GW CSPRI Newsletter

July 21, 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

-July 21, 4:00 p.m. – 5:30 p.m., **Living With Cyber Insecurity: Reducing the National Security Risks of America's Cyber Dependencies** – This event will feature a panel discussion of proposals for U.S. government responses to cyber insecurity by the Honorable Richard Danzig and the rollout of a major new report from the Center for New American Security: "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies." Abelson/Haskins Conference Room, American Association for the Advancement of Science, 1200 New York Avenue NW. More information.

-July 21, 5:30 p.m. – 8:00 p.m., **NoVA Hackers Association Meetup** – SRA International, 4350 Fair Lakes Court, Fairfax, VA, 22033. More information.

-July 31, 7:00 p.m. – 10:00 p.m., **CharmSec Meetup** – Heavy Seas Alehouse, 1300 Bank Street, Baltimore, MD, 21231. An informal, all-ages, citysec-style meetup of information security professionals in Baltimore. 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.

Legislative Lowdown

- A new surveillance bill just became law in the United Kingdom, only a week after it was introduced in the British parliament. As Gov Info Security reports, the controversial U.K. "emergency" surveillance bill is already drawing promises of a court challenge by privacy rights groups. “The Data Retention and Investigatory Powers Bill was first introduced to Parliament by the British government on July 10. The House of Commons fast-tracked the bill July 15, moving it to the House of Lords. On July 17, the Lords agreed to not add any amendments - which would have returned the bill to the Commons for further debate - and approved the bill without a vote.”

Cyber Security Policy News

-A story last week by Business Week details how the FBI tracked cybercrooks who broke into the NASDAQ stock exchange and gained direct access to the organization’s central servers. According to Bloomberg, multiple intelligence agencies got involved in the investigation, but came up with inconclusive findings. “Intelligence and law enforcement agencies, under pressure to decipher a complex hack, struggled to provide an even moderately clear picture to policymakers. After months of work, there were still basic disagreements in different parts of government over who was behind the incident and why,” Bloomberg’s Michael Riley reports. “While the hack was successfully disrupted, it revealed how vulnerable financial exchanges—as well as banks, chemical refineries, water plants, and electric utilities—are to digital assault.”

-A new team at search giant Google is setting out to make the world safer against attacks on unknown security flaws in widely-used software, the company announced last week. According to CNN, “Google Project Zero” comprises some of the world's smartest, well-intentioned hackers. “They spend their days poking at holes in computer code we all rely on -- and making sure those holes get patched. The Project Zero name comes from the very types of bugs they're trying to eliminate: ‘zero day’ vulnerabilities, which are never-before-seen software flaws that hackers love to exploit,” CNN reported last week. “When Google researchers discover flaws in another company's software, they'll quietly alert that firm. If nothing gets done soon, they'll go public with it on their blog.” More on the team from Google’s blog.

-The U.S. Secret Service last week warned hotels and others in the hospitality industry to be on guard against keystroke-logging devices installed on computers made available to guests in hotel business centers. As KrebsOnSecurity.com reports, the advisory warned that a task force in Texas recently arrested suspects who have compromised computers within several major hotel business centers in the Dallas/Fort Worth areas. “In some cases, the suspects used stolen credit cards to register as guests of the hotels; the actors would then access publicly available computers in the hotel business center, log into their Gmail accounts and execute malicious key logging software, the advisory reads.”

Some are growing so concerned about unknown spies or thieves reading everything they type that the idea of reverting to old-fashioned typewriters is regaining some appeal. As Ars Technica reports, Patrick Sensburg, the chairman of the German parliament's National Security Agency investigative committee, now says he's considering expanding the use of manual typewriters to carry out his group's work. "In an appearance Monday morning on German public television, Sensburg said that the committee is taking its operational security very seriously. "In fact, we already have [a typewriter], and it's even a non-electronic typewriter," he said. As Ars notes, the country would be taking a page out of the Russian playbook. "Last year, the agency in charge of securing communications from the Kremlin announced that it wanted to spend 486,000 rubles (about $14,800) to buy 20 electric typewriters as a way to avoid digital leaks."

-Despite making progress on cybersecurity, most federal agencies fell short of their targets for 2014, according to newly released cross-agency priority goals released on Performance.gov. The Obama administration is pushing chief information officers to focus on priorities of continuous monitoring, phishing and malware, and authorization processes for 2015, reports Federal News Radio. "The administration continues encouraging agencies to implement information security continuous monitoring mitigation (ISCM), which continually evaluates agency cybersecurity processes and practices, according to the report. This goal carries over from last year, where agencies saw an increase in real-time awareness that enabled them to manage risks more effectively. Despite this improvement, the administration wants more cybersecurity evaluation."

Case in point: the Federal Deposit Insurance Corporation (FDIC), the federal entity that enforces banking laws and regulates financial institutions across the country, suffers from weaknesses in its security posture that place information assets at unnecessary risk, according to a new report from the Government Accountability Office (GAO). "The GAO report posits that while FDIC has 'made progress in securing key financial systems' following a series of GAO audits dating back to 2011, its failure to implement specific recommendations by the watchdog agency has led to vulnerabilities in the 'confidentiality, integrity and availability of financial systems and information,'" writes NextGov. "Specifically, GAO contends FDIC did not implement controls for identifying and authenticating users or restrict access to sensitive data or systems. In addition, FDIC did not encrypt sensitive data, complete background investigations for employees, or audit system access."

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.