GW CSPRI Newsletter

March 10, 2014

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. 11, 7:30 a.m. - 6:30 p.m., **Symantec Government Symposium** - The Symantec Government Symposium is the largest annual public sector-focused gathering of the leading global IT thought leaders from government, academia and industry who come together each year for one day in Washington, D.C., to discuss top tech trends and share best practices through successful peer collaboration sessions. Renaissance Hotel Washington D.C. 999 9th St. NW. More information.

-Mar. 11, 4:00 p.m. - 5:30 p.m., **Technical Tuesday: Virtualization Technologies in Cyberwarfare** - Virtualization is often talked about in the context of cloud computing, cost savings and enterprise environments. In this talk, Jason Syversen of Siege Technologies will introduce Intel, AMD and ARM virtualization architectures and describe novel approaches to implementing virtualization technology/hypervisors for offensive and defensive cyber security applications. Case studies will be presented for malware detection, reverse engineering, code protection, security testing, stealthy code and other applications. Leidos (formerly SAIC) facility at 6841 Benjamin Franklin Drive, Columbia, MD 21046. More information.

-Mar. 12, 5:30 p.m. - 8:30 p.m., **NoVA Hackers Association Meetup** - An informal gathering of security enthusiasts and professionals in Northern Virginia. SRI International, 4350 Fair Lakes Court, Fairfax, VA, 22033. More information.

-Mar. 12, 7:00 p.m. - 9:00 p.m., **NovaSec Meetup**, East - Velocity Five, 8111 Lee Highway, Falls Church, VA, 22042. More information.

-Mar. 10-12, **2014 AFCEA Homeland Security Conference** - This conference offers an opportunity for attendees to engage with key government and industry leaders on critical security matters. Conference tracks will address big data analytics; continuous diagnostics monitoring; information sharing; and professionalization of cyber security. Ronald Reagan Building and International Trade Center - Atrium Hall and Ballroom, 1300 Pennsylvania Ave, NW More information.

-Mar. 17, 12:15 PM - 1:45 PM, **The Global War for Internet Governance with Dr. Laura DeNardis,** Despite its wide reach and powerful global influence, the Internet is a medium uncontrolled by any one centralized system, organization, or governing body, a reality that has given rise to all manner of free-speech issues and cybersecurity concerns. In her book *The Global War for Internet Governance*, Internet governance scholar and American University professor, Laura DeNardis reveals the inner power structure of Internet governance on the international scene and explores the characteristics of Internet Governance that will ultimately determine Internet freedom. Rebecca MacKinnon, author of *Consent of the Networked,* and Senior Research Fellow at New America called The Global War for Internet Governance "required reading" for understanding Internet governance and power and Jonathan Zittrain, author of *The Future of the Internet - And How To Stop It,* and professor of Internet Law at Harvard Law School praises it as "an invaluable resource for anyone wishing to understand the political intricacies behind Internet protocols and the diverse group of power players vying to influence them." This event will be held at New America for the DC book launch and conversation about the future of Internet governance in relation to free-speech, cybersecurity, international law, and global power. More Information.

-Mar. 18, 6:30 p.m., **Innovation Regulation: Powering the Internet of Things** - The "Internet of Things" is going to revolutionize how people conduct business, stay healthy, care for loved ones, get educated, be informed, drive cars, etc. It is now time to start having the important conversations about the technologies, security, data privacy, regulation and enormous potential and capabilities of the Internet of Things. 1776 (an innovation accelerator), 1133 15th St. NW, 12th floor Penthouse. More information.

-Mar. 18-20, **The Federal Information Systems Security Educators' Association (FISSEA): Partners in Performance: Shaping the Future of Cybersecurity Awareness, Education, and Training** - The conference is a forum in which individuals from government, industry, and academia involved with information systems/cybersecurity workforce development (awareness, training, education, certification, and professionalization) learn of ongoing and planned training and education programs and initiatives. Green Auditorium, NIST, 100 Bureau Drive, Gaithersburg, MD, 20899. More information.

