GW CSPRI Newsletter

February 4, 2013

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

-Feb. 5, 12:00 noon - 1:00 p.m., **A Nation Forsaken - EMP: The Escalating Threat of an American Catastrophe** - The Heritage Foundation will host a discussion of the new book by the same title. The speaker will be Michael Maloof, the author. The event also will be Webcast. Lehrman Auditorium, Heritage Foundation, 214 Massachusetts Ave., NE. More information.

-Feb. 5, 10:30 a.m., **Fighting for Internet Freedom: Dubai and Beyond** - The House Commerce Committee's Subcommittee on Communications and Technology and the House Foreign Affairs Committee's Subcommittee on Terrorism, Nonproliferation, and Trade and Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations will hold a joint hearing. The witnesses will be FCC Commissioner Robert McDowell; Ambassador David Gross; Sally Wentworth, senior manager of public policy, Internet Society; and Harold Feld, senior vice president, Public Knowledge. Room 2123, Rayburn House Office Building. More information.

-Feb. 6, 2:00 p.m. - 4:00 p.m., **Measuring the Impact of Policy on Global Cybersecurity** - GW's Homeland Security Policy Institute will host an event for the release of a white paper by Microsoft Corporation's Trustworthy Computing Initiative. The paper seeks to identify reliable risk reduction metrics, and serve as a tool for national policymakers as they consider various approaches towards achieving greater cybersecurity. Co-authors and speakers Paul Nicholas and Kevin Sullivan will share the paper's key findings and recommendations, and participate in a Question & Answer session with the audience. More information.

-Feb. 7, 7:30 a.m. - 9:30 a.m., **Cybersecurity Priorities for 2013: New Legislation & Shrinking Budgets** - This discussion will explore the priorities for cybersecurity in 2013; the investments that will be needed to protect federal networks; and the policies, processes, people, and technology required to mitigate risk. The featured speaker is Michael Seeds, legislative director for Congressman Mac Thornberry (TX-13), co-author, House Cybersecurity Task Force report. Ronald Reagan Building, 1300 Pennsylvania Ave NW. More information.

-Feb. 7, 8:00 a.m. - 10:30 a.m., **Securing the Grid: Developing an Innovation Ecosystem for Grid Security and Resiliency** - Tech Council of Maryland forum hosts a discussion with former CIA Director R. James Woolsey, James Dwyer of the Patent and Trademark Office, William F. Lawrence of Lockheed Martin, and William H. Sanders of the University of Illinois at Urbana-Champaign. Bethesda Marriott, 5151 Pooks Hill Road. More information.

-Feb. 7, 6:30 p.m. - 8:00 p.m., **OWASP NoVa Meetup** - This is the sister chapter of the DC/MD organization, the Open Web Application Security Project, a worldwide free and open community focused on improving the security of application software. Living Social, 11600 Sunrise Valley Dr., Reston, Va. More information.

-Feb. 7, 6:00 p.m. - 7:30 p.m., **Mindforge Meetup** - An informal regular gathering of hackers, inventors and engineers who are looking to learn what can be done with new technologies in the arts, sciences, healthcare, gaming, academia and business venture opportunities. Bechtel Conference Center, 1801 Alexander Bell Dr., Reston, Va. More information.

-Feb. 8-9, **Spooks and Suits DC** - This conference brings members from the 16 agencies in the U.S. Intelligence Community together with innovative thinkers from a wide variety of disciplines including technology, finance, entertainment and science, for a day of frank discussions and innovative problem solving. This year’s topic is “Offense as Defense.” The Waterview Conference Center, 1919 N. Lynn St. Arlington, Va. More information.

-Feb. 15-17, **ShmooCon Conference** - An annual east coast hacker convention that offers three days of an interesting atmosphere for demonstrating technology exploitation, inventive software and hardware solutions, and open discussions of critical infosec issues. Hyatt Regency Washington, 400 New Jersey Ave., NW. More information.

