GW CSPRI Newsletter

August 11, 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

-Aug. 11-12, **Cyber-Physical Systems Public Working Group Workshop** - This workshop is the first face-to-face meeting of the new NIST Cyber-Physical Systems Public Working Group (CPS PWG). CPS are smart systems, in which essential properties and functionalities emerge from the networked interaction of cyber technologies—both hardware and software— co-engineered with physical systems. For example, CPS can 1) sense the current state of the system and the surrounding real world environment, and 2) respond to provide optimal performance. CPS will have a revolutionary and pervasive impact in multiple domains. Green Auditorium, Administration Building (101), 100 Bureau Drive, Gaithersburg, Md. More information.

-Aug. 13, 2:00 p.m. - 3:00 p.m., **National Security Telecommunications Advisory Committee Teleconference** -- The NTSAC will discuss cyber security. More information.

-Aug. 14, 8:15 a.m. – 4:45 p.m., **Washington D.C. Tech-Security Strategies Conference** -Washington Plaza Hotel, 10 Thomas Circle NW. More information.

-Aug. 20, 1:00 p.m. – 2:30 p.m., **NIST Cybersecurity Framework: Lessons Learned at the Six-Month Mark** - Join ISC-ISAC and DCT Associates for an important webinar that reviews the crucial lessons learned about the benefits and challenges of implementing the framework and how the framework continues to evolve. Hear from government officials, industry experts and top technologists the best methods for ensuring that the framework can help your organization improve your cybersecurity practices and minimize threats. More information.

Legislative Lowdown

-The House and Senate are away for August recess.

Cyber Security Policy News

-A U.S. contractor that conducts background checks for the Department of Homeland Security was hit by a major computer breach that likely resulted in the theft of employee's personal information, The Washington Post reported last week. Ellen Nakashima writes that the hacked company – USIS -- said in a statement that the intrusion has all the markings of a state-sponsored attack. "The breach, discovered recently, prompted DHS to suspend all work with USIS as the FBI launches an investigation. It is unclear how many employees were affected, but officials said they believe the breach did not affect employees outside the department. Still, the Office of Personnel Management has also suspended work with the company "out of an abundance of caution," the Post quotes a senior administration official.

-Last week's back-to-back security conventions Black Hat and Defcon saw the release of new hacks, vulnerabilities and security research. Ruben Santamarta, a consultant with IOactive Labs, described how he figured out how to hack the satellite communications equipment on passenger jets through their WiFi and inflight entertainment systems.

Billy Rios, director of vulnerability research at Qualys, described for conference attendees how he discovered backdoors in a broad range of equipment used by the Transportation Security Administration (TSA), including x-ray machines, trace detection scanners, as well as time and attendance clocks. Speaking at Black Hat, Rios said that technician accounts and their passwords can provide a potential way for would-be attackers to gain access and control over the equipment. "These 'backdoors' are often hardwired into the software," Teri Robinson wrote for SC Magazine. "And the passwords that access these accounts cannot be changed without disrupting the applications, business processes, external software and training programs that depend on them."

The New York Times carried a story about consultant Alex Holden's research, which he said was based on some 1.2 billion unique usernames and passwords that a Russian gang had allegedly stolen and trading. "The records, discovered by Hold Security, a firm in Milwaukee, include confidential material gathered from 420,000 websites, including

household names, and small Internet sites. Hold Security has a history of uncovering significant hacks, including the theft last year of tens of millions of records from Adobe Systems," wrote The Times' Nicole Perlroth. "Hold Security would not name the victims, citing nondisclosure agreements and a reluctance to name companies whose sites remained vulnerable. At the request of The New York Times, a security expert not affiliated with Hold Security analyzed the database of stolen credentials and confirmed it was authentic. Another computer crime expert who had reviewed the data, but was not allowed to discuss it publicly, said some big companies were aware that their records were among the stolen information."

Not everyone at the Vegas security conferences was pleased with Holden's research, charging that his refusal to name victims or offer more specifics amounted to scare tactics designed to sell fear.

But as veteran tech journalist Brian Krebs reported in a Q&A on Holden's disclosure, 1.2B stolen credentials is not out of the ordinary these days. "full-time. These actors — mostly spammers and malware purveyors (usually both) — focus on acquiring as many email addresses and account credentials as they can," Krebs writes. "Their favorite methods of gathering this information include SQL injection (exploiting weaknesses in Web sites that can be used to force the site to cough up user data) and abusing stolen credentials to steal even more credentials from victim organizations."

For its part, the Federal Trade Commission is urging consumers to take precautions, such as changing passwords regularly and avoiding the re-use of email account passwords at other sites.

-A company that makes and sells computer spyware for governments was apparently hacked recently, and 40 GB of its data unceremoniously dumped on the Internet, reports ZDNet. The slick and highly secret surveillance software can remotely control any computer it infects, copy files, intercept Skype calls, log keystrokes -- and now we know it can do much, much more," Violet Blue writes. "A hacker has announced on Reddit and Twitter that they'd hacked Anglo-German company Gamma International UK Ltd., makers of FinFisher spyware sold exclusively to governments and police agencies."

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.