GW CSPRI Newsletter

March 24, 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

CSPRI Event: Mar. 26, 6:00 p.m. - 7:00 p.m., **DHS Cyber Forward: Resiliency and Partnership in a Networked World** - Dr. Phyllis Schneck serves as the deputy under secretary for cybersecurity and communications for the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security. GWU Gelman Library, Suite 702. More information.

-Mar. 25, 12:15 p.m. - 1:45 p.m. **Transatlantic Solutions to Government Surveillance** - The New America Foundation will host a panel discussion titled. The speakers will be Konstantin von Notz, member of German Parliament; Jan Philipp Albrecht, member of European Parliament; Malte Spitz, Federal Party Council of the German Green Party; and Kevin Bankston, policy director, New America Foundation. This event will be webcast. NAF, Suite 400, 1899 L St., NW. More information.

-Mar. 25, 8:30 a.m. - 4:30 p.m., **China Defense and Security Conference 2014** - The Jamestown Foundation will hold its Fourth Annual China Defense and Security Conference on March 25 in Washington, D.C. Speakers at the conference will provide an extensive overview of recent developments in military training and operations reform, and take on challenging

questions in Chinese foreign policy, including: the role of cyber-warfare in Chinese strategic thought. Carnegie Endowment for International Peace, Root Conference Room, 1779 Massachusetts Avenue, NW. More information.

-Mar. 26, 10:00 a.m., **Strengthening Public Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure** - The Senate Homeland Security and Governmental Affairs Committee will hold a hearing. The witnesses will be Phyllis A. Schneck, Ph.D., deputy under secretary for cybersecurity, National Protection and Programs Directorate, U.S. Department of Homeland Security; Donna Dodson, chief cybersecurity advisor, National Institute of Standards and Technology, U.S. Department of Commerce; Stephen L. Caldwell, director, Homeland Security and Justice Issues U.S. Government Accountability Office; Elayne Starkey, chief security officer, Delaware Department of Technology and Information; David M. Velazquez, executive vice president for power delivery; Pepco Holdings, Inc.; Doug Johnson, vice chairman, Financial Services Sector Coordinating Council; Steven R. Chabinsky, chief risk officer, CrowdStrike, Inc. Dirksen Senate Office Bldg., Room 342. More information.

-Mar. 26, **SEC Cybersecurity Roundtable** - The Securities and Exchange Commission today announced that it will host a roundtable next month to discuss cybersecurity and the issues and challenges it raises for market participants and public companies, and how they are addressing those concerns. The growing interest in cybersecurity across financial markets and other sectors has raised questions about how various market participants can effectively manage cybersecurity threats. Cybersecurity breaches have focused public attention on how public companies disclose cybersecurity threats and incidents. SEC Headquarters 100 F Street, NE Washington, DC 20549. More information.

-Mar. 26, 2:30 p.m., **Protecting Personal Consumer Information from Cyber Attacks and Data Breaches** - U.S. Senate Committee on Commerce, Science, and Transportation will hold a hearing. Witnesses will be The Honorable Edith Ramirez, chairwoman, Federal Trade Commission; John J. Mulligan, vice president and chief financial officer, Target Corporation; Wallace D. Loh, president, University of Maryland; David Wagner, president, Entrust, Inc.; Peter J. Beshar, executive vice president and general counsel, Marsh & McLennan; Ellen Richey, chief enterprise risk officer, Visa Inc. Russell Senate Office Bldg., Room 253. More information.

-Mar. 28, 10:00 a.m. - 5:00 p.m., **Corporate Counter-Terrorism: The Role of Private Companies in National Security** - The keynote speaker will be John Carlin, assistant attorney general for national security at the Department of Justice. Speakers will include current and senior officials from the Justice Department, National Security Agency, Office of the Director of National Intelligence, FBI, DHS, Google, Microsoft, among others. American University Washington College of Law, 4801 Massachusetts Avenue N.W., Room 603. 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.

Legislative Lowdown

-As the U.S. Senate this week considers a significant Ukrainian aid package, U.S. Sens. Mark Warner (D-Va.) and Mark Kirk (R-Ill.) said last week that they plan to offer an amendment creating a law enforcement partnership between the United States and Ukraine to combat cybercrime and improve cybersecurity. "Ukraine has long been considered an international haven for hackers, and last year's massive data breach affecting millions of U.S. customers of Target and other leading American retailers has been traced to cybercrime syndicates operating in Ukraine," writes The Augusta Free Press. "The Warner/Kirk Amendment would require U.S.-Ukraine bilateral talks on cybercrime cooperation, establish a standing senior-level working group to conduct regular dialogue on cybercrime, explore opportunities to build-up Ukraine's capacity to combat cybercrime in cooperation with American and European law enforcement agencies, and develop improved extradition procedures between the U.S. and Ukraine."

