GW CSPRI Newsletter

January 21, 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

A Good Start - But Only a Start

With all the NSA revelations and reactions, we asked our visiting scholar, Allan Friedman, to summarize the key points for the CSPRI readers.

President Obama's NSA speech on Friday had a little bit of a throwback feel. The first third, in which the President held forth on how advances in technology could change existing balances between security and individual right, read a little like an early internet policy research paper. But by clearly acknowledging the risks of surveillance oversight, the style of the speech attempted to mollify critics of recently disclosed NSAs actions. Read more.

Events

-Jan. 21, 7:45 a.m., **GovConnects Event: Financial Incentives for Cybersecurity Businesses** - The Howard County Tech Council will hold an event on tax incentives of building cybersecurity

businesses in the area. University of Maryland University College, Dorsey Station, 6865 Deerpath Rd., Elkridge, Md. 21075, Room 2128. More information.

-Jan. 21, 6:30 p.m. - 9:00 p.m., **ISSA DC Meetup: Social Engineering to Improve Security Awareness** - While many organizations perform social engineering assessments to test their security, they end up being useless games of "gotchas," with results that prove the obvious. Rarely, do they provide recommendations that could not have been found through less expensive, overt methodologies. This presentation provides guidance on performing penetration tests in a systematic way that tests levels of security awareness. The results allow for a very tailored awareness program that is specific to the organization's employee base. As the level of awareness increases, the number and severity of incidents can dramatically decrease. Center for American Progress, 1333 H Street, NW. More information.

-Jan. 23, 1:00 p.m., **Privacy and Civil Liberties Oversight Board Meeting** - The board will vote on the formal issuance of its report to the President, Congress, and the public. Additional information on the Board's review of the telephone records program, such as the prior public workshop and hearing, is available at www.pclob.gov. Pre-registration is not required. There will be a press availability after the meeting has concluded; the Board requests notification from any press that plan to attend. George Washington University Marvin Center, 800 21st St. NW. More information.

-Jan. 23, 6:30 p.m. - 8:15 p.m., **OWASP DC Meetup: Tackling Your AppSec New Year's Panel Resolutions** - This talk will include information on how organizations build AppSec programs, how to gain executive and organizational-wide acceptance to your AppSec program, as well as the current trends within the application security industry. Uber, 1200 18th St. NW, Suite 700. More information.

-Jan. 24, 7:45 a.m. - 9:30 a.m., **GovConnects Event: Cyber Threat Landscape, How the FBI is Counteracting the Current Threats** - A breakfast briefing where FBI Section Chief Donald J. Good of the Cyber Operations and Outreach Section shares his insight on how the FBI works with other government agencies and the private sector to counteract the current cyber threat scenario. University of Maryland University College, 6865 Deerpath Rd., Elkridge, Md. 21075. More information.

-Jan. 30, 7:00 p.m. - 10:00 p.m., **CharmSec Meetup** - An informal gathering of security professionals in the Baltimore area. Heavy Seas Alehouse, 1300 Bank St., Baltimore, Md. 21231. More information.

Legislative Lowdown

-The recent breaches at Target and Neiman Marcus have prompted new legislation from Congress. The Data Security Act, offered by Sens. Tom Carper (D-Del.) and Roy Blunt (R-Mo.), is essentially a bid to resurrect the push for a nationwide data breach disclosure law, says The Hill. Some 49 states and the District of Columbia already have laws on the books, forcing breached entities that lose control over consumers' personal and financial information to alert

affected individuals. Supporters of the new bill say it is necessary to set a strong set of national data security standards to replace a patchwork of state laws.

Judiciary Committee Chairman Sen. Patrick Leahy (D-Vt.) also introduced a measure earlier this month that would establish a national data breach disclosure law. The Personal Data Privacy and Security Act would establish a national standard for data breach notification, and require American businesses that collect and store consumers' sensitive personal information to safeguard that information from cyber threats. Among other things, Leahy said his bill would include "tough criminal penalties for individuals who intentionally or willfully conceal a security breach involving personal data when the breach causes economic damage to consumers." A copy of the bill is here (PDF).

-The House of Representatives voted to enact stringent new security standards for healthcare.gov, NextGov.com reports. The Health Exchange Security and Transparency Act, was introduced earlier this month and voted on the House floor three days later. "The White House slammed the proposed law on Thursday, saying it 'would impose an administratively burdensome reporting requirement that is less effective than existing industry standards and those already in place for federal agencies,'" NextGov wrote. The bill is considered unlikely to move at all in the Senate.

Cyber Security Policy News

- In a much-awaited speech last week, President Obama outlined ways his administration plans curb the National Security Agency's high-tech surveillance practices. The New York Times writes that the president said he would restrict the ability of intelligence agencies to gather phone records and would ultimately move that data out of the hands of the government. But many thought the bulk of the suggested changes "seemed more calculated to reassure audiences at home and abroad than to force radical change. Mr. Obama said he would require prior court approval each time an agency analyst wants access to calling records, except in emergencies. He also said he had forbidden eavesdropping on the leaders of allied countries, after the disclosure of such activities ignited a diplomatic firestorm with Germany, Brazil and other countries."

Privacy groups were nonplussed by the president's speech, and instead used the occasion to call for meaningful reforms to the nation's most-used snooping laws, The Hill reports. Jim Dempsey, vice president for public policy at the Center for Democracy and Technology, said Obama should address proposed reforms to the Electronic Communications Privacy Act (ECPA), a 1986 law that allows law enforcement officials to access emails older than 180 days without a warrant.

The Times also covers the president's speech from the perspective of the technology industry, which the publication says was looking for public assurances from the White House that the government would no longer secretly hoover up data from the industry's corner of the Internet cloud. "Perhaps the most striking element of Mr. Obama's speech on Friday was what it omitted: While he bolstered some protections for citizens who fear the N.S.A. is downloading their every dial, tweet and text message, he did nothing, at least yet, to loosen the agency's grip on the world's digital pipelines," wrote David E. Sanger and Claire Cain Miller.

So, what exactly did the tech industry get from the president's speech? According to Wired.com, they will have more freedom to disclose the number and the nature of requests from the government for data related to national-security concerns. "So we can expect more detailed transparency reports from the companies showing that they only provide a fraction of their information to the government," Steven Levy reports. "Additionally, the secret Foreign Intelligence Surveillance Court will add members with expertise in civil liberties and technology and will declassify more of its decisions."

Meanwhile, for those folks not trying to read the tea leaves of the president's promises, little seemed to have changed, at least from the perspective of daily disclosures in the news media about newly-discovered NSA snooping programs. As the Times, NBC, and others reported last week, the National Security Agency has planted software in nearly 100,000 computers around the world -- but not in the United States -- that allows the U.S. to conduct surveillance on those machines. Citing documents leaked by ex-NSA employee turned international fugitive Edward Snowden, The Times writes that the technology relies on radio waves that can be transmitted from tiny circuit boards and USB cards inserted covertly into computers. Among the most frequent targets of the NSA and U.S. Cyber Command, the Times reported, has been China's army.

The U.S. Supreme Court has agreed to decide the unsolved constitutional question of whether police may search, without warrants, the mobile phones of suspects they arrest, Wired.com writes. The justices did not immediately schedule a hearing for this issue, "but the outcome is expected to shore up conflicting federal and state rulings, as well as varying state laws that are all over the map as mobile phones have become virtual extensions of ourselves, housing everything from email to instant-message chats to our papers and effects," reports David Kravets. "The Pew Research Center's Internet & American Life Project last year found that about 91 percent of adult Americans own a mobile phone.

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.