GW CSPRI Newsletter

March 18, 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

CSPRI Event:

-Mar. 26, 6:00 p.m. - 7:00 p.m., ***"DHS Cyber Forward: Resiliency and Partnership in a Networked World"*** - Dr. Phyllis Schneck serves as the Deputy Under Secretary for Cybersecurity and Communications for the National Protection and Programs Directorate (NPPD). Department of Homeland Security National Protection and Programs Directorate works with a vast number of partners within government, industry, and academia. Day-to-day, DHS not only protects the Federal civilian cyberspace, it partners with private sector critical infrastructure, responds to and investigates threats, engages all levels of state and local government, and collaborates with academia for research and to ensure a robust and capable cyber workforce. In our increasingly networked world, the way forward necessitates these robust and comprehensive partnerships to holistically address the varying nature and increasing number of today's cyber-threats. The event is free, but registration is required. Click here for the EventBrite page.

-Mar. 12, 1:00 p.m. - 2:30 p.m., **The Ethical Implications of NSA Surveillance for Lawyers** - The American Bar Association will host a webcast panel discussion. The speakers will be Dave Ries, member, Clark Hill Thorp Reed; John Simek, vice president, Sensei Enterprises; and Sharon Nelson, moderator, Sensei Enterprises. More information.

-Mar. 12, 1:00 p.m. - 2:30 p.m., **Police, Privacy and New Technologies** - The American Bar Association will host a webcast panel discussion. Speakers include David Gray, professor of law, University of Maryland; Jennifer Lynch, senior staff attorney, Electronic Frontier Foundation; and Robert M. Ross, magistrate, 15th Judicial District, Supreme Court of Virginia. More information.

-Mar. 12-15, **NIST Information Security and Privacy Advisory Board Meeting** - The Department of Commerce's National Institute of Standards and Technology's Information Security and Privacy Advisory Board will hold a meeting. The agenda includes Executive Order 13636 (cyber security regulation), legislative proposals regarding information security and privacy; the Federal Risk and Authorization Management Program (FedRAMP), federal cloud computing; and potential use of smart cards for Medicare, embedded software security. Residence Inn, 1199 Vermont Ave., NW. More information.

-Mar. 17-18, **NIST Smart Grid Advisory Committee Meeting** - Portrait Room, Administration Building, NIST, 100 Bureau Drive, Gaithersburg, MD. More information.

-Mar. 18, 8:30 a.m. - 12 noon, **First Data Cyber Security Symposium: Commerce in the Crosshairs: Solutions to the Growing Threat** - First Data's Cyber Security Symposium will provide a forum for data security professionals, merchants and financial institutions, among others, to discuss and explore several trends in payment security as well as the nature of the rapidly multiplying and evolving threats to global security. The speakers will include Mary Margaret Graham, former United States Deputy Director of National Intelligence for Collection; Fran Townsend, former Homeland Security Advisor to President George W. Bush; Art Coviello, Executive Chairman of RSA Security; and Alex Karp, CEO of Palantir. More information and registration.

-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. The time is now 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, 6:30 p.m. - 8:00 p.m., **ISSA DC Meetup: Man-in-the-Browser Session Hijacking** - This chapter of the Information Systems Security Association is based in Washington, DC and run by Bob Schlansker. The National Capital Chapter of the ISSA is comprised of information security professionals located in the Washington D.C. Metropolitan Area. Members are actively involved in information security in government agencies, the military, non-profit organizations, and in large and small companies. The chapter holds regular meetings at various locations throughout the D.C. area. Through its meetings and other events, the chapter fosters professional development and support for computer and information security professionals. Membership is open to practicing security professionals or to those with an interest in the profession. This talk will be given by Raphael Mudge, the founder and Principal at penetration testing firm Strategic Cyber LLC. Center for American Progress, 1333 H Street, NW. 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 forum in which individuals from government, industry, and academia who are 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 is also perhaps 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.

