GW CSPRI Newsletter

April 2, 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

-Apr. 2, 12:00 noon - 1:00 p.m., **The White House's Proposal For A Framework for Protecting Privacy: Consumer Data Privacy in a Networked World** - The Internet Caucus hosts the event, which features Daniel Weitzner, deputy chief technology officer for Internet policy in the White House's Office of Science and Technology Policy. Those interested in attending this free event can register by contacting rsvp@netcaucus.org, or 202-407-8829. Lunch will be served. Room HC-5, Capitol Building.

-Apr. 2-4, **GovSec 2012** - This conference includes entire tracks of talks dedicated to critical infrastructure protection, cyber terrorism and cybercrime, network-centric security, and contingency planning and management. Walter E. Washington Convention Center, 801 Mount Vernon Place, NW. More information.

-Apr. 3-5, **FOSE Conference and Expo** - This year's Cybersecurity Conference focuses on the essential defensive security solutions from both the executive program view as well as the technical execution perspective. FOSE will deliver two tracks – executive and technical – that delve into federal CIO and CISO initiatives driven by recent changes in the federal Information

Security Management Act (FISMA). Talks will include a discussion of continuous monitoring programmatics and technologies, threat intelligence sources and strategies, and insider threats. Walter E. Washington Convention Center, 801 Mount Vernon Place, NW. More information.

-Apr. 9, 6:00 p.m., **Effective Cybersecurity: Perspectives on a National Solution** - The George Washington University's Homeland Security Policy Institute holds its 13th Annual Robert P. Maxon Lecture, featuring Wes Bush, Chairman, CEO and President of Northrop Grumman Corporation. Mr. Bush will discuss the pathway to improving the effectiveness of our national cybersecurity effort, through crafting effective and comprehensive public-private partnerships. GWU School of Media and Public Affairs, Jack Morton Auditorium, 805 21st St. NW.

Announcements

-Join us on April 11, 2012 6:30 p.m. the next discussion in the Frank Howard Distinguished Lecture Series: "Why We Won't Solve the Cybersecurity Problem." Lecture with reception to follow. Don't miss Prof. Eugene Spafford, one of the most well-known, noted and cited experts in cybersecurity research and education. He has an ongoing record of accomplishment as a senior advisor and consultant on issues of security and intelligence, education, cybercrime and computing policy to a number of major companies, law enforcement organizations, and academic and government agencies, including Microsoft, Intel, Unisys, U.S. Air Force, National Security Agency, GAO, FBI, National Science Foundation, U.S. Department of Justice, U.S. Department of Energy, and two U.S. Presidents. With over three decades of experience as a researcher and professor, "Spaf" has worked on various aspects of cyber security including software engineering, reliable distributed computing, host and network security, digital forensics, computing policy, and computing curriculum design. He is currently the chair of the ACM's US Public Policy Council.

We have been developing computing ("cyber") resources for over 60 years as an area of both research and practice. In that time we have made computing affordable, dependable, and ubiquitous. Today, there isn't a sector of society — government, commerce, research, entertainment — that doesn't depending on some underlying computational resource. Why, Prof. Spafford asks, despite decades of experience and research, are our cyber resources still so vulnerable? What are the factors that keep us from really addressing our cyber vulnerabilities? In this talk, he will summarize some of the biggest obstacles to protecting our cyber enterprises. These include problems of technology, economics, policy and simple human will. He will also discuss some of the factors that we can change, and thus improve the overall security of our systems in the future. George Washington University; Media & Public Affairs Building, Room B07; 805 21st Street NW; Washington, D.C. Free and open to the public but registration requested at https://secure.www.alumniconnections.com/olc/pub/GEW/event/showEventForm.jsp?form_id=117448.

-The new March-April 2012 issue of IEEE Security & Privacy magazine focuses on cybersecurity training and education. In it, an article, "Holistically Building the Cybersecurity Workforce" by three CSPRI-affiliated professors describes how fields such as public health care,

like cybersecurity, are inherently complex and cross-disciplinary. Professors Lance Hoffman, Costis Toregas, and Diana Burley encourage computer science educators, human resources professionals, and experts in cybersecurity to think beyond their individual fields and collaborate to produce an appropriate workforce for the years ahead. An abstract and pointer to the article (fee required) is at http://www.computer.org/portal/web/csdl/doi/10.1109/MSP.2011.181 and a slightly different pre-publication version is available free on the CSPRI website at this link (PDF).

Legislative Lowdown

The House and Senate will be in recess for the Easter break through April 13.

