GW CSPRI Newsletter

August 4, 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. 5, 12 noon – 1:00 p.m., **Managing Liabilities from Cyber Threats Using the Safety Act** – The law firm Venable will host a Webcast panel discussion. More information.

-Aug. 7, 1:00 p.m., **The Business Shock of a Data Breach Incident: Who Are You Going to Call?** – U.S. Telecom will host a Webcast program. The speaker will be Craig Spiezel of the Online Trust Alliance. More information.

-Aug. 8, 12 noon, **Can Europe Force Search Engines to Censor Information You're Looking for on the Internet? Assessing the Right to be Forgotten** -The Internet Caucus will host a panel discussion. Rayburn House Office Bldg., Room 2226. More information.

-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. 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

-The House of Representatives last week passed a measure that requires the Department of Homeland Security to develop a strategy for protecting the nation's infrastructure from a terrorist attack, according to The Hill. "Passed by voice vote, the measure would require DHS to craft a strategic plan for research and development on protecting critical infrastructure from cyber or other attacks."

Several U.S. senators are advocating legislation that would call for better safeguard students' privacy by placing new limits on schools and companies that share personal information, The Hill's Julian Hattem writes. "The bill introduced on Wednesday would require companies that hold students' data to protect it with a set of security standards and forbid them from using identifiable information like students' names or Social Security numbers for advertising. The bill also would give parents the ability to review and correct their kids' personal information and allow them to know how the records are being used."

-Another bill approved by the House last week would require new federal Web sites that collect Social Security numbers, dates of birth and credit card numbers to receive approval from agency chief information officers (CIOs) before going live, NextGov reports.

Cyber Security Policy News

- The director of the Central Intelligence Agency last week apologized to the Senate Intelligence Committee for spying on computers used by the committee's staffers who were preparing an investigation into the CIA's post-9/11 interrogation and detention programs, CNN reports. "The episode was the subject of an unusual, public dispute between the panel and the spy agency over access to classified information," CNN observed. "The CIA had accused the committee staffers of getting access to internal agency documents and of improperly handling classified material."

-A new staff report issued by the Federal Trade Commission finds that many mobile apps for use in shopping do not provide consumers with important information – such as how the apps manage payment-related disputes or handle consumer data – prior to download. The report (PDF) surveyed a total of 121 different shopping apps across the Google Play and Apple App Stores. The survey included 47 price comparison apps, which let consumers compare prices on a particular item in real-time; 50 “deal” apps, which provide consumers with coupons or discounts; and 45 in-store purchase apps, which enable consumers to use their phones to pay for goods they purchase in physical stores.

The FTC is a consumer watchdog agency, but some companies are challenging its authority to enforce data security standards. The Third Circuit Court of Appeals agreed last week to hear an appeal from Wyndham Worldwide Hotels over whether the FTC has that authority. “The appeal throws back into question the agency's authority over data breaches — and could upend consumers’ primary champion against companies with lax security practices,” Politico reports. “A federal judge in New York ruled earlier this year that the FTC does have jurisdiction. While those sorts of decisions aren't usually immediately appealable, the judge in that case said earlier this month the Third Circuit could review the decision.”

- A U.S. federal judge has upheld a warrant requiring Microsoft to give the Justice Department copies of e-mails being stored at a data center in Dublin. Experts say the decision could set up a dramatic collision with foreign data protection and privacy laws. “Microsoft has contested the subpoena since receiving it in December 2013. In April, U.S. Magistrate Judge James Francis rejected Microsoft's initial move to have the subpoena quashed, ruling that the company must comply with valid U.S. government warrants, even for information stored overseas,” Matthew J. Schwartz writes for GovInfoSecurity. Otherwise, he said, ‘the burden on the government would be substantial, and law enforcement efforts would be seriously impeded.’ The European Commission, meanwhile, has said it expects any company that does business inside Europe and works with Europeans' data to comply with EU privacy and data protection laws.”

-Wired.com carries a preview of one piece of research set to be released at this week’s Black Hat security convention in Las Vegas, Nevada: a vulnerability discovered in USB data storage drives that could be used to fundamentally undermine the security of the devices. “That’s the takeaway from findings security researchers Karsten Nohl and Jakob Lell plan to present next week, demonstrating a collection of proof-of-concept malicious software that highlights how the security of USB devices has long been fundamentally broken. The malware they created, called BadUSB, can be installed on a USB device to completely take over a PC, invisibly alter files installed from the memory stick, or even redirect the user’s internet traffic.” Read more here.

-The National Science Foundation's (NSF) Secure and Trustworthy Cyberspace (SaTC) program last week announced two new "Frontier" awards to support large, multi-institution projects that address grand challenges in cybersecurity science and engineering with the potential for broad economic and scientific impact. “The Frontier awards are part a diverse $74.5 million portfolio of more than 225 new projects in 39 states,” NIST explained. “These cybersecurity research and education projects are aimed at minimizing the misuses of cyber-technology, bolstering education and training in cybersecurity, establishing the science of security, and transitioning promising cybersecurity research into practice.”

In other tech-agency news, the National Institute of Standards and Technology is updating its guidance that helps organizations assess their IT systems to determine which security and privacy controls to adopt, GovInfoSecurity reports. “Just before midnight on Aug. 1, NIST issued a draft of SP 800-53A Revision 4, ‘Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. ‘The draft furnishes a set of procedures to conduct assessments of security and privacy controls used by U.S. federal government information systems and organizations. But NIST guidance is often adopted by other governments and businesses worldwide.”

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.