-Mar. 18, 6:00 p.m. - 9:00 p.m, **NoVa Infosec Meetup West** - A casual gathering of information security professionals in Northern Virginia. Velocity Five, 19286 Promenade Drive, Leesburg, VA, 20176. More information.

-Mar. 20, 7:00 a.m. - 3:45 p.m., **Intelligence and National Security Alliance: Security Policy Reform Implications for Industry: Maintaining Momentum for Transformational Change** - This unclassified, but sensitive symposium will be off the record, and will bring together stakeholders from the executive and legislative branches as well as their counterparts in the private sector. Following unprecedented attention on the security clearance process in 2013, 2014 promises to be a year of consequence to a fundamental aspect of how the IC carries out its mission. This symposium will provide attendees an opportunity to participate in the current debate and learn about future technologies that will influence security policies and procedures. The Honorable Stephanie O'Sullivan, principal deputy director of national intelligence of the ODNI will deliver the keynote address. The symposium panelists will include representatives from the CIA, DIA, DHS, ODNI and NSA. The SI Organization 15050 Conference Center Dr, Chantilly, Va. More information.

-Mar. 20, 5:30 p.m. - 8:30 p.m., **ISSA NoVA Meetup: Emerging Trends in Cybersecurity** - This chapter of the Information Systems Security Association is based in Reston, VA and is ISSA's largest chapter. The ISSA-NOVA chapter meets monthly (except August). The meetings are normally held on the third Thursday of each month, at various NoVA locations. Oracle, 1910 Oracle Way, Reston, VA, 20190. More information.

-Mar. 25, 8:30 a.m. - 4:30 p.m., **China Defense and Security Conference 2014** - The Jamestown Foundation will hold its Fourth Annual China Defense and Security Conference on March 25 in Washington, D.C. In keeping with the Foundation's mission, the conference will focus on understanding China's rising military power and strategy by carefully examining Chinese-language sources. Speakers at the conference will provide an extensive overview of recent developments in military training and operations reform, and take on challenging questions in Chinese foreign policy, including: How do Chinese leaders reconcile a drive to improve relations with neighboring states with increasingly aggressive actions in territorial disputes? Is popular nationalism an external constraint on Chinese policy-making, or it is cultivated to support China's positions? What is the role of cyber-warfare in Chinese strategic thought? Carnegie Endowment for International Peace, Root Conference Room, 1779 Massachusetts Avenue, NW. More information.

-Mar. 26, **SEC Cybersecurity Roundtable** - The Securities and Exchange Commission today announced that it will host a roundtable next month to discuss cybersecurity and the issues and challenges it raises for market participants and public companies, and how they are addressing those concerns. The growing interest in cybersecurity across financial markets and other sectors has raised questions about how various market participants can effectively manage cybersecurity threats. Cybersecurity breaches have focused public attention on how public companies disclose cybersecurity threats and incidents. SEC Headquarters 100 F Street, NE Washington, DC 20549. More information.

-Mar. 28, 7:30 a.m. - 11:00 a.m., **CyberBiz Summit** - Learn first-hand how to get your cyber business started, how to raise capital, and what to do to make it happen. The Westin Baltimore Washington Resort, 1110 Old Elkridge Landing Road Linthicum Heights MD 21090. More information.

-Mar. 28, 10:00 a.m. - 5:00 p.m., **Corporate Counter-Terrorism: The Role of Private Companies in National Security** - The keynote speaker will be John Carlin, assistant attorney general for national security at the Department of Justice. Speakers will include current and senior officials from the Justice Department, National Security Agency, Office of the Director of National Intelligence, FBI, DHS, Google, Microsoft, among others. American University Washington College of Law, 4801 Massachusetts Avenue N.W., Room 603. More information.

Legislative Lowdown

-Lawmakers on the Senate Intelligence Committee are coming "very close" to an agreement on a new cybersecurity bill, The Hill reports. "Lawmakers have for years pushed for a comprehensive bill to protect American financial markets, transportation systems and the electric grid in the event of a massive cyber attack. The Senate tried in 2012 to establish legislation with a set of security standards, but failed to overcome a Republican filibuster," The Hill's Julian Hattem writes. "One persistent problem for advocates of a bill has been ways to craft incentives for businesses to support a set of cyber standards without overly burdening them. Lawmakers have tried to offer some legal protection from lawsuits to companies that join the effort.