-The House Oversight and Government Reform Committee unveiled a bill last week to overhaul a decade-old law detailing how federal agencies protect their computer networks from cybersecurity threats. Reps. Darrell Issa (R-Calif.) and Elijah Cummings (D-Md.), the chairman and ranking member of the committee, respectively, introduced the legislation. The "Federal Information Security Amendments Act of 2012" would reestablish the Office of Management and Budget's role — as opposed to the Homeland Security Department's — in developing and overseeing agency cybersecurity guidance, Federal News Radio reports. That appears to put it at odds with competing cybersecurity bills in the Senate. One of them — the Cybersecurity Act of 2012 introduced by Sens. Joe Lieberman (I-Conn.), Susan Collins (R-Maine) and Jay Rockefeller (D-W.Va.) — calls for DHS to have a larger role in overseeing agency networks under FISMA. The other — the SECURE IT Act, introduced by Sen. John McCain — directs the Commerce Secretary to issue policies and guidance governing agency cybersecurity while tasking DHS with conducting ongoing security analyses and developing a timeline for establishing continuous monitoring of federal networks.

-House and Senate lawmakers introduced the SECURE IT Act, a legislative acronym which stands for "Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology." According to The Hill, the measure is an alternative to the Cybersecurity Act, which is backed by Sens. Joe Lieberman (I-Conn.), Susan Collins (R-Maine) and others. Unlike the Lieberman-Collins bill, the Republicans' SECURE IT Act would not give the Homeland Security Department the power to require that critical computer systems meet minimum security standards. Supporters of the SECURE IT Act warn that new regulatory powers would burden businesses and grow the budget deficit. Instead, that measure focuses on encouraging private companies to share information about cybersecurity threats with the government and toughening penalties for online crimes.

Cyber Security Policy News

-The United States is outgunned in the hacker wars, according to a frank assessment by the FBI's outgoing cyber chief. Shawn Henry, who is preparing to leave the FBI after more than two decades with the bureau, said in an interview with The Wall Street Journal that the current public and private approach to fending off hackers is "unsustainable." Computer criminals are simply

too talented and defensive measures too weak to stop them, he said. His comments weren't directed at specific legislation but came as Congress considers two competing measures designed to buttress the networks for critical U.S. infrastructure, such as electrical-power plants and nuclear reactors. Though few cybersecurity experts disagree on the need for security improvements, business advocates have argued that the new regulations called for in one of the bills aren't likely to better protect computer networks.

Meanwhile, former U.S. counterterrorism czar Richard A. Clarke warned last week that Chinese hackers have infiltrated every major American corporation, and that the effects for American innovation -- especially for corporate R&D -- may be brutal. In the interview, published in Smithsonian magazine, Clarke states that "I'm about to say something that people think is an exaggeration, but I think the evidence is pretty strong--every major company in the United States has already been penetrated by China." Clarke also alleges that Chinese hackers stole details about the manufacture of the F-35 fighter bomber, and that America's tech supply chain for chips, routers, and hardware may be infected with Chinese logic bombs, trapdoors, and Trojans waiting to be activated at a future date. Clarke, who runs a consulting group called Good Harbor Consulting (which counts cybersecurity consulting as one of its core businesses) said one of his greatest fears is a "death of a thousand cuts" for American innovation at the hands of corporate trade secrets systematically stolen by Chinese and foreign hackers.

In related news, it seems American intelligence officials are finding it less difficult to blame the Chinese for cyberattacks. Typically, U.S. military officials resist pointing fingers at China, even when many in the Internet security community say the country and its government are in cooperation to raid corporate secrets through concerted hacking campaigns. But last week, the director of the National Security Agency publicly blamed China for the high-profile cyber security breach at tech security giant RSA last year. According to Information Week, NSA director Gen. Keith Alexander told the Senate Armed Services Committee last week that China is stealing a "great deal" of military-related intellectual property from the United States and was responsible for last year's attacks against cybersecurity company RSA, U.S. Cyber Command commander and National Security Agency director. "I can't go into the specifics here, but we do see [thefts] from defense industrial base companies," Alexander said, declining to go into details about other attacks. "There are some very public [attacks], though. The most recent one was the RSA exploits." RSA had earlier pinned the attacks on a "nation state."

Wired.com has a different take on the Senate Armed Services Committee hearing. The NSA continued to downplay its role in the cyberdefense of private networks when Gen. Keith Alexander told a Senate committee Tuesday that his intelligence agency absolutely did not want to be lurking in private networks monitoring data for threats, the publication wrote. Instead, Alexander said the NSA should only play a role in providing malware signatures to private industry to help them monitor their networks on their own in order to detect threats. Companies could then tell the government about those attacks in real time so that the government could analyze and help stop them.

-In a piece for the Stanford Law Review, Scott J. Shackleford, assistant professor of business law and ethics at Indiana University's Kelley School of Business, takes stock of the competing

cybersecurity measures before Congress, and their prospects for passage and reconciliation, and potential for ameliorating the problems they purport to address.

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.