GW CSPRI Newsletter

July 2, 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.

Table of Contents

Events

-July 7-15, **SANSFIRE** - In addition to a week's worth of security training, each evening the SANS Internet Storm Center handlers share talks on their most interesting experiences and newest cyber hazards. Hilton Washington & Towers, 1919 Connecticut Avenue NW. More information.

-July 10-11, **U.S. Cyber Command Intelligence Support to Cyber** - Organized by the United States Cyber Command (USCYBERCOM), this conference will cover a range of cybersecurity issues, from creating a unifying intel strategy, to building shared situational awareness of the cyber threat to the Department of Defense, to developing a common understanding of current US adversaries' cyber capabilities policy and cyber challenges. NSA Headquarters, Ft. Meade, Md., OPS 1 Cafeteria Party Room. More information.

-July 11-13, **Symposium on Usable Privacy and Security** - The eighth Symposium on Usable Privacy and Security (SOUPS), sponsored by Carnegie Mellon CyLab, will bring together an interdisciplinary group of researchers and practitioners in human computer interaction, security, and privacy. AAAS building in Washington, 1200 New York Ave., NW. More information.

Legislative Lowdown

-Sen. Pat Toomey (R-Pa.) introduced a bill on behalf of himself and four other Republican senators setting national standards for how companies inform individuals of a breach of security related to personal information, The Hill writes. The act would direct corporations, trusts, cooperatives and similar entities that retain personal information to inform the owners of that information of a breach as quickly as possible. The breached entities would have to inform the owners of the breached information on the date it was accessed, the information that was stolen and how to contact the breached entity for more information. The notification can be by telephone, email or on paper. The personal information cited by the legislation includes Social Security numbers, driver's license numbers, financial account numbers, credit or debit card numbers and related security codes. Failure to follow the notification standard under the act goes results in a fine as high as $500,000.

Cyber Security Policy News

-A group of researchers at the University of Texas at Austin Radionavigation Laboratory recently succeeded in hijacking a drone by spoofing the global positioning system (GPS) on board the aircraft. With just around $1,000 in parts, the team took control of an unmanned aerial vehicle owned by the college, all in front of the US Department of Homeland Security. Domestic drones are already being used by the DHS and other governmental agencies, and several small-time law enforcement groups have accumulated UAVs of their own as they await clearance from the Federal Aviation Administration, Reuters reports. Indeed, by 2020 there may be tens of thousands of drones diving and dipping through US airspace. With that futuristic reality only a few years away, this action suggests that the FAA may have their work cut out for them if they think it’s as easy as just approving domestic use anytime soon.

-Cybercrime and data disclosures in filings with securities regulators are rare, despite a new SEC rule that mandates them, according to The Associate Press. Most recently, hackers broke into computers at hotel giant Wyndham Worldwide Corp. three times in two years and stole credit card information belonging to hundreds of thousands of customers. Wyndham didn't report the break-in in corporate filings even though the Securities and Exchange Commission wants companies to inform investors of cybercrimes. Amid whispers of sensational online break-ins resulting in millions of dollars in losses, it remains remarkably difficult to identify corporate

victims of cybercrimes. Companies are afraid that going public would damage their reputations, sink stock prices, or spark lawsuits.

Not that Wyndham got off the hook that easily. The Federal Trade Commission announced last week that it was suing the company, alleging that Wyndham had subjected consumers' data to an "unfair and deceptive" lack of protection that led to a series of breaches of Wyndham hotels and those of three subsidiaries. The statement describes a series of three attacks on the hotel chain and its franchisees beginning in 2008 that first compromised 500,000 credit card numbers stored by the firm, followed by attacks that breached another 50,000 and 69,000 accounts at other locations. The commission claims that those breaches are a result of Wyndham's failure to properly use complex passwords, a network setup that didn't properly separate corporate and hotels systems, and "improper software configurations" that led to sensitive payment card information being stored without encryption.

-European regulators have urged an Internet standards-setting body to let Microsoft set users' preferences for the "Do Not Track" privacy feature in the upcoming Internet Explorer 10 (IE10), Computerworld writes. But the European Commission also asked the Worldwide Web Consortium (W3C) to require browser makers to present Do Not Track (DNT) options to users when they first install or run a browser, and allow them to change the default.

-Current financial rules may not be fully up to the task of regulating the growing number of mobile payment systems, government officials told a House subcommittee on Friday. NextGov reports that Stephanie Martin, associate general counsel for the Federal Reserve Board of Governors, warned members of the House Financial Services Subcommittee on Financial Institutions and Consumer Credit that in the broader regulatory scheme, many mobile systems may not be covered, especially those used by people or organizations that aren't banks. Mobile payments usually refer to making purchases, bill payments, charitable donations, or payments to other persons using a mobile device, with the payment applied to a phone bill, credit card, or withdrawn directly from a bank account. As mobile payment options have multiplied, however, concerns have been raised over ensuring that the transactions are secure and private; and that consumers have recourse if something goes wrong.

-The Homeland Security Department last week released a new policy detailing requirements on what continuous monitoring looks like and giving agencies and vendors a clearer idea of how they will be expected to implement it, Federal News Radio writes. Congress has attempted to update federal agency information security guidelines for more than three years with requirements for agencies to take a new, dynamic approach to securing their systems, but its efforts have stalled. So the Obama administration slowly has been using policy and regulations to make the change to continuous monitoring.

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.