GW CSPRI Newsletter

March 31, 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

Announcements 1

Events 1

Legislative Lowdown 2

Cyber Security Policy News 3

Announcements

Allan Friedman, visiting CSPRI scholar, discusses cybersecurity and Huawei: See the interview here. (Scroll to the bottom of the page).

Privacy buffs and those worried about its future will appreciate the latest lament set to the music of American Pie -- much higher quality than the usual video posted to YouTube and the singer sounds exactly like Don McLean. See https://www.youtube.com/watch?v=sxfTHHltsWA for a video clip that is extraordinary.

Events

-Apr. 1, 8:15 a.m. - 6:00 p.m., **Big Data, Life Sciences and National Security** - The American Association for the Advancement of Science (AAAS) Center for Science, Technology, and Security Policy (CSTSP) and the Biological Countermeasures Unit of the WMD Directorate of the Federal Bureau of Investigation (FBI) present a public event on the implications of big data and analytics to national and international biological security. Renaissance Washington, DC Downtown Hotel, 999 Ninth Street NW. This event also will be Webcast. More information.

-Apr. 2, 10:30 a.m., **Ensuring the Security, Stability, Resilience, and Freedom of the Global Internet** - The House Energy and Commerce Committee will hold a hearing. The speakers will include Larry Strickling, assistant secretary for communications and information administration, National Telecommunications and Information Administration, U.S. Department of Commerce; David A. Gross, partner, Wiley Rein, LLP; Fadi Chehade, president and CEO, Internet Corporation for Assigned Names and Numbers; Steve DelBianco, executive director, NetChoice; Carolina Rossini, project director, Latin American Resource Center, Internet Governance and Human Rights Program, New American Foundation. Rayburn House Office Bldg., Room 2322. More information.

-Apr. 2, 1:00 p.m., **Bitcoin: Examining the Benefits and Risks for Small Business** - The Committee on Small Business will hold a hearing to examine both the benefits and the risks associated with the Bitcoin as a payment for small businesses. The hearing will be webstreamed live. Rayburn House Office Bldg., Room 2360. More information.

-Apr. 3, 12:30 p.m., **System and Conscience: NSA Bulk Surveillance and the Problem of Freedom** - The Global Internet Freedom and Human Rights Distinguished Speaker Series hosts Yochai Benkler, the Berkman Professor of Entrepreneurial Legal Studies at Harvard Law School, and faculty co-director of the Berkman Center for Internet and Society at Harvard University. Microsoft Innovation & Policy Center, 11th Floor, 901 K Street, NW. More information.

-Apr. 5, 11:00 a.m. – 5:00 p.m., **Wireless Hacking -** In this workshop we will learn to perform the steps used in wireless penetration testing such as cracking the keys and gain access to a variety of increasingly secure wireless access points. From WEP to the trusted WPA2, nothing is safe from attack with the right tools and the right motivation. UberOffices, 1751 Pinnacle Drive, Ste. 600, McLean, VA 22102. 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.

Legislative Lowdown

-Lawmakers in the Senate are reviving legislation aimed at cracking down on mobile application makers that collect location data without permission. The Hill writes that Sen. Al Franken, chair of the Senate Judiciary subcommittee on Privacy, introduced an updated version of his Location Privacy Protection Act, which would require companies to get users' permission before collecting or sharing location information from their smartphones, tablets and in-car navigation systems. "In 2012, the Senate Judiciary Committee passed Franken's original bill. The new bill, which is backed by Sens. Chris Coons (D-Del.) and Elizabeth Warren (D-Mass.), would require

companies collecting location information from more than 1,000 devices to disclose their data collection and sharing practices. It would also ban 'stalker apps,' which are designed to collect and share a user's location information without that user knowing. If enacted, the bill would allow law enforcement officials to seize proceeds from the creation and sale of such apps and redirect the proceeds to anti-stalking organizations."

Cyber Security Policy News

The National Security Agency and a British intelligence service snooped on private German communications companies, according to documents provided by Edward Snowden to German magazine Der Spiegel. The report alleges that the agencies targeted employees of leading German firms in an attempt to learn about the technology behind key satellite Internet service providers. "The document, which is undated, states that the goal of the effort was developing wider knowledge of Internet traffic flowing through Germany," Der Spiegel writes. "The 26-page document explicitly names three of the German companies targeted for surveillance: Stellar, Cetel and IABG."

While the United States has for years insisted that Chinese tech hardware giant Huawei Technologies may contain backdoors that could be used to spy on customers, a new report from The New York Times last week alleges that the NSA broke into servers at China's Huawei Technologies to spy on company communications, gather information about the company's products, and establish backdoors on the systems. "But even as the United States made a public case about the dangers of buying from Huawei, classified documents show that the National Security Agency was creating its own back doors — directly into Huawei's networks," The Times stated. "The agency pried its way into the servers in Huawei's sealed headquarters in Shenzhen, China's industrial heart, according to N.S.A. documents provided by the former contractor Edward J. Snowden. It obtained information about the workings of the giant routers and complex digital switches that Huawei boasts connect a third of the world's population, and monitored communications of the company's top executives."

Meanwhile, longtime NSA chief -- 4-star Gen. Keith Alexander -- stepped down from his post last week. According to The Guardian -- the newspaper that featured by far the most damning coverage so far of the NSA's surveillance activities and NSA whistleblower Edward Snowden -- notes that Alexander pointedly barely referenced Snowden in his departure speech. "Feted at a retirement ceremony attended by intelligence colleagues, legislators, fellow officers and White House chief of staff Denis McDonough, Alexander hailed the NSA by quoting General Douglas MacArthur's musings on patriotism, morality and service from his 1962 retirement speech at West Point, which Alexander called "especially applicable with all that has gone on in the past year," The Guardian wrote. "It was the only reference to Snowden that Alexander permitted himself in a brief speech."

-Federal agents notified more than 3,000 U.S. companies last year that their computer systems had been hacked, White House officials have told industry executives. This marks the first time the government has revealed how often it tipped off the private sector to cyberintrusions, according to The Washington Post. "The alerts went to firms large and small, from local banks to

major defense contractors to national retailers such as Target, which suffered a breach last fall that led to the theft of tens of millions of Americans' credit card and personal data, according to government and industry officials," writes The Post's Ellen Nakashima.

The disclosure came the same week that a Senate committee called out Target Corp. for missteps that some members said contributed to one of the biggest data heists in U.S. history. As the Minnesota Star Tribune writes, "Sen. Richard Blumenthal, D-Conn., told Target's chief financial officer that Target missed 'multiple warnings' that could have enabled it to thwart the breach of financial and personal information for up to 110 million customers. Blumenthal was not the only senator to criticize Target's handling of the breach. Committee Chairman Jay Rockefeller, D-W.Va., said Target 'fell far short' of protecting its customers, based on a report his staff prepared. The report showed missed opportunities for Target to intervene to stop the hacking. Rockefeller expressed concern that several Target executives may have known about suspicious activity in the computer system in November, a month ahead of the actual data theft."

For its part, Uncle Sam won't be accused of underspending on security anytime soon. According to The Associated Press, the Pentagon plans to more than triple its cybersecurity staff in the next few years to defend against Internet attacks that threaten national security. Speaking at the National Security Agency headquarters in suburban Washington, Defense Secretary Chuck Hagel said The Department of Defense is on its way to building an 'elite, modern cyberforce.' "The Pentagon has been recruiting outside talent for the work as well as encouraging people already in the military to train for the jobs," The AP writes. "By 2016, the Pentagon should have 6,000 cyber professionals, Hagel said. That compares to some 1,800 by the end of this year."

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.