GW CSPRI Newsletter

April 16, 2012

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 1

Announcements 2

Legislative Lowdown 3

Cyber Security Policy News 3

GW Events

-Apr. 18, 12:00 noon – 2 p.m., **Legal and Technical Implications of Recent and Future Data Breaches**. *See Events below for more information.*

-Last week's Frank Howard Distinguished Lecture by Prof. Eugene Spafford of Purdue University on "Why Fixing Cybersecurity is So Difficult" is now available at http://www.seas.gwu.edu/seasmisc/fhl.html.

Events

-Apr. 16, 1:00 p.m. - 2:00 p.m., **Asia Pacific Economic Cooperation: Cross Border Privacy Rules Introduction and Spotlight on Canada** - Speakers will include Daniele Chatelois, Canadian government's Industry Canada; and Josh Harris, senior policy analyst of the U.S. Department of Commerce's Office of Technology and Electronic Commerce. Fulbright & Jaworski, 801 Pennsylvania Ave., NW. More information (PDF).

- Apr. 17, 8:00 a.m. - 10:00 a.m., **Social Networking, the End of Media and Future of Privacy** - Speakers will include FTC Commissioner Julie Brill; Bruce Gottlieb, general counsel of Atlantic Media Company; Sarah Hudgins, director of public policy, Interactive Advertising Bureau; and Jules Polonetsky, director and co-chair, Future of Privacy Forum. Breakfast will be served. This event is open to the public. The price to attend is $47.12. Clyde's of Gallery Place, 707 7th St. NW. More information.

-Apr. 18, 10:00 a.m. **Nominations to the Privacy and Civil Liberties Oversight Board** - The Senate Judiciary Committee will hold a hearing. Witnesses will be the five nominees: James Dempsey, Elisebeth Cook, Rachel Brand, David Medine, and Patricia Wald. This hearing will be Webcast. Room 226, Dirksen Senate Office Building. More information.

-Apr. 18, 12:00 noon – 2 p.m., **Legal and Technical Implications of Recent and Future Data Breaches** – Panelists include Prof. Howard Beales, GW Business School; Prof. Orin Kerr, GW Law School; and Prof. Nan Zhang, GW Computer Science Department (and just-announced winner of the GW Business Plan Competition). Following the event, attendees will have the opportunity to congratulate and engage with GW's 2012 CyberCorps graduates and meet those who will be a part of securing the data of the United States and U.S. industries in the coming years. Lunch included. Visit http://databreaches.eventbrite.com/ to RSVP for this event. More information.

-Apr. 19, 12:00 noon – 1:30 p.m., **Cybersecurity and Smart Infrastructure: Ensuring Resilience and Deterrence** – Moderated by Herb S. Lin, National Research Council. Speakers include Sunil Cherian, Spirae Inc.; Stacy Prowell, Oak Ridge National Laboratory; William Sanders, University of Illinois at Urbana-Champaign; and Marianne Swanson, National Institute of Standards and Technology. Room 2325, Rayburn House Office Building. More information.

-Apr. 19, 2:00 p.m. - 3:00 p.m., **Fresh Prints of Malware** - Mandiant's Doug Wilson and Will Gibb will step through world of OpenIOC, an open framework for sharing threat intelligence. This Webinar is free but requires registration.

Announcements

Upcoming Wednesday Panel Discussion and Launch

Join George Washington University professors in a discussion from noon until 2:00 p.m. on April 18, titled "Legal and Technical Implications of Recent and Future Data Breaches." Recently Master Card and Visa announced a data breach at one of their payment processor companies that compromised 1.5 million credit card numbers and associated information. This announcement launched the payment processing pipeline into the rapidly expanding spotlight of public scrutiny and has prompted discussion about the implications of recent and future data breaches. Will data ever be safe? Is technology, human error, or a combination of both to blame? Experts in the fields of computer

science, law, and business discuss the current data breaches and what can be expected to address these concerns from government, business, and educational perspectives.

Speakers will include Howard Beales, a professor of strategic management and public policy at The George Washington University School of Business; Orin Kerr, professor of law at The George Washington University in Law School; and Nan Zhang, assistant professor in the Computer Science Department at The George Washington University. Visit http://databreaches.eventbrite.com/ to RSVP for this event.

Following the event, attendees will have the opportunity to congratulate and engage with GW's 2012 CyberCorps graduates and meet those who will be a part of securing the data of the United States and U.S. industries in the coming years. As President Obama said on May 29, 2009, "America's economic prosperity in the 21st century will depend on cybersecurity." Read more.

