GW CSPRI Newsletter

June 9, 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

Announcement

CSPRI-sponsored event: Views of the Estonian ICT Success Story: the Rise of Skype and E-governance

Two panelists will discuss Skype and E-governance. Click here for more information.

This event is co-sponsored with the GW Center for International Science and Technology Policy.

Events

-June 10, 10:00 a.m., **Emerging Technologies and the Future of Global Security** - A discussion of the book by the same name, which is available via the Web site of the Center for Global Security Research. The speakers will include Zachary Davis and Ron Lehman from the Center for Global Security Research, Lawrence Livermore National Laboratory; Michael Nacht, Thomas and Allison Schneider Professor for Public Policy, University of California, Berkeley; and Mathew Burrows, director, Strategic Foresight

Initiative, Brent Scowcroft Center on International Security, Atlantic Council. 1030 15th St NW, 12 Floor. More information.

-June 11, 8:15 a.m. - 4:00 p.m., **National Institute of Standards and Technology's Visiting Committee on Advanced Technology Meeting** - The agenda includes a presentation by the VCAT Subcommittee on Cybersecurity on "its progress on the review of NIST cryptographic standards and guidelines development process." Portrait Room, Administration Building, NIST, 100 Bureau Drive, Gaithersburg, MD. More information.

-June 11, 8:30 a.m. - 6:00 p.m., **The 2014 Cloud Computing Policy Conference** - The 2014 Cloud Computing Policy Conference USA will bring together over 150 delegates from the digital industries, the public sector, civil society and policymaking communities to debate the priorities facing the US cloud computing sector. It will explore market developments in cloud computing and how businesses and government administrations can best exploit the opportunities offered by the technology. Central to the discussions will be a debate on how to frame and deliver the necessary measures to restore trust following the PRISM revelations, ensuring that at both and home and abroad, the US continues to lead the way in cloud innovation and services. W Washington DC Hotel, 515 15th St NW. More information.

-June 11, 1:00 p.m. - 1:45 p.m., **What to Consider When Preparing to Purchase Cyber Insurance** - Join Christine Marciano, cyber insurance expert and president, Cyber Data Risk Managers, for this webinar to learn what your organization needs to consider before purchasing cyber/data breach insurance coverage. More information.

-June 11, 6:30 p.m. - 8:30 p.m., **OWASP Meetup: Analyzing and Reversing iOS Apps with iRET** - This talk will review the manual tasks that have traditionally been required in iOS penetration testing and then introduce a new industry tool called the iOS Reverse Engineering Toolkit (iRET) that will demonstrate how these manual tasks can be automated. This automation not only saves time, but also simplifies some of the more complex iOS reversing tasks. Thus allowing the tester to spend more time on areas of his/her testing that may require more attention and focus. Uber, 1200 18th Street NW, Suite 700, Washington, DC, 20036. More information.

-June 11, 7:00 p.m. - 9:00 p.m., **NovaInfosec Meetup East** - An informal gathering of security professionals in the Northern Virginia area. Velocity Five, 8111 Lee Highway, Falls Church, VA, 22042. More information.

-June 17, 6:30 p.m. - 8:00 p.m., **ISSA DC Meetup: The Five Stages of Grief** - How to Implement a Software Assurance Program - Presenters will share some of the challenges we encountered while implementing a software assurance program. We will discuss the various stakeholders, and their varying goals, expectations, and fears. The speakers will present suggestions based on our experience that may help your program gain acceptance and produce more secure software. In addition, the discussion will briefly describe Continuous Integration/DevOps and discuss some of the security benefits – and risks –

that come from this software development approach. Government Printing Office, 732 North Capitol Street, Washington, DC, 20401. More information.

-June 17-19, **NIST's Identity Ecosystem Steering Group (IDESG) 9th Plenary Meeting** - The National Strategy for Trusted Identities in Cyberspace (NSTIC), signed by the President in April 2011, states, "A secure cyberspace is critical to our prosperity." This powerful declaration makes clear that securing cyberspace is absolutely essential to increasing the security and privacy of transactions conducted over the Internet. The Identity Ecosystem envisioned in the NSTIC is an online environment that will enable people to validate their identities securely, but with minimized disclosure of personal information when they are conducting transactions. The IDESG is the private sector led organization created to achieve this mission by administering the development of policy, standards, and accreditation processes for the Identity Ecosystem Framework. Red Auditorium, NIST, 100 Bureau Drive, Gaithersburg, MD, 20899. More information.

-June 18, 7:30 a.m. - 1:30 p.m., **MeriTalk's Cybersecurity Brainstorm** - The second annual Cyber Security Brainstorm on Wednesday, June 18, 2014 at the Knight Conference Center at the Newseum in Washington, D.C. The event will bring together savvy Federal cyber security experts to share best practices, collaborate on challenges, and discuss what is needed for the future of cyber security. As cyber security is front and center in 2014 for Federal IT management professionals, this half day program will examine the evolving dialogue on issues including continuous monitoring, information sharing, cloud security, and cyber threats. Knight Conference Center at the Newseum, 555 Pennsylvania Ave., N.W. More information.

