GW CSPRI Newsletter

July 7, 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

Announcements

Peter W. Singer and Allan Friedman (CSPRI Research Scientist), authors of *Cybersecurity and Cyberwar: What Everyone Needs to Know*, discuss the five biggest cybersecurity myths. Read the article here.

Events

-July 8, 1:00 p.m., **DNSSEC Key Security** - Because DNS was never designed with security in mind, inherent DNS vulnerabilities pose a risk to all Internet services. To counter these risks, DNSSEC is being deployed across the top level domains to guarantee the authenticity of the information in each domain's zones. DNSSEC uses strong key cryptography, the security of which depends on the robust protection of key material. This Webinar will cover the basics of setting up DNSSEC within your environment. More information.

-July 8, 4:00 p.m., **You're Gonna Need A Warrant for That: The Path to Digital Privacy Reform** – A unanimous Supreme Court recently declared that that our networked mobile devices merit the highest level of Fourth Amendment protection against government searches, since these devices often contain more sensitive information than even “the most exhaustive search of a house” would reveal. Yet increasingly, the vast troves of personal data they contain are synched to “the cloud,” where the outdated Electronic Communications Privacy Act of 1986 allows many types of information to be accessed without a warrant. The need to bring the law up to date has been recognized not only by privacy advocates, but major technology companies, more than half of the House of Representatives, and even federal law enforcement officials. This discussion will tackle the questions of how and why to drag federal privacy law into the 21st century, with keynote remarks by Rep. Ted Poe (R-TX) and a panel discussion featuring both policy experts and representatives of the tech firms we increasingly entrust with our most private data. The event also will be Webcast. CATO Institute, 1000 Massachusetts Ave. NW. More information.

-July 10, 4:15 p.m. EST – **The Internet of Things Privacy Summit Live Stream,** CSPRI Director Lance Hoffman gives a keynote address at the Internet of Things Privacy Summit in Silicon Valley. Please note that this stream will occur on Eastern Time. Register to receive livestream coverage here.

-July 12, 1:00 p.m. - 6:00 p.m., **IPv6 Hacking & Tracking** - Women's Society of Cyberjutsu will host a workshop dedicated to the exploration of IPv6! It will consist of several varying levels of difficulty, all of which build upon the next. You will learn the basic of IPv6, setup your system(s) to use IPv6, as well as route traffic to and from systems using the protocol. Using a combination of Wireshark and Kali you will perform malicious actions against the IPv6 protocol and enabled v6 systems and analyze the traffic. You will see old attacks become new again using the protocol by using man in the middle attacks, packet fragmentation, address collection, DDOS/Floods, fake host and more! Teqcorner, 1616 Anderson Rd., McLean, VA 22102. More information.

-July 15, 6:30 p.m., **Social Media and the Insider Threat -** With the onslaught of new social media platforms and the handheld devices used by people to gain access to apps, the web, and social media, insider threat may need a new perspective. The presentation will conclude with some recommendations on how to better understand the contemporary insider threat and discuss technologies and solutions that can address the mitigation of risk. More information.

-July 17, 12 p.m., **Reflections on Decades of Defending Imperfect Software -** Crispin Cowan addresses this topic in NSF's WATCH Seminar Series. "Perfect" (bug-free) software is impractically expensive and slow to produce, and so the vast bulk of consumer and enterprise software products are shipped when they are "good enough" but far from bug-free. As a consequence, there has been a constant struggle to keep attackers from exploiting these chronically inevitable bugs. Much of that attention has been on memory corruption attacks against type-unsafe C/C++ programs, but in recent years has expanded to the web, where most development is done in dynamically typed scripting languages. This talk will review the evolution of increasingly sophisticated memory corruption defenses followed by attackers discovering how to bypass them, and how the mitigations have caused attackers to choose to exploit other, non-memory-corruption threats, and some surprising similarities between the memory corruption issue and the scripting issues. More Information.

Legislative Lowdown

-The San Francisco Chronicle carries a story about efforts to beef up the funding and the reach of the National Cybersecurity and Communications Integration Center (NCCIC), a 5-year-old institution that monitors threats to government networks. The Chronicle writes that federal lawmakers are fast-tracking a measure that would legally protect companies that tell the center and each other about malicious activities on their networks. “The legislation is designed to address industry executives' concerns that disclosing these vulnerabilities could expose them to lawsuits or regulators' scrutiny, or that certain communications with competitors could invite antitrust actions. The House has passed the measure and a Senate committee plans to take it up this month. The bill's chief sponsors say they believe they have the momentum to get it onto President Obama's desk this year.”

