GW CSPRI Newsletter

March 26, 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

-Mar. 26, 9:00 a.m. - 3:00 p.m., **Developments in China's Nuclear and Cyber Programs** - The U.S. China Economic and Security Review Commission will hold a hearing. Hylton Performing Arts Center, 10960 George Mason Circle, Manassas, VA. More information.

-Mar. 27-29, **Federal Information Systems Security Educators' Association (FISSEA)**. Now a NIST program under the National Initiative for Cybersecurity Education (NICE), this year's theme, "A New Era in Cybersecurity Awareness, Training, and Education", will focus on security training on a budget, current cybersecurity projects, emerging trends and initiatives. Attendees will gain new techniques for developing and conducting training, professional development, networking, and an opportunity to meet industry partners at the Vendor Exhibit. CSPRI's Professors Lance Hoffman, Costis Toregas, and Diana Burley will lead a panel on "Leveraging Models from other Professions to Build a Holistic Cybersecurity Education Framework on Tuesday afternoon. More information.

-Mar. 27, 10:00 a.m., **IT Supply Chain Security: Review of Government and Industry Efforts** - The House Commerce Committee's Subcommittee on Oversight and Investigations will

hold a hearing. Witnesses will include Gregory Wilshusen, director of information security issues, Government Accountability Office (GAO); Mitchell Komaroff, director, trusted mission systems networks, U.S. Department of Defense; Gil Vega, associate CIO for cybersecurity and CISO, U.S. Department of Energy; Larry Castro, managing director, The Cherthoff Group; and Dave Lounsbury, vice president, The Open Group. Room 2123, Rayburn House Office Building. More information.

-Mar. 28, 10:00 a.m., **Cybersecurity: Threats to Communications Networks and Public-Sector Responses** - The House Commerce Committee's Subcommittee on Communications and Technology will hold a hearing. Witnesses will include Fiona Alexander, associate administrator, National Telecommunications and Information Administration (NTIA); James Barnett, chief of the FCC's Public Safety and Homeland Security Bureau; Bob Hutchinson, senior manager for information security sciences, Sandia National Laboratories; Greg Shannon, chief scientist, CERT, Software Engineering Institute, Carnegie Mellon University; and Roberta Stempfley, acting DHS Assistant Secretary for Cyber Security and Communications. Room 2322, Rayburn House Office Building. More information.

-Mar. 28, **Exposing the Recent Flood of Targeted Attacks** - Bradley Anstis, Vice President of Technical Strategy at M86 Security, presents an overview of today's Internet threat landscape and the steps that agencies can take to protect themselves. This webcast will look at the anatomy of common attacks such as spear-phishing, blended threat emails and malicious email attachments. More information.

-Apr. 2-4, **Network Centric Security Conference and Expo** - Keynotes and talks include discussions of mass notification, IT security, wireless technology, video analytics and access control. Speakers include Ralph S. Boelter, assistant director FBI Counterterrorism Division; Gordon Snow, assistant director, FBI Cyber Division; and Sen. George J. Mitchell, former U.S. special envoy for Middle East peace. Walter E. Washington Convention Center, 801 Mount Vernon Place, NW. More information.

-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.

Announcements

-GW's Computer Science Department is now accepting applications for a new Master of Science degree in cyber security. Students will follow a 30-credit curriculum in the program, which has the same core courses as the school's advanced computer science program, but includes many other cyber security courses. Applications have opened and are tentatively due by May 1. More details are available here.

-Join us on April 11, 2012 at 6:30 p.m. for the Frank Howard Distinguished Lecture sponsored by GW's School of Engineering and Applied Science. The topic is "Why We Won't Solve the Cybersecurity Problem". If you haven't heard Gene Spafford talk about cyber security, you now have the chance to see one of the most well-known acknowledged experts in cybersecurity research and education here at GW. "Spaf" 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. These include 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. Lecture with reception to follow. George Washington University; Media & Public Affairs Building, Room B07; 805 21st Street NW; Washington, D.C.

