GW CSPRI Newsletter

August 12, 2013

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

-Aug. 12, 9:00 a.m. - 5:15 p.m., **2013 USENIX Workshop on Health Information Technologies (HealthTech '13**) - Previously known as HealthSec, the USENIX Workshop on Health Security and Privacy, is broadening its scope to encourage the development of new technologies that generally improve the quality and safety of healthcare, as well as the access to it. By bringing together researchers, practitioners, and industrial partners, HealthTech aims to provide a forum for cross-disciplinary interactions among the technology, medicine, and policy communities. Hyatt Regency Washington on Capitol Hill, 400 New Jersey Avenue, NW. More information.

-Aug. 12, 9:00 a.m. - 5:30 p.m., **6th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '13) -** The program includes presentations on economics and business, botnet analysis and evolution, modern DDOS and threats, and the general untrustworthiness of the Web. It also features a work-in-progress session and the following invited talks: "Bitcoin in Cybercrime," by Stefan Savage, University of California, San Diego; "Testing, Testing, 1 2 3: The History and Challenges of Testing Anti-Malware Software," by Mark Kennedy, Anti-Malware Testing Standards Organization (AMTSO) and Symantec

Corporation; and "Stepping P3wn3: Adventures in Full-Spectrum Embedded Exploitation and Defense Configure," by Ang Cui, Red Balloon Security and Columbia University. Hyatt Regency Washington on Capitol Hill, 400 New Jersey Avenue, NW. More information.

-Aug. 13, 9:00 a.m. - 4:45 p.m., **The 2013 USENIX Summit on Hot Topics in Security (HotSec '13)** - Held in conjunction with the 22nd USENIX Security Symposium, HotSec aims to bring together researchers across computer security disciplines to discuss the state of the art, with emphasis on future directions. Speakers and their topics include Joseph Bonneau, Google, on the death of passwords; Jeremy Clark, Concordia University, on eroding trust and the CA debacle; Dan Wallach, Rice University, on balancing academic freedom and responsibility in security research; David Wagner, University of California, Berkeley, on security and privacy for wearable computing. Hyatt Regency Washington on Capitol Hill, 400 New Jersey Avenue, NW. More information.

-Aug. 13, 9:00 a.m. - 5:45 p.m., **7th USENIX Workshop on Offensive Technologies (WOOT '13)** - Progress in the field of computer security is driven by a symbiotic relationship between our understandings of attack and of defense. WOOT '13 brings together researchers and practitioners in systems security to present research advancing the understanding of attacks on operating systems, networks, and applications. The program includes sessions on network attacks, mobile attacks, and low-level attacks. Hyatt Regency Washington on Capitol Hill, 400 New Jersey Avenue, NW. More information.

-Aug. 13, 9:00 a.m. - 5:30 p.m., **3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI '13)** - A subset of the USENIX Symposium, this workshop brings together researchers and practitioners from technology, law, and policy who are working on means to study, detect, or circumvent practices that inhibit free and open communications on the Internet. The day-long program includes a Rump Session, as well as 9 refereed paper presentations on state-level censorship, detection and circumvention, and anonymity and evasion. Hyatt Regency Washington on Capitol Hill, 400 New Jersey Avenue, NW. More information.

-Aug. 14-16, **22nd USENIX Security Symposium** - This conference brings together researchers, practitioners, system administrators, system programmers, and others interested in the latest advances in the security of computer systems and networks. Key speakers include Edward W. Felten, director, Center for Information Technology Policy, and Professor of Computer science and Public Affairs, Princeton University and Andy Ozment, Senior Director for Cybersecurity, White House. Hyatt Regency Washington on Capitol Hill, 400 New Jersey Avenue, NW. More information.

-Aug. 14, 6:00 p.m. - 9:00 p.m., **NovaInfosec Meetup East** - A casual meetup of infosec professionals in the Northern Virginia area. Velocity Five, 8111 Lee Highway, Falls Church, VA, 22042. More information.

-Aug. 16, 1:00 p.m. - 2:30 p.m., **Encryption Made Simple for Lawyers** - The American Bar Association will host a Webcast and teleconferenced panel discussion. The speakers will be John

Simek, vice president, Sensei Enterprises; and David Ries, member, Clark Hill Thorp Reed. More information.

-Aug. 21, 7:30 a.m. - 9:30 a.m., **Leveraging Defense Community Resources for the Next Generation of Threats** - The Defense Industrial Base comprises more than 100,000 companies and subcontractors who work alongside DoD to secure critical systems against intrusions. But with slashed defense budgets, federal and corporate plans for protecting the U.S. cyber infrastructure are subject to serious alterations. NextGov's Aliya Sternstein and Scott Bousum, senior manager of national security policy at TechAmerica will discuss what cyber vulnerabilities are taking priority on the Defense Industrial Base's agenda, how the Department of Defense best leverages public-private partnerships to fend off the most critical threats, and which sectors of the Defense Industrial Base are most heavily affected by budget cuts. Ronald Reagan Building, 1300 Pennsylvania Ave NW, Rotunda. More information.

