GW CSPRI Newsletter

June 25, 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.

Contents

Events 1

Legislative Lowdown 2

Cyber Security Policy News 2

Recent Publication 4

Events

-June 26, 8:00 a.m. - 5:00 p.m., **National Cybersecurity Center of Excellence Workshop** - The Department of Commerce's National Institute of Standards and Technology will announce the National Cyber Security Center of Excellence (NCCoE) and host an initial informational workshop to gather input. Universities at Shady Grove, 9630 Gudelsky Drive, Rockville, MD. More information.

-June 26, 1:00 p.m. - 2:30 p.m., **Government, Technology and the Expectation of Privacy in the Aftermath of U.S. v. Jones** - The American Bar Association will host a teleconferenced presentation on the U.S. Supreme Court holding that GPS tracking of a vehicle constitutes a search within the meaning of the 4th Amendment. More information.

-June 27, 9:00 a.m. - 6:00 p.m., **Apps for Security: Amphion Forum** - Apps for Security promotes civic engagement, open innovation, and entrepreneurship while making everyone safer and more secure in cyberspace. FHI 360 Conference Center 1825 Connecticut Ave NW. More information.

-June 28, 10:00 a.m., **Identity Theft and Income Tax Preparation Fraud** - The House Judiciary Committee's Subcommittee on Crime, Terrorism, and Homeland Security will hold a hearing. Rayburn House Office Building, Room 2141. More information.

-June 28, 10:00 a.m., **A Need for Privacy Protections: Is Industry Self Regulation Adequate?** - The Senate Commerce Committee will hold a hearing. Witnesses will include Bob Liodice, president and CEO, Association of National Advertisers; Peter Swire, law professor, Ohio State University; Berin Szoka, founder, Tech Freedom; and Alex Fowler, global privacy and public policy lead, Mozilla. Russell Senate Office Building, Room 253.

Legislative Lowdown

-Lawmakers in the Senate last week introduced a bill that directs 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 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 Hill reports. 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

-The cost of protecting ourselves against cybercrime can far exceed the cost of the threat itself, according to a study released last week by a team of scientists and security experts from academia and industry, led by the University of Cambridge. The report (PDF), "Measuring the Cost of Cybercrime," attempts a systematic estimate of the direct and indirection costs of defense against different types of cybercrime. The BBC quotes lead author, Cambridge Prof. Ross Anderson, as saying that a small number of gangs lie behind many incidents, and that locking them up would be far more effective than telling the public to fit an anti-phishing toolbar or to purchase antivirus software. "Cybercrime has created a swamp," Anderson told the BBC. "You need to drain the swamp by arresting people."

The Cambridge study was released the same week as a survey of large financial institutions released last week suggests that banks faced more attacks by hackers to take over customer banking accounts last year than in the two previous years, and about a third of these attacks succeeded. Computerworld's Ellen Messmer summarized the study: "The total number of attacks to try and break in and transfer money out of hacked customer accounts was up to 314 over the course of 2011, according to the Financial Services Information Sharing and Analysis Center (FS-ISAC), which released findings of its survey of 95 financial institutions and five service providers. That's an increase from 87 attacks against bank accounts in 2009 and 239 in 2010." Although attacks against accounts were up, the amount crooks were able to steal was down significantly. "The actual dollar losses taken by the financial institutions last year was $777,064,

down from a high of $3.12 million in 2010. Dollar loss for customers was $489,672 in 2011, as compared with $1.16 million in 2010."

-Owners of critical IT infrastructure might be shamed into providing the necessary security to safeguard their information assets, if they don't take steps to adequate protect the critical information infrastructure that both industry and government rely upon. According to GovInfoSecurity, a draft outline of a bill by Sen. Sheldon Whitehouse (D-R.I.), and Jon Kyl (R-Ariz.) makes it fairly clear that government won't regulate critical infrastructure owners but does propose a process in which infrastructure owners voluntarily work with the Department of Homeland Security to develop and implement practices to safeguard these critical IT systems and audit their security performance.

The bill comes as lawmakers in the Senate seem to be deadlocked in efforts to pass comprehensive cybersecurity legislation before the July 4 holiday break. But that may not be such a bad thing, according to The Washington Times. The bill from Sen. Dianne Feinstein (D-Calif.) -- which would be incorporated into the Cybersecurity Information Sharing Act of 2012 -- is designed to provide "increased authority for cyber-threat information sharing and reduces legal barriers to allow private entities to share cybersecurity information with each other and the federal government." Sen. John McCain (R-Ariz.) has sponsored an alternate version of the bill entitled the "Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Technology Act" (SECURE IT). Writing for The Times, Mike LaPointe argues that both versions are similar in scope – and similarly flawed. "Even without the imposition of 'minimum performance requirements,'" LaPointe wrote, "the bulk of this legislation still lays the foundation for greatly increased governmental capacity to use (and potentially abuse) the private information of individual citizens. Some Senators believe the bill will not reach the floor prior to the July 4th break, jeopardizing its chances of being passed before the current legislative session ends. If it does however, it appears the White House won't stand in the way."

-Apple is preparing to offer users a way to manage which third-party applications made for the device will have permission to access their contact information, as part of a new privacy control panel that's coming in iOS 6 for its iPhone and iPad devices, CNet reports. Recently, lawmakers in the House have been asking Apple why it didn't force app developers to ask users for permission before downloading contacts. The issue came to fore when Path -- a popular iOS and Android application -- was found to be collecting user contact information without permission. Path quickly issued an apology on the issue, saying that it was using that data to alert users to when their friends joined the social network. The company then introduced an updated version that required users to opt-in to the feature.

-The Department of Homeland Security has added another cybersecurity boffin to its roster, according to Federal News Radio. Rosemary Wenchel, who has spent a majority of her career in the Defense Department working on cyber issues, moved to the National Protection and Programs Directorate as the new deputy assistant secretary for cybersecurity coordination. In her new role, Wenchel will use her long-time DoD experience to coordinate joint cybersecurity efforts between the two agencies, including the National Security Agency. She also will oversee operations at the DHS-DoD Joint Coordination Element located at Fort Meade, Md. Additionally, Wenchel will work with the DHS Science and Technology Directorate to make

sure cybersecurity research and development efforts are coordinated with agency policy and operations.

-In a New York Times op-ed article, Misha Glenny, a visiting professor at the Columbia University School of International and Public Affairs, views with alarm the “gradual militarization of the Internet” and argues for the United States to discuss with the world’s major powers rules governing the Internet as a military domain.

Recent Publication

- CSPRI Associate Director Costis Toregas joined Ron Dodge from the US Military Academy to deliver a paper on "Cybersecurity Workforce Development Directions" coauthored by Dodge, Toregas and Lance Hoffman. It can be found here and is published in the Proceedings of the Sixth International Symposium on Human Aspects of Information Security and Assurance HAISA 2012 co-edited by Clarke and Furnell. A video of the presentation is expected to be made available from Plymouth University's on-line program soon- stay tuned!

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.