-Mar. 19, 3:00 p.m., **Cyber Risk Wednesday: Risk and Resilience for the Financial Sector** - The financial industry spends more than any other sector on Internet security. Keeping a focus on resilience, this sector has perhaps the most extensive defenses to deal with threats that range from insiders, to organized crime, fraud, and intrusions, to nation-state sponsored disruptive attacks. With an existing global governance structure, the finance sector may be the most international of all infrastructure sectors. Yet gaps remain both within systemically critical firms and in the overall system itself that could initiate or amplify global cyber shocks. The fifth Cyber Risk Wednesday discussion will focus on cybersecurity challenges facing this sector and methods of reducing the existing and future vulnerabilities. 1030 15th Street, NW, 12th Floor. More information.

Legislative Lowdown

-The European Union is getting close to a vote on changes to rules and agreements that allow U.S. companies to process data belonging to European citizens, and the proposed changes, intended to keep that data out of the hands of the National Security Agency. The pending vote has many in the tech industry bracing for the worst, The Hill reports. "Starting on Monday, the EU Parliament will consider two measures that would affect the way American tech companies do business in Europe," Kate Tummarello writes. "The first is a privacy regulation that would end the Parliament's role in a two-year process to update, strengthen and make cohesive EU privacy law, heightening privacy and security standards for the companies that deal with European citizens' data. Once the Parliament approves the regulation, which is the expected outcome of next week's vote, the EU legislators have to negotiate over the law with the individual governments of EU countries."

Cyber Security Policy News

-A federal surveillance court has rejected the Obama administration's bid to hold onto millions of phone records beyond the current five-year limit, the National Journal writes. "The ruling is a rare rebuke for the government from the secretive Foreign Intelligence Surveillance Court. The court has rejected less than 1 percent of government spying requests over the past 30 years. But Judge Reggie Walton said he found the Justice Department's argument for extending the retention of phone records 'simply unpersuasive'."

-An lack of due diligence on behalf of a Big Three consumer credit monitoring firm, Experian, gave the proprietor of an online identity theft service access to more than 200 million consumer records, investigative reporter Brian Krebs reports. The information came to light in a hearing last week in which the owner of the identity theft service -- a Vietnamese national named Hieu Minh Ngo who was lured by Secret Service agents to Guam and then arrested and taken to stand trial in New Hampshire -- admitted running a service that catered to fraudsters involved in a variety of schemes, from tax fraud to identity theft. Posing as a private investigator from Singapore, Ngo tricked an Experian subsidiary into giving him access to countless consumers' personal and financial data. "Government investigators found that over an 18-month period ending Feb. 2013, Ngo's customers made approximately 3.1 million queries on Americans."

Krebs writes that while Experian has promised lawmakers that it will protect consumers who may have been impacted by the oversight, the data broker is not aware of any specific people victimized in the scam."

That may be cold comfort to lawmakers in the House who've had their identities stolen and are none too happy about it. As The Hill's Julian Hattem reports, "at a House Financial Services subcommittee hearing on the rash of data breaches and ways to protect people's data, lawmakers revealed that they, too, had been victims of identity theft. Rep. Carolyn Maloney (D-N.Y.), said during the hearing that she had spoken with fellow members of the Financial Institutions and Consumer Credit subcommittee and "all four of us have had our identities stolen." Another lawmaker, Rep. Robert Pittenger (R-N.C.), told members that he and his wife learned on Tuesday that their identity had been stolen, resulting in $4,000 of fraud.

-The Transportation Security Administration has canceled live tests of technology that would expand background checks on airplane passengers to include analyses of their online presences. According to NextGov, "the idea was to have contractors analyze consumer data -- potentially including dating profiles and shopping histories -- on fliers who apply for the voluntary "Pre-check" program. Pre-check, open to all U.S. citizens, lets passengers breeze through dedicated checkpoints without removing shoes, belts, laptops or TSA-compliant liquids after paying an $85 fee and proving their identities. The agency got as far as watching 'prototype implementations' but decided against trying a system out on actual passengers, according to a March 4 notice published in a government acquisition database."

-A new report shows that the Washington D.C. metropolitan area is a great place to live if you are in the market for a cybersecurity job. Burning Glass, which conducts daily reviews of job postings across 32,000 online sites, said in a report released last week that the nation's capital had more than 23,000 job postings for cybersecurity positions in 2013. The Washington Post writes that this is a "figure that far surpasses the number of such postings in any other region. New York had the second-highest number with just over 15,000. The San Francisco-San Jose metro area, which includes Silicon Valley, had more than 12,000."

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.