-Aug. 21, 8:00 a.m. - 5:00 p.m., **Human Cyber Forensics Forum** - This conference addresses the human element of cyber forensics. Presentation will look at the tradecraft and efforts required to identify, understand, navigate, and possibly influence human behavior within and across networks. The forum brings together subject matter experts to discover and share new means of recognizing human related cyber indicators, and the evolution of these human indicators in the coming decades. L'Enfant Plaza Hotel, 480 L'Enfant Plaza, SW More information.

Announcements

The Cyber Statecraft Initiative is looking for a Fall Intern to join the team to focus on international cooperation, competition, and conflict in cyberspace. Interns with the Cyber Statecraft Initiative work closely with Jason Healey, Jason Thelen, and the impressive list of Atlantic Council Senior Fellows. Although the position is unpaid, interns gain valuable experience in conference planning and event management, and have the opportunity to make key contacts with both government and private sector cybersecurity experts. Interns are exposed to the inner-workings of non-profit research institutions and are encouraged to pursue their own research projects and to write and publish their own policy briefs or blog posts. More information.

Legislative Lowdown

The House and Senate are in August recess.

Cyber Security Policy News

-The Obama administration and its supporters spent much of last week defending the government's broad domestic surveillance activities. President Barack Obama on Friday announced plans to overhaul key parts the National Security Agency's surveillance programs, The Wall Street Journal reports. The proposal — which comes in the wake of this year's revelations from fugitive NSA leaker Edward Snowden — drew sharp responses from Republican lawmakers who suggested the president was retreating under political pressure. The tone of the reaction from Republicans and skeptical Democrats suggested Mr. Obama has a new fight on his hands, reminiscent of the two-year battle that preceded reforms of the surveillance law in 2008, during the George W. Bush administration. The Journal notes that the most significant proposal would restructure the Foreign Intelligence Surveillance Court, the secret court that oversees surveillance programs in the U.S., to provide for an advocate for privacy concerns. Mr. Obama is also seeking unspecified reforms to the Patriot Act to increase oversight and place more constraints on the provision that permits government seizure of business records.

The president's call for more oversight and transparency in the National Security Agency’s surveillance programs shows that he wants to make Americans "more comfortable" with the agency’s operations, former NSA director Michael Hayden said.

Meanwhile, the Justice Department last Friday released its legal rationale for why all U.S. phone calls are "relevant" to terrorism investigations. The Hill reports that the administration released the memo as part of President Obama's push to enhance public confidence in the National Security Agency's controversial surveillance programs. Section 215 of the Patriot Act allows the government to collect business records if they are "relevant" to a terrorism investigation. The NSA has acknowledged that it has been using the provision to force phone companies to turn over records on all U.S. phone calls.

The Hill also writes that Senate Intelligence Chairman Dianne Feinstein (D-Calif.) last week said the Intelligence Committee will hold a series of hearings in the fall to examine National Security Agency surveillance programs. Feinstein, who has defended the legitimacy of the NSA surveillance programs, said she hoped the hearings will better explain the scope of the programs and their purpose, as well as "increase the public's confidence in their effectiveness."

-In an outgoing speech as director of the FBI, Robert Mueller called the NSA and CIA essential in finding and deterring malicious "individuals behind keyboards." Ars Technica writes that Mueller stressed the need to continue to develop the technical skills and tools to prevent cyber intrusions and limit their damage. To do that, Mueller said, "we absolutely need the considerable skills of Keith (Alexander)'s experts at NSA. But we also need the human intelligence capabilities of John’ (Brennan)'s team at the CIA. I do believe that in the future, the cyber threat will equal or even eclipse the terrorist threat. And just as partnerships have enabled us to address the terrorist threat, partnerships will enable us to address the cyber threat. But the array of partners critical to defeating the cyber threat is different. In this case, the private sector is the essential partner." The Senate has confirmed as Mueller's successor James B. Comey, deputy attorney general in the George W. Bush administration.

The revelations about NSA interest in those using encrypted email services have spooked two different encrypted email services into closing their doors forever, The Guardian writes. Lavabit, which is believed to have been used by Snowden and which claimed to have 350,000 customers, closed after apparently rejecting a US government court order to cooperate in surveillance on its customers by allowing some form of access to the encrypted messages on its servers. Its founder

Ladar Levison wrote on the company's website: "I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit." Silent Circle, another American company which had offered encrypted email – where messages stored on its server would be unreadable – also announced last week that it was ending its "Silent Mail" service, "to prevent spying".

-The Washington Post highlights a White House blueprint for incentivizing businesses to comply with heightened cybersecurity standards, the crux of President Obama's "cybersecurity framework" for better protecting cyber and physical national assets. "U.S. Cybersecurity coordinator Michael Daniel lists eight possible ways to encourage businesses to voluntarily adopt cybersecurity standards," The Post writes. "These include collaborating with the insurance industry to provide cybersecurity insurance, offering federal grants, expediting government services to participants, and providing legal privileges such as liability limitation. It also suggests streamlining existing legal regulations to make it easier for participants to comply with new standards, publicly recognizing participants, allowing businesses to recover some of their cybersecurity investments, and emphasizing cybersecurity research to help participants find solutions to their specific cyber problems."

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.