GW CSPRI Newsletter

December 16, 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

Publications

Anna Choromanska, Krzysztof Choromanski, Geetha Jagannathan, and Claire Monteleoni, *Differentially-Private Learning of Low Dimensional Manifolds.*

Geetha, Jagannathan, Claire Monteleoni, and Krishnan Pillaipakkamnatt, *A Semi-Supervised Learning Approach to Differential Privacy.*

Events

-Dec. 16, 6:00 p.m. - 9:00 p.m., **The Role of Circumvention Tools in Internet Filtering Countries** - Countries throughout the world filter Internet content, including Iran, China, Cuba, and Vietnam, among others. Find out why users adopt different censorship circumvention tools, and the impact and role they play in their respective countries. 1899 L Street, N.W., Suite 400. More information.

-Dec. 17, 6:30 p.m. - 8:30 p.m., **ISSA DC Chapter: DNS Security** - Matt Bianco of InfoBlox will take a look at how mobile device proliferation is adding to the strenuous task of maintaining and allowing access to the network, and how adding security at that layer can aid in incident response. Government Printing Office, 732 North Capitol Street, Washington, DC, 20401. More information.

--Dec. 18, 2:00 p.m. - 3:00 p.m., **State of the Hack** - Mandiant's Chief Security Officer Richard Bejtlich will be joined by Kelly Jackson Higgins, senior editor at Dark Reading and Kristen Verderame, chief executive officer at Pondera International to share highlights from the past twelve months. The Webinar discussion will center around high profile security events of 2013, thoughts on what's working in security and what needs improvement, and what to expect in 2014. More information.

-Dec. 18, 2:30 p.m., **What Information Do Data Brokers Have on Consumers, and How Do They Use It?** - The Senate Commerce Committee will hold a hearing. Russell Senate Office Bldg., Room 253. More information.

-Dec. 18, 3:00 p.m., **Cyber Risk Wednesday: Risks and Resilience of the Electrical Sector** - The third Cyber Risk Wednesday discussion will focus on cybersecurity challenges facing this important sector and methods of reducing the existing and future vulnerabilities. The panel will feature Gib Sorebo, the chief cybersecurity technologist at Leidos and Tom Parker, the chief technology officer of FusionX. Additional speakers will be announced. The Atlantic Council, 1030 15th Street NW, 12th Floor. More information.

-Dec. 19, 2:00 p.m., **BlackHat 2013 Infosec Year in Review** - Whichever metrics you choose to employ, 2013 was a bumper year for the information security industry: An unholy mix of advanced research and APT attacks. "Cyberwar" started the year strong but lost ground to "opsec" as the year’s most overused (but least understood) terms. Speakers in this Webcast will include Haroon Meer, founder of Thinkst; Marco Slaviero, lead researcher at Thinkst; and Amit Yoran, senior vice president of unified products at RSA and former director of the National Cybersecurity Division and US-CERT at the Department of Homeland Security. More information.

-Dec. 19, 7:00 p.m. - 9:00 p.m., **CharmSec Meetup** - Part of the CitySec movement, this is a monthly informal meetup of information security professionals in Baltimore. Unlike other meetups, you aren’t expected to pay dues, “join up”, or present a zero-day exploit to attend. Heavy Seas Alehouse, 1300 Bank Street, Baltimore, MD, 21231. More information.

Legislative Lowdown

-Lawmakers in the House of Representatives have introduced legislation to curb cyber attacks targeting the nation's critical infrastructure. SC Magazine reports that the bill, The National Cybersecurity and Critical Infrastructure Protection Act of 2013 (PDF) lays out how real-time threat detection can be improved via the National Cybersecurity and Communications Integration Center (NCCIC) and seeks to ensure that the National Cybcersecurity Incident Response Plan is updated and implemented regularly. "The legislation would also amend the SAFETY Act, 'to establish a threshold for qualifying cyber incidents' so private entities are encouraged to relay their security procedures, in order to gain liability protections should a cyber attack strike," SC Magazine's Danielle Walker writes. "The SAFETY Act, which stands for 'support anti-terrorism by fostering effective technologies,' was introduced in 2002."

On Dec. 18, the Senate Homeland Security Committee will hold mark up the "Cybersecurity Recruitment and Retention Act." A copy of this new bill is not yet available from the Library of Congress Web site. The markup will be held in the Dirksen Senate Office Bldg., Room 342.

