GW CSPRI Newsletter

April 14, 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

CSPRI in the News

CSPRI Visiting Scholar, Dr. Allan Friedman, is interviewed on WTOP Radio about the online bug "Heartbleed." **Click here for the audio.**

Events

-Apr. 15, 6:30 p.m. - 8:00 p.m., **ISSA DC Meetup** - The National Capital Chapter of the ISSA is comprised of information security professionals located in the Washington D.C. Metropolitan Area. Members are actively involved in information security in government agencies, the military, non-profit organizations, and in large and small companies. This month's speaker is Dmitri Alperovitch, co-founder and CTO of CrowdStrike /Inc. Center for American Progress, 1333 H. St., NW. More information.

-Apr. 15-16, **Washington DC Information Security Forum** - This event brings together experienced IT and information security practitioners for confidential information sharing on the industry's most important issues, technologies, and trends. The two-day forum includes keynote addresses, technical and strategic roundtable discussions led by IANS' Faculty, networking

events, and the opportunity to learn about new technologies. Washington Convention Center, 801 Mount Vernon Place, NW. More information.

-Apr. 16, 10:00 a.m. - 11:00 a.m., **Edward Snowden's Betrayal** - The American Enterprise Institute will host a discussion. The speakers will include Liam Fox (UK Member of Parliament, and former Minister of Defense), and Marc Thiessen (AEI). This event will be Webcast. AEI, 12th floor, 1150 17th St., NW. More information.

-Apr. 16, 8:30 a.m., **Beyond Data Breaches: Global Interconnections of Cyber Risk** - Featuring remarks by Michael Kerner, CEO general insurance, Zurich Insurance Group; Steve Crocker, board chair, ICANN; Jason Healey, director, Cyber Statecraft Initiative, Brent Scowcroft Center on, International Security, Atlantic Council; and Catherine Mulligan, senior vice president, Zurich North America. This event will be Webcast. 1030 15th Street, NW, 12th Floor (West Tower). More information.

-Apr. 16, 10:00 a.m., **Protecting Your Personal Data: How Law Enforcement Works With the Private Sector to Prevent Cybercrime** - The House Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will hold a field hearing which is expected to be Webcast. More information.

-Apr. 24, 8:30 a.m. - 3:00 p.m., **Cybersecurity: Innovation and Challenges From Mobiles, Automobiles, Internet of Things to Insider Threats** - A day of presentations featuring updates on the latest innovations in cybersecurity, and subsequent challenges, in areas ranging from automobiles and transportation to medical devices and the smart home. As traditionally non-internet enabled products morph into internet-enabled technologies, the need for advanced cybersecurity is increasing rapidly. The speakers and panelists at this event will discuss the impact this is having on the field and what changes are occurring in policy, technology, and leadership initiatives in order to provide this new level of cybersecurity. George Mason University, 4400 University Drive, Fairfax, VA, 22030. More information.

Legislative Lowdown

-In a major policy development, The European Union's top court has declared "invalid" an EU law requiring telecoms firms to store citizens' communications data for up to two years. The BBC reports that the EU Data Retention Directive -- adopted in 2006 -- violates two basic rights - respect for private life and protection of personal data, according to the European Court of Justice. "The 28-nation EU is currently drafting a new data protection law. The ECJ ruling says the 2006 directive allows storage of data on a person's identity, the time of that person's communication, the place from which the communication took place and the frequency of that person's communications." This is further explained by the ruling by the Luxumbourg court: "by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data."

-A House Commerce subcommittee voted last week to halt the Obama administration's plan to relinquish U.S. oversight of the Internet's Web address system, The Hill reports. "Over objections and amendments from Democrats, the subcommittee's 16 Republicans approved the Domain Openness Through Continued Oversight Matters (DOTCOM) Act, which would prevent the Commerce Department from relinquishing its oversight role of the Internet Assigned Numbers Authority (IANA). The bill — authored by Rep. John Shimkus (R-Ill.) — is a response to the Commerce Department's announcement earlier this year that it is beginning a process to have global Internet stakeholders develop a plan to transition the IANA oversight role away from the U.S."

Cyber Security Policy News

-Researchers last seek uncovered an extremely critical vulnerability in recent versions of OpenSSL, a technology that allows millions of Web sites to encrypt communications with visitors. Complicating matters further was the release of a simple exploit that can be used to steal usernames and passwords from vulnerable sites, as well as private keys that sites use to encrypt and decrypt sensitive data. At the time of the exploit's release, the vulnerability was thought to be present in roughy 60 percent of the Web sites on the Internet, and for many hours major Web destinations -- such as Yahoo.com -- remained vulnerable, exposing tens of millions of user accounts.

In a story published late last week, Bloomberg cited two unnamed sources stating that the National Security Agency had known about the bug and had been exploiting it for at least two years. For its part, the NSA denied to multiple media sources that it even knew about the bug before it was made public last week.

While most major Web sites have since fixed the bug – called "Heartbleed", removing the vulnerable components from Internet hardware and other technologies that are more difficult to upgrade is going to present challenges for some time to come, The Wall Street Journal reports. "Cisco Systems Inc. and Juniper Networks Inc., two of the largest manufacturers of network equipment, said Thursday that some of their products contain the Heartbleed bug," the publication reported. The report went on to note, "…hackers might be able to capture usernames, passwords and other sensitive information as they move across corporate networks, home networks and the Internet. […] These devices likely will be more difficult to fix. The process involves more steps and businesses are less likely to check the status of network equipment, security experts said. Bruce Schneier, a cybersecurity researcher and cryptographer, said, 'The upgrade path is going to involve a trash can, a credit card, and a trip to Best Buy.'"

-The Obama administration is once again has taking action on an issue it believes is not moving fast enough through Congress. Last week, two federal agencies clarified that companies can share cybersecurity information to protect consumers from hackers without violating antitrust rules. As US News & World Report writes that, "stricter cybersecurity for businesses has been a priority for the Obama administration, but Congress has been unable to agree on legislation that could set standards for critical infrastructure security. Lawmakers have disagreed on the legal barriers for what information companies can share about their networks to coordinate on threats

from hackers, and have been divided over the privacy rights of customers. To enable more teamwork between companies on cybersecurity, the Department of Justice and the Federal Trade Commission this week issued guidance saying antitrust rules should not hinder the sharing of threat information."

Meanwhile, a report from the Government Accountability Office says that major U.S. federal government agencies for the most part failed to respond effectively to cyber-incidents. "Appearing April 2 before the Senate Homeland Security and Governmental Affairs Committee, GAO's Gregory Wilshusen said a preliminary assessment of a study of the effectiveness of government responses shows that the 24 major agencies did not consistently demonstrate adequate response in about 65 percent of reported incidents," GovInfoSecurity writes. "The number of information security incidents at federal agencies has grown dramatically in recent years, more than doubling from 2009 through 2013, according to a GAO analysis of U.S.-CERT statistics."

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.