-Credit unions are repeating their calls to Congress to establish federal data security laws. Congress has been talking for more than a decade about enacting national regulations that would standardize disparate state data breach disclosure laws. While the financial industry and business community largely support such harmonization, Congress has failed to act. But according to The Hill, a trade group representing the nation's credit unions is making another attempt. "In a letter on Wednesday to congressional leadership, the National Association of Federal Credit Unions pointed to recent high-profile data breaches, including one at Target that impacted the financial and personal information of tens of millions of consumers," The Hill wrote. "How many more consumers will have to be affected before Congress will act?"' In the letter, the credit union group urged Congress to create federal standards to protect consumers and financial institutions.

Cyber Security Policy News

The National Security Agency has built a surveillance system capable of recording "100 percent" of a foreign country's telephone calls, enabling the agency to rewind and review conversations as long as a month after they take place, The Washington Post reported last week. "A senior manager for the program compares it to a time machine — one that can replay the voices from any call without requiring that a person be identified in advance for surveillance. The voice interception program, called MYSTIC, began in 2009. Its RETRO tool, short for 'retrospective retrieval,' and related projects reached full capacity against the first target nation in 2011. Planning documents two years later anticipated similar operations elsewhere."

-Amid another week of new disclosures from NSA whistleblower Edward Snowden, the U.S. intelligence community's most vocal ally and defender in Congress -- Sen. Dianne Feinstein (D-Calif.) -- now says she is "open to changes" on how spy agencies gather and store phone records on millions of Americans, National Journal reports. "The shift from the powerful chairwoman of the Senate Intelligence Committee arrives a week ahead of a March 28 deadline that President Obama gave his administration to deliver alternatives to him on how the National Security Agency operates one of its most controversial programs, the bulk collection of phone 'metadata.' The intelligence community and the Justice Department have a deadline of next Friday to deliver

their recommendations to Obama on how to implement NSA surveillance reforms that the president outlined during a policy speech in January."

-Uncle Sam doesn't have a monopoly on deploying intrusive spying methods: a number of police departments in California have been using controversial "StingRay"-type of cellular interception devices for at least six years, with little or no disclosure, according to documents obtained by Sacramento's News10. "A StingRay is a device law enforcement uses to track people and collect real time data from every cellphone within a certain radius," News10 reports. According to NBC News, "StingRays belong to a class of device made by Florida-based Harris Corporation that imitates part of the cellular infrastructure, causing nearby phones to connect to it. Some devices can even intercept calls and texts, though the documents don't indicate police used them for this purpose."

Californians may not be so upset if the technology is used to catch cyberthieves: according to Calif. Attorney General Kamala Harris, California is the top U.S. destination for cyber crooks. "As an international hub, more narcotics, weapons and humans are trafficked in and out of California than any other state," writes Harris in the report. "The size and strength of California's economy make our businesses, financial institutions and communities lucrative targets for transnational criminal activity."

That assessment came as news broke that the California DMV appears to have suffered a wide-ranging credit card breach involving cards used at agency's online portals. On Saturday, KrebsOnSecurity.com wrote about a series of private alerts sent by MasterCard to banks nationwide. According to Krebs, the alerts "did not name the breached entity but said the organization in question experienced a 'card-not-present' breach — industry speak for transactions conducted online. The alert further stated that the date range of the potentially compromised transactions extended from Aug. 2, 2013 to Jan. 31, 2014, and that the data stolen included the card number, expiration date, and three-digit security code printed on the back of cards." In response to the story, the CA DMV issued a statement placing blame for the incident on its credit card processing firm.

Microsoft is planning to cease shipping security updates for its Windows XP operating system next month, so you might think that federal agencies would have already moved away from this increasingly insecure OS. But according to The Washington Post, despite a recent rush to complete upgrades, an estimated 10 percent of government computers — out of several million — will still be running the operating system on that date. "That includes thousands of computers on classified military and diplomatic networks, U.S. officials said. Such networks have stronger defenses generally but hold more sensitive material, raising the stakes for breaches if they occur."

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.