GW CSPRI Newsletter

September 15, 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

New CSPRI Report:

Cost/Benefit Analysis of Cyber Surveillance Techniques

A study just completed evaluates cyber surveillance techniques employed by government signals intelligence agencies. The model attempts to disambiguate surveillance practices and potential adverse outcomes following their disclosure. Data related to techniques employed by signals intelligence surveillance agencies are inputs to a model, which produces estimates of intelligence-related, economic, political, and technological effects of these techniques. The model can be used to provide first-order approximation estimates of costs vs. benefits of various surveillance and data security techniques. These values, based on estimates of likelihood, impact, and weight, may vary widely depending on the positions of various stakeholders, such as intelligence agencies, civil liberties organizations, multinational corporations, news organizations, diplomats, and politicians.

This approach bypasses the intense sensitivities related to national security, safety, and privacy, in favor of a rational approach that highlights areas of agreement and disagreement. By explicitly acknowledging differing subjective valuations, some measure of objectivity through
careful classification is introduced. The paper is very clear in addressing its own limitations:

“As far as the quantitative output of the model, users should not read the numerical results as being rigorous or corresponding to another standard effect of any kind, whether it would be U.S. Dollars, bytes, or percentage points in the polls. All of the model inputs were purely subjective. Additionally, the techniques and effects that are included in this model are only a sample of the full population of surveillance techniques and effects in use today.”

Nonetheless, this project established a useful framework for further work, including the potential for productive use of several data-generation processes to supplement the estimates with more rigorous methods. In its present form, the project provides a usable Excel spreadsheet for stakeholders to input their own estimates and arrive at their own evaluations of various techniques and solutions.

This work arose out of a master’s thesis project by Jonathan Berliner (GW ESIA 2014), who recently graduated, worked at CSPRI over the summer further developing the work, supported in part by internal funding from the GW Office of the Vice President for Research. The project is described athttp://www.cspri.seas.gwu.edu/costbenefit-analysis-of-cyber-surveillance-techniques/ and links to the paper and the spreadsheet are given there.

Events

Sept. 15, **Big Data: A Tool for Inclusion or Exclusion?** - The Federal Trade Commission (FTC) will host a workshop. FTC Conference Center, 400 7th St., NW. More information.

Sept. 16, 9:30 a.m. – 11:45 a.m., **Wired for the Future: U.S. – Japan Cooperation for the New Internet Economy** - The Center for American Progress will host an event. Breakfast will be served from 9:00 AM. CAP, 10th floor, 1333 H St., NW. More information.

-Sept. 16, 8:00 a.m. – 5:30 p.m., **5th Annual Billington Cybersecurity Summit** – This conference will feature talks from well-known cybersecurity speakers including Admiral Michael Rogers, Commander, U.S. Cyber Command and Director, National Security

Agency/Chief, Central Security Service. This leading summit also will feature Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator, The White House; David DeWalt, Chairman and Chief Executive Officer, FireEye; Dr. Phyllis Schneck, Deputy Under Secretary for Cybersecurity, NPPD. Capital Hilton, 1001 16th St. NW. More information.

Sept. 17, 10:00 a.m., **Worldwide Threats to the Homeland** - The House Homeland Security Committee will hold a hearing. The witnesses will include Jeh Johnson (Secretary of Homeland Security), James Comey (FBI Director), and Matthew Olsen (Director of the ODNI's National Counterterrorism Center). Cannon House Office Bldg., Room 311. More information.

-Sept. 17, 10:00 a.m., **Tiversa, Inc.: White Knight or Hi-Tech Protection Racket? -** The purpose of the hearing is to examine Tiversa, Inc.'s business and marketing practices, especially as they pertain to Tiversa's relationship with the federal government. Rayburn House Office Bldg., Room 2154. More information.