Last Week's Lecture on April 11 by Prof. Eugene Spafford

If you missed last week's Frank Howard Distinguished Lecture by Prof. Eugene Spafford of Purdue University on "Why Fixing Cybersecurity is So Difficult", you have a second chance. Prof. Paul Rosenzweig of the GW Law School, calling it "droll and entertaining", blogs about the lecture at http://www.lawfareblog.com/2012/04/spafford-to-congress-just-say-no/. And the entire video is at http://www.seas.gwu.edu/seasmisc/fhl.html.

Legislative Lowdown

In an attempt to re-create the backlash that killed anti-piracy legislation earlier this year, activists are planning a "week of action" beginning on Monday to protest the Cyber Intelligence Sharing and Protection Act (CISPA), according to The Hill. Many of the groups leading the protest are veterans of the fight against the Stop Online Piracy Act (SOPA) and the Protect Intellectual Property Act (PIPA), including the Electronic Frontier Foundation, the Center for Democracy and Technology, Free Press, Fight for the Future and the American Civil Liberties Union (ACLU).

Meanwhile, hacktivist groups including Anonymous are promising to protest CISPA with additional attacks on supporters; last week, the hacking collective claimed responsibility for knocking down the Web sites of two industry trade groups that support the measure, telephone association USTelecom and technology group TechAmerica.

At the same time, the bill's sponsors are pushing back, saying the measure has little to do with stopping online piracy -- the illegal activity targeted by the original and now-defeated SOPA bill. CISPA, introduced by House Intelligence Committee Chairman Rep. Mike Rogers (R-Mich.) and Maryland Rep. Dutch Ruppersberger, the ranking Democrat on the Intelligence Committee, would allow government authorities to make classified and non-classified data available to the private sector for the purpose of shoring up the

electronic defenses of critical infrastructure. The Hill cited an anonymous congressional staffer familiar with the CISPA bill, who stressed that its requirements are “totally voluntary” and do not require private companies to share information with the military, as some have claimed.

Cyber Security Policy News

-The largest wireless carriers are banding together with regulators and law enforcement officials to launch an effort to make stolen cellphones and other mobile devices as useless as an empty wallet. The goal is to cut down on increasing thefts of smartphones by making them less appealing to criminals. AT&T Inc., Verizon Wireless, T-Mobile USA and Sprint Nextel Corp. said Tuesday they will create a central database to track stolen devices and prevent them from being reactivated.

-The debate over whether we need laws to bar employers from asking potential new hires to share their Facebook passwords is becoming a campaign issue, The Hill writes. Richard Carmona, the presumptive Democratic nominee in the Arizona Senate race, is accusing Republican candidate Rep. Jeff Flake of not protecting users' Facebook passwords. The Carmona campaign has launched a website, WhatsYourPasswordJeff.com, that slams Flake over his vote against a procedural motion in the House that Carmona claims would have helped to bar businesses from demanding that job applicants or employees reveal the passwords to their social networking accounts. Meanwhile, Maryland last week became the first state to ban the increasingly common employer practice.

In other Facebook security and policy news, ZDNet last week published a handy guide detailing the pages and pages of data Facebook typically hands over when authorities send a subpoena to Facebook for your account information. "Facebook already shares its Law Enforcement Guidelines publicly, but we’ve never actually seen the data Menlo Park sends over to the cops when it gets a formal subpoena for your profile information," ZDNet's Emil Protalinski writes. "Now we know."

-A widespread computer virus outbreak at the Department of Commerce's Economic Development Administration (EDA) has prompted the agency to unplug its operating system, bar employees from browsing the Web or using email until further notice, The Washington Post reports. The outage has persisted for 12 weeks, with little end in sight. The EDA gives grants to distressed communities out of six regional offices, with a small Washington presence.

-A series of hacks perpetrated against so-called “smart meter” installations over the past several years may have cost a single U.S. electric utility hundreds of millions of dollars annually, the FBI said in a cyber intelligence bulletin obtained by security blogger Brian Krebs. The law enforcement agency said this is the first known report of criminals compromising the high-tech meters, and that it expects this type of fraud to spread across the country as more utilities deploy smart grid technology.

The smart meter hacking story surfaced the same week that White House cyber czar Howard Schmidt warned that the nation's power utilities must pinpoint security gaps in their electricity delivery systems on a regular basis, NexGov writes. The nation's energy sector must perform "active risk management performance evaluations, continuous monitoring, exercises and simulations to determine on a regular basis how we're doing," Schmidt told industry and government leaders at McAfee's annual public sector conference. The Energy Department, in cooperation with the White House, Homeland Security Department and power companies, this month is expected to test a voluntary reporting model that assesses an individual utility's security posture to identify where safeguards are needed most. As of March 30, the Office of Management and Budget was finalizing information collection procedures for the trial.

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.