GW CSPRI Newsletter

April 7, 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 1

Cyber Security Policy News 2

Events

-Apr. 9, 7:00 a.m. - 12:30 p.m., **2014 GovCon Cyber Summit** - Speakers include Congressman Mike Rogers, Rep. Dutch Ruppersberger, Joe Demarest (FBI), Harvey Rishikof (ABA), Steve Chabinsky (CrowdStrike), Bobbie Stempfley (DHS), Michael Daniel (The White House), Stewart Baker (Steptoe & Johnson LLP), Jim Koenig (Booz Allen Hamilton), and Annejanette Pickens (General Dynamics AIS). McLean Hilton, 7920 Jones Branch Drive, McLean, VA 22102. More information.

-Apr. 9, 7:00 p.m. - 9:00 p.m., **NovaInfosec Meetup** - An informal gathering of information security professionals in Northern Virginia. Velocity Five, 8111 Lee Highway, Falls Church, Va. 22042. More information.

-Apr. 9-10, **NIST Privacy Engineering Workshop** - The National Institute of Standards and Technology will hold a workshop focused on the advancement of privacy engineering as a basis for the development of technical standards and best practices for the protection of individuals' privacy or civil liberties. By examining existing models such as security engineering and safety risk management, the workshop will explore the concepts of a privacy risk management model, privacy requirements and system design and development. 100 Bureau Drive, Gaithersburg, MD, 20899. More information.

-Apr. 10, 9:00 a.m., **Should the Department of Commerce Relinquish Direct Oversight Over ICANN?** - The House Judiciary's Subcommittee on Courts, Intellectual Property, and the Internet will hold a hearing about plans to shift control over the Internet's domain name system from U.S. control to a more international apparatus. Rayburn House Office Bldg., Room 2141. More information.

-Apr. 11, 10:30 a.m., **Bitcoin: The Future of Currency?** - A discussion with Chris Brummer, project director, Transatlantic Finance Initiative and C. Boyden Grey Fellow on Finance and Growth, Global Business and Economics Program, Atlantic Council, and professor of law, Georgetown University; Jason Healey, director, Cyber Statecraft Initiative, Brent Scowcroft Center on International Security, Atlantic Council; Kevin Houk, research and development, Blockchain.info, and bitcoin miner; Ronald Marks, president, Intelligence Enterprises LLC, and senior fellow, Homeland Security Policy Institute, The George Washington University. 1030 15th Street, NW, 12th Floor (West Tower). More information.

-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. The chapter holds regular meetings at various locations throughout the D.C. area. Through its meetings and other events, the chapter fosters professional development and support for computer and information security professionals. Membership is open to practicing security professionals or to those with an interest in the profession. New members are always welcome. 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.

Cyber Security Policy News

-The U.S. Department of Justice is asking for new rules to make it easier for law enforcement to get warrants to hack into the computers of criminal suspects across the country, The Wall Street Journal reports. "The move, which would alter federal court rules governing search warrants, comes amid increases in cases related to computer crimes," Jennifer Valentino-Devries writes. "Investigators say they need more flexibility to get warrants to allow hacking in such cases, especially when multiple computers are involved or the government doesn't know where the suspect's computer is physically located."

Attorneys general in at least two U.S. states are now investigating a data breach last year at a unit of big-three credit monitoring firm Experian, according to Reuters. The news comes following

revelations from security blogger Brian Krebs that a company owned by Experian for nearly 10 months in 2013 sold consumer records to a service marketed in the cybercrime underground as an identity theft bazaar. Experian responded to the flurry of media attention last week with a series of talking points about the incident, and Krebs last week follows up with a fact-check of those points here.

-Google is asking the U.S. Supreme Court to decide the legality of the company's previous practice of "sniffing" unencrypted traffic that flows across WiFi networks encountered by vehicles that map out its StreetView program across the country. Wired.com reports that an appeals court last September found that the sniffing may have violated the Wiretap Act. "The company's fleet of photo-snapping cars is equipped with Wi-Fi hardware to record the names and MAC addresses of nearby routers to improve Google geolocation services," Kevin Poulsen writes. "From 2008-2010, those vehicles were also capturing tiny snippets of internet traffic from countless thousands of routers that weren't employing encryption, turning every Street View vehicle into a rolling spy machine."

-In December, Reuters shook the foundations of the security industry when it reported that RSA, a company whose cryptographic algorithms have become deeply embedded in the public Internet, took $10 million from the National Security Agency in the 1990s in exchange for an agreement to weaken the cryptography of a standard it used in some of its products and technologies. Last week, Reuters reported that RSA adopted not just one but two encryption tools developed by the NSA. From that story: "Reuters reported in December that the NSA had paid RSA $10 million to make a now-discredited cryptography system the default in software used by a wide range of Internet and computer security programs. The system, called Dual Elliptic Curve, was a random number generator, but it had a deliberate flaw - or "back door" - that allowed the NSA to crack the encryption. A group of professors from Johns Hopkins, the University of Wisconsin, the University of Illinois and elsewhere now say they have discovered that a second NSA tool exacerbated the RSA software's vulnerability."

-Congress is again holding hearings this week on plans for the Internet Corporation for Assigned Names and Numbers (ICANN) to hand over control of the domain name system from a U.S. based nonprofit to a consortium of international entities. The Hill reports that "Republicans in the House and Senate wants answers from the Obama administration about whether a recent Commerce Department decision will threaten the open Internet. Through questions — both in a House hearing and Senate letter — Republicans on Wednesday pushed the Commerce Department to justify its decision to step back from its oversight role of the Internet's Web address system."

In fact, some Republican leaders say the plan could pave the way for Russia or China to gain new influence over the management of the Internet. "Make no mistake: Threats to the openness and freedom of the Internet are real," National Journal quotes Republican Rep. Greg Walden, the chairman of the House Energy and Commerce Communications and Technology Subcommittee, which held a hearing on the issue Wednesday. "Leaders such as Vladimir Putin have explicitly announced their desire to gain control of the Internet. Walden and other Republicans are pushing a bill that would block the transfer of authority until the Government Accountability Office can study the issue. Dozens of Senate Republicans, led by John Thune and Marco Rubio, sent a letter

to the administration on Wednesday, demanding more answers about the plan. But Democrats at Wednesday's hearing insisted that if Republicans were serious about Internet freedom, they would support the U.S. proposal. Assistant Secretary of Commerce Larry Strickling said the U.S. will make sure that no foreign government will be able to seize new powers over the Internet."

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.