Legislative Lowdown

-The Senate Committee on Commerce said last week that it is making cybersecurity legislation a priority for the year. Sens. Jay Rockefeller (D-W.V.), Dianne Feinstein (D-Calif.) and Tom Carper (D-Del.) announced the introduction of the Cybersecurity and American Cyber Competitiveness Act of 2013 and said that the private and public sectors must work together to address the threat of a cyber attack. Congress came close to passing a comprehensive cybersecurity bill in the last session, but negotiations fell apart in the measure's final days.

-Senate Homeland Security and Governmental Affairs Committee Chairman Tom Carper (D-Del.) said the White House has signaled that it will likely introduce its cybersecurity order in the second half of February, following President Obama's State of the Union address, the lawmaker told The Hill. After the White House releases the cyber order — which it has been crafting over the last several months — Carper said he plans to hold a joint hearing with the Commerce and Intelligence committees to discuss the measures included in the order. Carper said he wants to hear from administration officials and stakeholders' feedback as well.

Cyber Security Policy News

-Three of the nation's top newspapers disclosed last week that Chinese hacker groups had wide-ranging access to the newsrooms after compromising numerous systems over several months last year. On Jan. 30, The New York Times disclosed that Chinese hackers had persistently attacked the Gray Lady, infiltrating its computer systems and getting passwords for its reporters and other employees. The Times said that the timing of the attacks coincided with the reporting for a Times investigation, published online on Oct. 25, that found that the relatives of Wen Jiabao, China's prime minister, had accumulated a fortune worth several billion dollars through business dealings. The following day, The Wall Street Journal ran a story documenting similar incursions on their network. On Friday, The Washington Post confirmed that it also dealt with extensive compromises from Chinese hacking groups, after former Post reporter Brian Krebs released details about the newspaper's compromise.

-The disclosures come as the Obama administration is considering more assertive action against Beijing to combat a persistent cyber-espionage campaign it believes Chinese hackers are waging against U.S. companies and government agencies. The Associated Press reports that two former U.S. officials said the administration is preparing a new National Intelligence Estimate that, when complete, is expected to detail the cyberthreat, particularly from China, as a growing economic problem. Neither of the former officials was authorized to discuss the classified report and spoke only on condition of anonymity. One of the former officials said the NIE, an assessment prepared by the National Intelligence Council, also will cite more directly a role by the Chinese government in such espionage. The former official said the NIE will underscore the administration's concerns about the threat and will put greater weight on plans for more aggressive action against the Chinese government.

-The Pentagon has approved a major expansion of its cybersecurity force over the next several years, increasing its size more than fivefold to bolster the nation's ability to defend critical computer systems and conduct offensive computer operations against foreign adversaries, according to U.S. officials, according to The Washington Post. The move, requested by the head of the Defense Department's Cyber Command, is part of an effort to turn an organization that has focused largely on defensive measures into the equivalent of an Internet-era fighting force. The command, made up of about 900 personnel, will expand to include 4,900 troops and civilians.

-The Federal Trade Commission has issued a report (PDF) on mobility issues and said less than one-third of Americans feel they are in control of their personal information on their mobile devices. The report makes recommendations for critical players in the mobile marketplace: mobile platforms (operating system providers, such as Amazon, Apple, BlackBerry, Google, and Microsoft), application (app) developers, advertising networks and analytics companies, and app developer trade associations. The report recommends that mobile platforms should: Provide just-in-time disclosures to consumers and obtain their affirmative express consent before allowing apps to access sensitive content like geolocation; Consider developing a one-stop "dashboard" approach to allow consumers to review the types of content accessed by the apps they have downloaded; Consider offering a Do Not Track (DNT) mechanism for smartphone users.'

-The FTC action comes as the maker of the Path social networking app will pay a US$800,000 civil penalty to settle FTC charges that it illegally collected personal information from children without parental consent. PC World writes that Path has also settled FTC charges that it collected personal information from users' mobile address books without their knowledge and consent, the FTC said. The settlement requires Path to establish a comprehensive privacy program and to obtain independent privacy assessments every other year for 20 years, FTC Chairman Jon Leibowitz said during a press conference.

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.