GW CSPRI Newsletter

June 11, 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

-June 11, **National Symposium on Moving Target Research** - The National Science Foundation, National Coordination Office for Networking and Information Technology Research and Development (NITRD), will host a symposium to examine whether there is scientific evidence to show that moving target techniques are a substantial improvement in the defense of cyber systems. Historic Inns of Annapolis, Annapolis, MD. More information.

-June 11-14, **Gartner Security & Risk Management Summit** - The summit features five in-depth programs and more than 140 sessions. Speakers include Dell Inc. Chairman and CEO Michael Dell; Howard Schmidt, cybersecurity coordinator and special assistant to the president; David McClure, associate administrator, General Services Administration. Gaylord National, 201 Waterfront Street, National Harbor, Md. More information.

-June 12, 5:30 p.m. - 7:30 p.m., **Schieffer Series: Washington Book Launch with Best-Selling Author, David E. Sanger** - The Center for Strategic and International Studies will host a book launch for Sanger's "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power," a story of how this administration authorized the development and use of sophisticated cyber weapons against Iran. More information

-June 12, 10:30 a.m. - 12 noon, **Re-inventing Cybersecurity: Moving from Crime Scene Investigators to Pre-Crime Oracles** - Dr. Anup Ghosh will discuss the question of whether prevention is a failed security strategy. The talk will feature discussion of new strategies for prevention, explore the revolutionary potential of virtualization for Pre-Crime Forensic Analysis, and review details of a campaign against America's Defense Industrial Base that was detected, while active, using these techniques. Cypherpath, Center for Innovative Technology 2214 Rock Hill Rd, Suite 160, Herndon, Va. More information.

-June 13, 7:00 p.m. - 9:00 p.m., **Emerging Trends in Biotechnology: You, Your Health, and Your Information** - A discussion of health information technology, privacy and ethics. Speakers include Howard J. Federoff, executive vice president for health sciences and executive dean of the School of Medicine, Georgetown University; Subha Madhavan, director of clinical research informatics, Georgetown Lombardi Comprehensive Cancer Center; and Jasmine Gatti, medical officer, Food & Drug Administration. DoubleTree by Hilton Hotel Bethesda, 8120 Wisconsin Avenue, Bethesda, Maryland. 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.

Legislative Lowdown

-Sens. Sheldon Whitehouse (D-R.I.) and Jon Kyl (R-Ariz.) are circulating a draft cybersecurity bill on Capitol Hill that they hope will win over two competing camps on the issue. According to The Hill, the proposal would put the Department of Homeland Security in charge of developing a program to pressure, but not force, critical infrastructure companies to better protect their computer systems. A key point of disagreement in the cybersecurity debate is how much power the federal government should have to require critical infrastructure systems, such as power grids and gas pipelines, to meet cybersecurity standards.

-In an effort to combat identity theft, a bill that would require information stored on copier machines and scanners used by consumers be wiped clean has passed the New Jersey Assembly, the Courier Post reports. State Democrats Paul Moriarty, Herb Conaway, M.D., and Dan Benson sponsored to combat identity theft by requiring the hard drives of all digital copy machines to be wiped clean to protect sensitive, personal information was approved 51-28 Thursday.

Cyber Security Policy News

-Lawmakers on Capitol Hill are calling for hearings on who leaked information about a classified U.S. intelligence agency project to develop and release the Stuxnet worm. The enormously complex malware was built to derail or at least delay Iran's nuclear ambitions, yet was discovered when it began spreading to scientific labs and production environments outside of

Iran. Sen. Dianne Feinstein has called for Capitol Hill hearings about the leak — but not about the extraordinary attack itself. “I am deeply disturbed by the continuing leaks of classified information to the media, most recently regarding alleged cyber efforts targeting Iran’s nuclear program,” Feinstein (D-Calif.) said in a statement released last week.

The calls come after the New York Times published snippets from a new book by reporter David E. Sanger, which details how the malware was created and unleashed. The FBI has reportedly already launched a criminal investigation into the leaks, according to the Wall Street Journal. The Obama administration has been extremely aggressive in investigating and prosecuting leakers of other information, including using subpoenas to journalists in an attempt to unmask their sources and going after email and phone records.

Writing for The Atlantic, Marc Ambinder observes that the covert operation set back Tehran's nuclear program several years -- but may have put America's own infrastructure at risk. "The notion that the United States is wide open to attack has been a key argument advanced by senior U.S. intelligence and technology officials when they call for laws that would give the government more control over the dot.com domain," he wrote. "The legitimate concerns about how this protection scheme would work, or whether it would stifle innovation or compromise civil liberties, now must be paired with a fact: For every public expression of law, we can assume there's is a covert purpose also being served."

Meanwhile, Israeli officials are apparently miffed that the United States is taking more than its share of the credit for Stuxnet. Breitbart's Joel B. Pollak writes that Israeli officials who were placed at risk by the Obama administration's leaks about the Stuxnet virus are disputing American claims that the cyber-weapon was jointly developed by the U.S. and Israel. Rather, they say, Israeli intelligence first started developing cyberspace warfare against Iran, only convincing the U.S.--with some difficulty--to join in. The Israelis allege that President Barack Obama claimed credit for Stuxnet to boost his re-election campaign.

-Google has fired new salvos in a battle with Beijing over the future of information. The Times of India wrote last week that the search giant announced a new feature that warns users in China who enter search keywords that might produce blocked results and suggests they try other terms. In a separate move, Google will now be informing Gmail account holders when "state-sponsored attackers" compromise their emails. Gmail users get this pop-up message: "Warning: We believe state-sponsored attackers may be attempting to compromise your account or computer. Protect yourself now." Users are told how to do so, including with a new login process.

-Business networking site LinkedIn.com disclosed last week that a breach of some kind exposed millions of user passwords. The breach came to light after researchers discovered a large number of LinkedIn passwords were being pasted to an online forum that specializes in cracking passwords hashed with various types of encryption. The company said it was taking steps to beef up security, but the data leak came as other sites -- including Last.fm and dating site eHarmony.com also disclosed password breaches. The stream of breach news last week, dubbed by some as "breach week," saw lawmakers once again calling for national data security standards.

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.