Legislative Lowdown

-The House Foreign Affairs Committee will meet on Tuesday, March 27 at 2:00 p.m. to markup H.R. 3605, the "Global Online Freedom Act of 2011". The bill's stated purpose is "to prevent United States businesses from cooperating with repressive governments in transforming the Internet into a tool of censorship and surveillance, to fulfill the responsibility of the United States Government to promote freedom of expression on the Internet, to restore public confidence in the integrity of United States businesses, and for other purposes." The markup will take place in Room 2172, Rayburn House Office Building.

The Hill writes that Rep. Chris Smith (R-N.J.) has been pushing the Global Online Freedom Act for several years, but the issue has gained more attention after countries including Egypt and Syria began shutting down Internet access and blocking websites to quell popular uprisings: David Hardin, an international trade attorney, said that in addition to the bill's regulations, it would raise publicity about companies cooperating with oppressive regimes and could pressure them to change their behavior. But he said the measure could create diplomatic challenges for the United States. He noted that the U.S. has close relations with the United Arab Emirates and Saudi Arabia even though "governments in those countries are known to conduct severe intelligence."

Cyber Security Policy News

-The US Department of Defense may issue rules of cyber engagement within the next one to two months, military officials said at a House Armed Services Committee hearing last week. The rules will set forth how the military should respond to cyber attacks and describe when they can take proactive defensive measures. According to Information Week, the policy, which the Joint Staff and the Office of the Secretary of Defense's Office of Policy have been collaborating on for "a long time," according to assistant secretary of defense for global strategic affairs Madelyn Creedon, builds on the DOD's Strategy for Operating in Cyberspace, released last year.

-The Pentagon is accelerating efforts to develop a new generation of cyberweapons capable of disrupting enemy military networks even when those networks are not connected to the Internet, The Washington Post reports. The possibility of a confrontation with Iran or Syria has highlighted for American military planners the value of cyberweapons that can be used against an enemy whose most important targets, such as air defense systems, do not rely on Internet-based networks. But adapting such cyberweapons can take months or even years of arduous technical work.

-Agencies that deal with national security data and programs must do more to secure their information technology supply chains, a government watchdog told lawmakers last week. NextGov writes about a Government Accountability Office (GAO) report finding that federal agencies aren't required to track "the extent to which their telecommunications networks contain foreign-developed equipment, software or services," and that they typically are aware only of the IT vendors nearest to them on the supply chain, not the numerous vendors downstream. The GAO warned that this deficiency has left IT systems at the Energy, Homeland Security and Justice departments more vulnerable to malicious or counterfeit software installed by other nations' intelligence agencies or by nonstate actors and hackers.

-In contrast to years past, when the majority of data breaches were motivated by financial theft, hacker activists such as the group Anonymous were behind 58 percent of all stolen data in 2011, according to a report (PDF) released last week by Verizon. The report, produced in conjunction with the U.S. Secret Service and law enforcement agencies in Ireland, the Netherlands, the United Kingdom and Australia, found that 58% of data stolen world-wide was the result of hacktivist activity even though they were responsible for only 3% of the incidents. Cyber criminals continue to be the biggest threat with 83% of data breaches.

-Two Democratic senators are asking Attorney General Eric H. Holder Jr. to investigate whether employers asking for Facebook passwords during job interviews are violating federal law, their offices announced Sunday. The New York Times reports that troubled by media reports of the practice, Senators Charles E. Schumer of New York and Richard Blumenthal of Connecticut said they were calling on the Justice Department and the Equal Employment Opportunity Commission to begin investigations. The senators are sending letters to the heads of the agencies.

-Eight US Internet service providers (ISPs) in the US, including the four largest in the country, have committed to implementing cyber security measures recommended by the US Federal Communications Commission (FCC) advisory board. The recommended steps are aimed at fighting botnets, domain name fraud, and Internet route hijacking. In all, eight ISPs committed to the measures, which include alerting customers when their machines show signs of being infected with botnet malware and helping them clean those computers. The eight ISPs provide service to approximately 80 percent of broadband users in the US. Critics of the plan note that while it is a positive step, the plan is voluntary and that ISPs should focus on cleaning up their pipes and preventing infections by blocking access to known malware locations.

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.