Cyber Security Policy News

-Going into the past week, a presidential advisory committee was to recommend major changes to the National Security Agency's surveillance programs, officials told the Wall Street Journal and The New York Times. Part of the plan was to place the NSA and the Cyber Command under separate leadership, and to put a civilian in charge of the NSA; the agency is currently headed by four-star general Keith Alexander. The other thrust of the proposed changes was to make changes to the NSA's controversial practice of collecting records on all U.S. phone calls. The Journal's report cited an individual familiar with the likely proposed changes commenting that it "aligns very closely" with the USA Freedom Act, a measure offered by Rep. Jim Sensenbrenner (R-Wis.) and Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.) that would end the bulk collection of phone records on millions of Americans.

-But on Friday, The Hill reported that the White House has decided to preserve the cyber war powers held by the director of the National Security Agency (NSA). "The decision to maintain NSA control over U.S. Cyber Command, a team of military hackers, means that the agency's next director will be a military officer and not a civilian, as privacy advocates had hoped," the Hill reported. The Washington Post also reported that the administration declined to split up the leadership of the NSA and its cyber program.

Turns out, fugitive NSA whitsleblower Edward Snowden may have stolen so much sensitive information that the only way to get some of it back and keep all of it from being slowly leaked to the media might be to offer him amnesty, some U.S. officials have acknowledged. "What National Security Agency leaker Edward Snowden has revealed so far is just a fraction of what he has. In fact, he has so much, some think it is worth giving him amnesty to get it back," CBS News reports, citing an interview with NSA Director Alexander. "The task force's job is to prevent another leak like this one from happening again. They're also trying to figure out how much damage the Snowden leaks have done, and how much damage they could still do."

Meanwhile, the new revelations from leaked Snowden documents surfaced last week that the NSA is secretly piggybacking on the tools that enable Internet advertisers to track consumers, using "cookies" and location data to pinpoint targets for government hacking and to bolster surveillance. "The agency's internal presentation slides, provided by former NSA contractor Edward Snowden, show that when companies follow consumers on the Internet to better serve them advertising, the technique opens the door for similar tracking by the government," The

Washington Post reported. "The slides also suggest that the agency is using these tracking techniques to help identify targets for offensive hacking operations.

The nation's top tech giants are getting more involved in protesting the NSA's domestic surveillance programs. As NBC News writes, eight Web giants have joined hands to start a public campaign for new limits on how governments collect user information amid concerns of growing online surveillance. The companies — Google, Microsoft, Apple, Facebook, Twitter, LinkedIn, Yahoo and AOL — issued an open letter to President Barack Obama and Congress to bring in reforms and restrictions on surveillance activities. The move comes amid a renewed push to get the Obama administration to take a position on efforts to reform the Electronic Communications Privacy Act (ECPA), a communications law that was first drafted in the mid-1980s prior to the advent of the commercial Internet. As KrebsOnSecurity.com reports, ECPA allows federal and local authorities to gain access to mobile phone and many email records without a court-issued warrant; rather, they simply need an administrative subpoena, which is far easier for investigators to obtain. Last week, a petition urging the White House to take a stand on ECPA reform received more than 100,000 signatures, the threshold for prompting a response from the administration.

-Michigan's new Cyber Civilian Corps, a rapid response team of volunteers, will assist the state and industries during a major cybersecurity incident, GovInfoSecurity reports. The Corps, described by the Michigan government as a 'Cyber National Guard' is to be deployed in late spring, and will include volunteers from government, education and business. State Chief Information Officer David Behen told the Information Security Media Group that the Cyber Civilian Corps "will be used to respond to cyber-attacks against the private and public sector in Michigan. He provides the following example: If a county finds itself under a cyber-attack, the county CIO would reach out to the Michigan Cyber-Command Center or Behen, who would determine the severity and scope of the attack."

-The Defense Advanced Research Project Agency (DARPA) accounted a new Cyber Grand Challenge on Oct. 22: Create an automated system that can recognize novel software flaws and threats in networks, in real-time. NextGov writes that the winning team will take home $2 million for creating an unmanned hacker-halter that finds and repairs bugs in software connected to a network, without disrupting the software program. Details about the new challenge are available at DARPA's Web site.

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.