GW CSPRI Newsletter

June 18, 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**

Legislative Lowdown **2**

Cyber Security Policy News **2**

Recent Publications **3**

Events

-June 21, 7:30 a.m. - 4:00 p.m., Big Data and the Government Enterprise - This conference will explore the emerging challenges, trends, directions, architectures, and solutions for big data and proven analytical strategies. Speakers include Oren Falkowitz, director of technology and data science programs, U.S. Cyber Command, National Security Agency, Department of Defense; Chris Greer, associate director, program implementation, IT Laboratory, National Institute of Standards and Technology (NIST); Suzi Iacono, senior science advisor, directorate for computer and information science and engineering, National Science Foundation, and co-chair, Big Data Senior Steering Group, Networking Information Technology Research and Development (NIRTD) Program; and George Strawn, director, National Coordination Office, NIRTD Program and co-chair, NITRD subcommittee on networking and information technology research and development, National Science and Technology Council Committee on Technology. The Willard InterContinental Hotel, 1401 Pennsylvania Avenue NW. More information.

-June 21, 3:00 p.m. - 5:00 p.m., **A Special Address on Cybersecurity** - The Heritage Foundation will host Gen. Peter Pace, 16th chairman of the Joint Chiefs of Staff. This event will be webcast, at myHeritage.org. The Heritage Foundation Douglas and Sarah Allison Auditorium, 214 Massachusetts Ave, NE. RSVP by June 14. More information.

-June 26, 9:00 a.m. - 6:00 p.m., **Apps for Security: Amphion Forum** - Apps for Security promotes civic engagement, open innovation, and entrepreneurship while making everyone safer and more secure in cyberspace. FHI 360 Conference Center 1825 Connecticut Ave NW. More information.

Legislative Lowdown

-Sen. Joe Lieberman (I-Conn.) is warning his colleagues that time may be running out for passage of broad-based cybersecurity legislation. In a floor speech last week, the senator cautioned that July could be the final opportunity to address the issue, writes The Hill. "The truth is, if we don't take it up in July and see if we've got the votes … we're not going to be able to pass this legislation in a way that's timely and allows us to go to conference, reach an agreement and send the bill to the president," Lieberman said. Lieberman's bill, which is co-sponsored by Sen. Susan Collins (R-Maine), would encourage private companies to share information about cyber threats with one another and with the government. The bill would also empower the Homeland Security Department to set minimum cybersecurity standards for critical infrastructure systems, such as electrical grids and gas pipelines. Supporters of the legislation, including the White House, say the mandatory standards are necessary to protect vital systems from attack.

-On the other side of the Senate, The Hill reports Sen. Rand Paul (R-Ky.) floated a bill that would require the government to obtain a warrant before using aerial drones to spy on U.S. citizens. The Preserving Freedom from Unwarranted Surveillance Act (PDF), would require the government to obtain a warrant to use drones with the exception of patrolling national borders, when drones are needed to prevent "imminent danger to life" or when there are risks of a terrorist attack. The bill would also give Americans the ability to sue the government for violating the act. And, it would prohibit evidence collected with warrantless drone surveillance from being used as evidence in court.

Cyber Security Policy News

-The Associated Press reports that cybersecurity researchers have found what they think is a link between the infrastructure-wrecking cyberweapon known as Stuxnet and the recently-discovered Flame virus — possibly offering a new clue about the latter's origins. Kaspersky Labs expert Alexander Gostev said in a blog post that his company had identified a similarity between a subset of the code used in Flame and another set of code used in an early version of Stuxnet, which is believed to have been aimed at Iran's disputed nuclear program.

-James A. Lewis, a senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies, argued in last week's U.S. News and World Report why a proposed cybersecurity treaty between the United States and other nations is a bad idea. "With all the excitement over Flame, Stuxnet, and the rest, a spokesperson for the Russian government has called for a global cybersecurity treaty," Lewis wrote. "It's a bad idea that dates back to the 1990s."

-The Federal Trade Commission has settled with two companies over allegations that they leaked sensitive data of individuals via file-sharing networks, writes SC Magazine. Both companies previously had sustained breaches. In 2008, the personal information, including Social Security numbers, health insurance numbers and medical diagnoses, of 3,800 consumers was exposed to any computer that connected to the Checknet peer-to-peer (P2P) network. Meanwhile, the confidential data of 95,000 consumers was publicly available through Franklin Toyota's file-sharing system. The information included names, birth dates, and driver's license and Social Security numbers.

-The Homeland Security Department later this month will present to federal computer contractors and remote cloud suppliers standards for finding and fixing cyber threats within 72 hours, DHS officials announced last week. The new approach aims to resolve what some cybersecurity specialists view as a flaw with the principle of automated “continuous monitoring” that the White House called for in 2010. Real-time tracking of potential network threats is intended to identify weaknesses faster and more economically than the old policy of manually reporting on computer inventories and incidents once a year. But spotting all the risks to personal computers and Internet connections in an organization does not make data any safer, critics note. Fixing them quickly does.

In related news, NextGov writes that the Defense Department on Friday released a mobile device strategy that provides top-level policy guidance on the use of smartphones and tablets, but offers no specifics on how to secure them for use on Defense networks. The Pentagon plans to set up a central mobile device management service at the enterprise level to ensure the security of mobile hardware. This will include over-the-air distribution of data, application and configuration settings and registration of end-user devices. Defense “must establish a federated mobile device management service to optimize operation and maintenance,” and support “access control, encryption, malware detection” and security updates, the strategy said.

Recent Publications

In Cybersecurity in the Private Sector, in Issues in Science and Technology published by the National Academy of Sciences, GW University Professor and CSPRI researcher Amitai Etzioni argues that the nation’s businesses manage a significant share of online activity related to national security and must play a larger role in ensuring the overall integrity of the system.

In “Fighting on a New Battlefield Armed with Old Laws: How to Monitor Terrorism in the Virtual World”, just published in the University of Pennsylvania Journal of Constitutional Law, CSPRI Director Lance Hoffman and Lisa Ugelow, a recent GW LL.M graduate., discuss how the possibility of terrorists using virtual worlds to recruit, communicate, launder money, and otherwise act may lead to certain interpretations of United States law or require new legislation that permits the federal government or Internet service providers ("ISPs") to monitor the virtual World for this type of conduct.

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.