-Sept. 17, 12:00 noon - 2:30 p.m., **Stepping Into the Fray: The Role of Independent Agencies in Cybersecurity** - The Center for Strategic and International Studies (CSIS) will host a panel discussion. The speakers will be **Julie Brill** (FTC Commissioner), **Valerie Abend** (Department of the Treasury's Office of the Comptroller of the Currency), Jacob Olcott (Good Harbor), **Joseph McClelland** (Federal Energy Regulatory Commission), and **David Simpson** (Chief of the FCC's Bureau of Public Safety and Homeland Security). CSIS, 1616 Rhode Island Ave., NW. More information.

-Sept. 17, 6:00 p.m. – 9:00 p.m., **NovaInfosec Meetup West** – If you are in the IT security business, like the idea of meeting to discuss the foibles of the industry, demo your recent discovery and conquest, or just drink a beer with like minded folks, then this meeting is for you. Lost Rhino Brewing Company, 21730 Red Rum Drive #142, Ashburn, VA, 20147. More information.

-Sept. 18, 9:00 a.m., 10:30 a.m., **Stealing for Profit: A Close Look at the Revenue of Online Piracy Websites -** The Information Technology and Innovation Foundation(ITIF) will host a panel discussion. The speakers will be Daniel Castro (ITIF), Sandra Aistars (Copyright Alliance), David Price (NetNames), Tom Galvin (463 Communications), and Rep. Adam Schiff (D-CA).,notice. Rayburn House Office Bldg., Room 2456. More information.

-Sept. 18, 11:00 a.m., **Examining ObamaCare's Failures in Security, Accountability, and Transparency** - This hearing will examine the failures in security, transparency and accountability during the launch of the federal exchange and the ongoing implementation of ObamaCare. On September 17th, the GAO is scheduled to release a report on the security of Healthcare.gov, assessing whether CMS took appropriate and sufficient steps to protect the website against security and privacy risks. On September 4, 2014, the Department of Health and Human Services publicly disclosed that Healthcare.gov had been the target of a successful malicious attack by a hacker. Rayburn House Office Bldg., Room 2154. More information.

Sept. 18, 2:00 p.m., **Safeguarding Privacy and Civil Liberties While Keeping our Skies Safe** - The House Homeland Security Committee's Subcommittee on Transportation Security will hold a hearing. Cannon House Office Bldg. More information.

-Sept. 18, 5:30 p.m. – 8:30 p.m., **ISSA NoVa Meetup: Secure Computing with AWS** – In this presentation, accompanied by live demonstrations, the speaker will make the case that the automation and scale of true utility-style cloud computing enables customers to build more secure systems than they can typically build on-premises at any reasonable cost. Avaya Government Solutions, 12730 Fair Lakes Circle, Fairfax, VA, 22033. More information.

-Sept. 23-24, **Safeguarding Health Information: Building Assurance Through HIPPA Security** - NIST and the Department of Health and Human Services (HHS), Office for Civil Rights (OCR) will host a conference to explore the current health information technology security landscape and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. This event will highlight the present state of health information security, and practical strategies, tips and techniques for implementing the HIPAA Security Rule. The Security Rule sets federal standards to protect the confidentiality, integrity and availability of electronic protected health information by requiring HIPAA covered entities and their business associates to implement and maintain administrative, physical and technical safeguards. Grand Hyatt, 1000 H Street NW. More information.

-Sept. 24-26, **2014 Trusted Cyber Collaboration Workshop** - An opportunity for professional information sharing, and a vendor exhibition. The event is focused on secure collaboration among industry partners and their supply chain members, mitigating the risks of information security breaches, and accelerating secure information sharing while reducing overall program costs. Hyatt Regency Crystal City, 2799 Jefferson Davis Hwy, Arlington, VA 22202. More information.

