile, media advocacy groups are warning (PDF) that the cybersecurity bill could allow for more government secrecy and jeopardize the rights of whistleblowers.

Cyber Security Policy News

-Telecom switch maker Nortel Networks was repeatedly breached by Chinese hackers for almost a decade, The Wall Street Journal reported last week. The story told of a former Nortel employee who led an internal investigation into the security breaches, and published claims that the hackers stole seven passwords from the company's top executives - including the CEO - which granted them widespread access to the entire Nortel network. The news comes amid revelations that former Nortel CEO Frank Dunn, now being tried for fraud, was among several senior company managers who were aware of a long-standing data breach into Nortel's computers systems, but chose to do nothing.

-The Department of Homeland Security and the National Institute of Science and Technology (NIST) both would see increases in funding for cybersecurity efforts under the administration's FY2013 budget request. NextGov reports that the proposed budget (PDF) released by the White House last week requests $769 million to fund DHS's National Cyber Security Division activities, compared to $459 million requested for 2011. In addition, the request includes $1.2 billion for DHS's Infrastructure Protection and Programs Directorate, up from an estimated $888.2 million in spending for this year. Proposed funding for other cybersecurity efforts, as outlined by Federal News Radio, includes $93 million for US-CERT Operations, $12.9 million for virtual cybersecurity education and training, and $64.5 million for R&D. The budget also requests $708 million in funding for NIST, up $86 million from FY 2012, to "accelerate advances in a variety of important areas," including cybersecurity. In addition, it requests $52.6 billion in funding for the National Intelligence Program to support "Presidential cybersecurity priorities, including cybersecurity research and development."

-A group of American and European researchers announced last week that they had discovered an obscure but potentially dangerous weakness in the encryption technology that protects online shopping carts, e-banking and other Internet services from prying eyes, according to The New York Times. The researchers unearthed a weakness in the way certain secure sockets layer (SSL) keys are generated, pointing out that in a small but measurable number of cases SSL keys could be reverse engineered and provide attackers a way to intercept or inspect SSL-encrypted traffic.

-Google and several advertising companies have been bypassing the privacy settings of millions of people using Safari, the default Apple-supplied browser, The Wall Street Journal reported last week. According to WSJ reporters, Apple's Safari browser accepts cookies only from sites that a user visits; these cookies can help the site retain logins or other information. Safari generally blocks cookies that come from elsewhere – such as advertising networks or other trackers. But there are exceptions to this rule, including that if you interact with an advertisement or form in certain ways, it's allowed to set a cookie even if you aren't technically visiting the site. Google's code, which was placed on certain ads that used the company's DoubleClick ad technology and was uncovered by Stanford researcher Jonathan Mayer, took advantage of this loophole, as did the code used by the other companies.

The disclosure comes as Google is getting ready to consolidate 60 privacy policies into one, and its rival Apple is trying to crack down on third-party application providers who were reportedly using the programs to collect user information without explicit permission. The news prompted lawmakers to call on the Federal Trade Commission to investigate whether Google violated its consent decree by using ad cookies to surreptitiously track Web surfers on Apple's Safari browser.

-Computer science researchers are turning to the ways of nature for clues about how to best prevent cyberattacks. Researchers and faculty from Wake Forest University are polishing a genetically inspired algorithm that could be used in any large computer infrastructure, including cluster computing, Federal Computer Week writes. The algorithm proactively seeks out more secure computer configurations by using the concept of "survival of the fittest." Early simulations have shown the increased diversity of each device's configuration boosts network safety, and the research team said their goal is to create a moving-target defense that quickly detects threats. The initiative is funded by a one-year grant from Pacific Northwest National Laboratory.

-The District of Columbia has the highest rates of cybercrime victims in the nation, according to a new report from Symantec Corp. The company found that the nation's capital earned top (or bottom) marks in nearly all cybercrime stats, including malware infections and Web attacks. Seattle, San Francisco, Atlanta and Boston were other top cities on the list.

-Lawmakers on Capitol Hill are looking into the Department of Homeland Security's emerging programs to keep tabs on social media networks for signs of impending national security, hacking and nuclear threats, FederalNewsRadio reports. Most of the information about DHS' formerly-obscure social media monitoring program came into public view within the past month as the result of a Freedom of Information Act request by the Electronic Privacy Information Center (EPIC), which wanted more details about a program it saw as a potential violation of First Amendment rights. DHS ignored the request, so EPIC sued and got access to hundreds of pages of contract language between DHS and General Dynamics. The list of those to be monitored include specific Facebook and Twitter accounts, as well as niche news sites that cover security issues, including Wired.com Danger Room and krebsonsecurity.com, the personal blog of computer security journalist Brian Krebs.

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.