Cyber Security Policy News

-The U.S. trade representative told reporters last week he doesn’t expect cyber-spying to overshadow talks when top officials from Washington and China meet next week. As Reuters reports, Beijing and Washington have traded charges of massive cyber-spying. “Many analysts have suggested these frictions could hamper progress on coordinating economic policy between the world's two largest economies. ‘It's going to be very hard to keep the (talks) insulated from that,’ said Adam Posen, who heads the Peterson Institute, a leading U.S. think tank on international economics. U.S. Treasury Secretary Jack Lew, however, noted that the talks are organized to prevent such contamination. Officials will hold parallel discussions on dozens of issues, he said. This compartmentalized process has helped keep past meetings productive even during public spats.”

- The Privacy and Civil Liberties Oversight Board for the most part supports the NSA's Internet surveillance program in its new report, meaning the independent watchdog agency believes The National Security Agency's Internet surveillance programs are legal and effective. The National Journal’s Brendan Sasso writes that the panel “expresses concern with certain elements of the NSA's massive collection of Internet data within the United States, and outlines several reforms it says would bolster privacy protections and improve transparency.” “But the report, …, is sure to disappoint privacy advocates, who had hoped the board would make a broad call for reform in its review of spying under Section 702 of the Foreign Intelligence Surveillance Act.”

-A prominent privacy organization has sued the National Security Agency (NSA) in a bid to determine the extent to which the agency relies on “zero-days,” security vulnerabilities in software and hardware that are unknown even to the makers of those products. PC World writes that the Electronic Frontier Foundation has filed a lawsuit against the NSA and the Office of the Director of National Intelligence "to gain access to documents showing how intelligence agencies choose whether to disclosure security flaws known as 'zero days.' These early stage flaws are typically discovered by researchers but are not yet patched by developers or the vendor. A market has even sprung up around the flaws, in which governments will purchase the vulnerabilities to gain access to peoples' computers, the EFF said."

-If you've used Tor, a software technology that enhances online privacy by routing one's communications through a network of encrypted hops around the globe, there's a decent chance that the NSA has identified you as worthy of special scrutiny, Wired reports. "This is according to code, obtained and analyzed by journalists and others in Germany, which for the first time reveals the extent of some of the wide-spread tracking the NSA conducts on people using or interested in using privatizing tools and services—a list that includes journalists and their sources, human rights activists, political dissidents living under oppressive countries and many others who have various reasons for needing to shield their identity and their online activity," Wired's Kim Zetter reports. She states that "The source code, for the NSA system known as XKeyscore, is used in the collection and analysis of internet traffic, and reveals that simply searching the web for privacy tools online is enough to get the NSA to label you an "extremist" and target your IP address for inclusion in its database."

-A story last month by CNBC about a sophisticated hacking campaign that targeted a hedge fund turns out to have never actually happened. In late June, CNBC reported that a company called BAE Systems Applied Intelligence said it had identified the attack, but declined to name the hedge fund involved. CNBC now says the BAE Systems subsequently admitted that the attack never happened, and that its expert who was quoted on camera saying that it did was confused and that the incident was part of a "scenario" that BAE had laid out.

-Federal and state courts allowed more than 3,500 wiretaps in 2013, the highest number in recent years, according to The Hill. "Federal judges authorized 1,476 wiretaps, and state judges authorized 2,100 last year — up 9 percent and 3 percent, respectively, from 2012," The Hill writes about the Wiretap Report, released last week. The report notes that the vast majority of wiretap orders – 97 percent – were for "portable devices," such as mobile phones.

-The U.S. Postal Service may one day soon accept Bitcoins for payment, according to NextGov. "The hard-up U.S. Postal Service is asking citizens whether they would ship more items if novel payment technologies were accepted, as virtual currencies and smartphone transactions gain in popularity," writes Aliya Sternstein. "The USPS inspector general website invites customers to post comments about 'innovative payment methods' that would entice them to use agency retail counters. The poll is part of an ongoing audit." The results of the audit aren't expected until September at the earliest.

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.