-Sept. 27, 10:30 a.m. – 5:00 p.m., **Open Government WikiHack** - The National Archives and Records Administration and Wikimedia DC, an official affiliate of Wikipedia, are teaming up to come up with solutions that help integrate government data into Wikipedia. After introductions and a brief presentation on the National Archives datasets, everyone will present their various ideas on how datasets can be used to improve Wikipedia or any of the Wikimedia projects (including Wikidata—an especially interesting opportunity). Attendees will be divided into teams, mixing together coders, experienced Wikipedians, and other enthusiastic volunteers. National Archives, 700 Pennsylvania Ave, NW. More information.

Legislative Lowdown

-Indecisiveness within and among lawmakers over whether legislation to curtail the National Security Agency's domestic surveillance budget was stringent enough has effectively won the NSA the funding it was seeking to continue the programs for another 90 days, National Journal writes. The Hill reports that "the House passed a bill to end the bulk collection program earlier this year, and instead allow the federal government to search for specific records in phone companies' databases with a court order. Privacy advocates balked, however, warning that the legislation was too broad and would have allowed the NSA to conduct searches for every number in a certain area code, for instance, or every Verizon subscriber. With a surveillance reform bill stuck in the Senate, the federal court overseeing spy agencies on Friday reauthorized the National Security Agency's controversial bulk collection of Americans' phone records." Read more here.

Cyber Security Policy News

- The U.S. government threatened to fine Yahoo $250,000 a day in 2008 if it failed to comply with a broad demand to hand over user communications — a request the company believed was unconstitutional, The Washington Post reported last week. The revelations came from newly unsealed court documents that show how federal officials forced American tech companies to participate in the National Security Agency's controversial PRISM program. "The documents, roughly 1,500 pages worth, outline a secret and ultimately unsuccessful legal battle by Yahoo to resist the government's demands," writes Craig Timberg. "The company's loss required Yahoo to become one of the first to begin providing information to PRISM, a program that gave the NSA extensive access to records of online communications by users of Yahoo and other U.S.-based technology firms."

-Democratic lawmakers on both sides of the aisle last week sought answers from Home Depot and Apple, the latest two companies to lose large amount of data in breach incidents. Both houses of Congress used the occasions to issue renewed calls for a national data breach disclosure law. "Cybersecurity threats are ongoing challenges for both the federal government and the private sector," wrote Elijah Cummings, ranking member on the House Committee on Oversight and Government Reform, in a letter (PDF) to the panel's chairman. "For those reasons, I believe an investigation of the data security breach at Home Depot will help the Committee learn from these witnesses about security vulnerabilities they have experienced in order to better protect our federal information technology assets."

Separately, Sen. John D. Rockefeller (D-W.V.), who chairs the Senate Committee on Commerce, Science and Transportation, wrote a letter (PDF) to Apple CEO Tim Cook asking for more details about the apparent vulnerability that led to the exposure of racy photos and other information on countless celebrities and iPhone users earlier this month.

“While reports of unauthorized access to iCloud accounts have been sensationalized and have largely focused on its impact on high-profile celebrities, the incident may be another example of potential security vulnerabilities as illustrated in a string of recent data breaches that have put millions of American consumers at risk,” Rockfeller wrote.

Mobile security was the focus a coordinated study of apps run by a group of national privacy and data protection bodies, which found that the vast majority are failing to provide adequate information on the privacy implications of using the app. The Global Privacy Enforcement Network looked at 1,211 apps and found 85% were not clearly explaining what data was being collected, and for what reason, according to the BBC. Nearly one-third of the apps were requesting an excessive amount of personal information, the report said.

- The Defense Advanced Research Projects Agency (DARPA) is looking for new program analysis techniques that might help analysts identify vulnerabilities in algorithms implemented in software used by the US government, military, and economic entities. Help Net Security writes that the Space/Time Analysis for Cybersecurity (STAC) program is particularly geared towards the discovery of vulnerabilities related to the space and time resource usage behavior of algorithms, as well as vulnerabilities stemming from algorithmic complexity and those exploitable for side channel attacks. Read more here.

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.