Cyber Security Policy News

-Top-secret documents reveal that the National Security Agency is dramatically expanding its ability to covertly hack into computers on a mass scale by using automated systems that reduce the level of human oversight in the process. The new revelations, offered by journalist Glenn Greenwald and Ryan Gallagher, note that the classified files – provided previously by NSA whistleblower Edward Snowden – "contain new details about groundbreaking surveillance technology the agency has developed to infect potentially millions of computers worldwide with malware 'implants.' The clandestine initiative enables the NSA to break into targeted computers and to siphon out data from foreign Internet and phone networks," the journalists allege, in their new publication Firstlook. "The covert infrastructure that supports the hacking efforts operates from the agency's headquarters in Fort Meade, Maryland, and from eavesdropping bases in the United Kingdom and Japan. GCHQ, the British intelligence agency, appears to have played an integral role in helping to develop the implants tactic."

The U.S. Foreign Intelligence Surveillance Court has temporarily reversed its earlier order that call records collected by the National Security Agency should be destroyed after the current five-year limit, according to IDG News. "The court modified its stand after a District Court in California on Monday ordered the government to retain phone records it collects in bulk from telecommunications carriers, as the metadata could be required as evidence in two civil lawsuits that challenge the NSA's phone records program under section 215 of the Patriot Act," the publication wrote. "The conflicting directives from federal courts puts the government in 'an untenable position' and are likely to create confusion and uncertainty among all concerned about the status of the data collected over five years ago, Reggie B. Walton, presiding judge of the FISC, wrote in his order."

Spy agencies at the service of democratically-elected governments are among the worst and most unrepentant online spies in the world, media watchdog group Reporters Without Borders says, putting them on the same level as offenders in Iran, China, and Saudi Arabia, ZDNet reports. "In the latest installment of the Enemies of the Internet report on Wednesday, wholesale spying by "free world" services — much of it exposed by US intelligence contractor Edward Snowden — has offered no distinction from the unabashed surveillance carried out by the world's worst dictatorships. Agencies such as the US National Security Agency, Britain's GCHQ, and the Centre for Development Telematics in India, embrace the worst methods of snooping in the name of governments that purportedly hold freedom of speech as a national priority."

-Last week, the US Commerce Department's National Telecommunications and Information Administration (NTIA) announced that it plans to transition key domain name functions to the global multistakeholder community. This is a significant step in the ongoing development of a truly global Internet. According to the Center for Democray & Technology (CDT), the transition will not happen until 2015 and there are many critical decisions to be made on how the naming system will be managed moving forward.

The NTIA's decision does not sit well with everyone. Rep. Marsha Blackburn (R-Tenn.), for instance, says the federal government has no business policing how cable television companies and other telecommunications firms provide access for customers large and small, writes Gannet's The Leaf Chronicle. "But some advocacy groups and other observers say that without stronger federal regulation, customers will soon have to worry about their favorite websites being blocked, loading at slower speeds or suffering other discriminatory treatment from Internet service providers. Blackburn says only a hands-off approach from Washington will foster a competitive market among service providers as well as the innovation and investment to improve the Internet experience for all."

Speaking of new frontiers in the Internet and domain name space, the world's first partisan top-level domain is set to launch: dot-GOP. But Hill watcher Roll Call says it's doubtful that Republican lawmakers are going to flock to the new domain space. "It would be surprising if many Republican candidates are anxious to put .GOP behind their name," the publication observes. "The Republican State Leadership Committee led the effort to secure the .GOP Web ending and unveiled it at the Beyond the Dot conference late last month. While the Web ending might bring some continuity to state parties and other functions of the Republican National Committee, it is not clear that the Web ending is a great tool for candidates to use in their campaigns." Read more here.

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.