Legislative Lowdown

-While Congress seemed primed to act on cybersecurity legislation in the wake of the breaches at retailers Target, Neiman Marcus and Michaels, none of the many bills introduced in the wake of these incidents have moved out of committee, The Hill writes. "With time running out before the midterms and the end of the legislative session, the odds are increasing that Congress will fail to pass a bill this year," writes Julian Hattem. "After the hacks, at least a half-dozen congressional committees held hearings on the issue across Capitol Hill. Multiple bills were introduced to protect people's information, give more power to regulators, and let consumers know if their data might have been stolen." Chief among the sticking points are criticisms from consumer advocacy groups, who have warned that a national data breach disclosure law may preempt stronger state statutes, leading to a weaker disclosure standard than is currently in place, which is tied to the states with the most strict disclosure regulations.

-After what some see as a loss in the House, pro-reform lawmakers and advocates are hoping for a comeback in the upper chamber, where they are seeking an end to the NSA's collection of bulk data from phone calls involving people in the United States, reports Kate Tummarello for The Hill. "Advocates for reform thought they would win in the House after Patriot Act author Rep. Jim Sensenbrenner (R-Wis.) offered legislation to

end bulk collection," Tummarello writes. "But in eleventh-hour negotiations between House leaders and the administration, reformers say the bill was watered down in a way that could allow bulk collection to continue. Specifically, the final bill included an overly-broad definition of "selectors," the terms intelligence officials can use to search for information in large data sets."

Meanwhile, legislation to rein in the NSA's surveillance powers could actually expand them, according to representatives from the agency itself who spoke at a Senate hearing last week. Rick Ledgett, the NSA's deputy director, acknowledged during a Senate hearing that the USA Freedom Act could 'potentially' help the NSA gain access to records on millions of cell phone calls that are currently out of the agency's reach. 'Under the guise of further protecting privacy … the universe [of call records] will be exponentially larger than what the prior system was,' Sen. Mark Warner, a Virginia Democrat, warned during a hearing of the Senate Intelligence Committee.

Cyber Security Policy News

-In the wake of non-stop disclosures about National Security Agency programs to hoover up massive amounts of data from Internet users, the giants of the Internet are taking steps to make it far more difficult — and far more expensive — for the National Security Agency and the intelligence arms of other governments around the world to pierce their systems. "Google, for example, is laying its own fiber optic cable under the world's oceans, a project that began as an effort to cut costs and extend its influence, but now has an added purpose: to assure that the company will have more control over the movement of its customer data," writes The New York Times. "A year after Mr. Snowden's revelations, the era of quiet cooperation is over. Telecommunications companies say they are denying requests to volunteer data not covered by existing law. A.T.&T., Verizon and others say that compared with a year ago, they are far more reluctant to cooperate with the United States government in "gray areas" where there is no explicit requirement for a legal warrant."

-The FBI joined law enforcement agencies in several countries last week in disrupting the "Gameover" botnet, a collection of an estimated 1 million hacked PCs that were used for more that $100 million in online banking heists and were instrumental in spreading "Cryptolocker," a contagion that held victim files for ransom. "Gameover is based on code from the ZeuS Trojan, an infamous family of malware that has been used in countless online banking heists," writes KrebsOnSecurity.com. "Unlike ZeuS — which was sold as a botnet creation kit to anyone who had a few thousand dollars in virtual currency to spend — Gameover ZeuS has since October 2011 been controlled and maintained by a core group of hackers from Russia and Ukraine. Those individuals are believed to have used the botnet in high-dollar corporate account takeovers that frequently were punctuated by massive distributed-denial-of-service (DDoS) attacks intended to distract victims from immediately noticing the thefts. According to the Justice Department, Gameover has been implicated in the theft of more than $100 million in account takeovers."

-Anyone who said cybercrime wasn't a growth industry hasn't been paying attention these past few years. "That's the main message from former U.S. intelligence officials, who in a report today outlined scenarios for how $445 billion a year in trade theft due to computer hackers will worsen," writes Chris Strohm, for Bloomberg. "They warned that financial companies, retailers and energy companies are at risk from thieves who are becoming more sophisticated at pilfering data from their servers. The outlook 'is increased losses and slower growth,' with no 'credible scenario in which cybercrime losses diminish,' according to the report published by the Washington-based Center for Strategic and International Studies. Some of the damage will be hard to trace, such as economic downturns caused by foreign competitors selling products based on stolen designs and financial markets undermined by hackers."

-The Department of Homeland Security hasn't done enough to secure the IT systems that manage American ports, according to a new report from the Government Accountability Office (GAO). "While the Coast Guard initiated a number of activities and coordinating strategies to improve physical security in specific ports, it has not conducted a risk assessment that fully addresses cyber-related threats, vulnerabilities and consequences," reads a report made public June 5 and covered by GovInfosecurity.com. "Each year, American ports handle cargo worth more than $1.3 trillion, and GAO says the operations of these ports are supported by information and communication systems that are susceptible to cyberthreats," reports Eric Chabrow.

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.