GW CSPRI Newsletter

June 3, 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

Events

-June 4, **Mobile Security: Potential Threats and Solutions** - The Federal Trade Commission (FTC) will host a forum to address mobile malware, how it spreads, its impact on U.S. consumers, the role of mobile platforms and others in the mobile ecosystem – from chipmakers to app developers – in securing mobile devices and data, and ways that consumers can protect themselves from mobile threats. The conference is free and open to the public, and will be Webcast. FTC Conference Center, 601 New Jersey Ave. NW. More information.

-June 4-5, **Security Industry Association Government 2013 Summit** - Panels are geared towards doing business with government and gaining a better understanding of the trends facing the industry, and the event provides one-on-one networking time with government and private sector insiders. Speakers include Connecticut Gov. Dannel Malloy; Rep. Michael T. McCaul (R-Texas); and Rep. Pat Meehan (R-Pa.). W Hotel, 515 15th Street NW. More information.

-June 6, 10:00 a.m. - 11:00 a.m., **Defending Against DDoS: Lessons Learned from High Profile Attacks on Financial Services Firms** - In this webinar, experts from Akamai will discuss aggregated information on the recent attacks; new attack methods and patterns observed;

current blocking techniques; why some defenses fail or result in performance degradation; and best practices for mitigation of DDoS attacks. More information.

-June 10-13, **Gartner Security & Risk Management Summit** - The summit features five role-based programs that delve into the entire spectrum of role evolution in IT security and risk, including: network and infrastructure security, compliance, privacy, fraud, BCM and resilience. Gaylord National, 201 Waterfront St., National Harbor, Md. 20745. More information.

-June 11-12, **Workshop on the Economics of Information Security** - Prior workshops have explored the role of incentives between attackers and defenders, identified market failures in Internet security, quantified risks of personal data disclosure, and assessed investments in cyber-defense. This year's workshop will build on past efforts using empirical and analytic tools to not only understand threats, but strengthen security and privacy through novel evaluations of available solutions. Georgetown University, Rafik B. Hariri building at 37th and O St. NW. More information.

Legislative Lowdown

-A bill waiting for Gov. Rick Perry's signature would set up even stricter protections for user data than current federal law. National Journal reports that "despite having lost his bid for the presidency, Texas Governor Rick Perry now finds himself again in a position of (potential) national leadership. On the way to his desk is a bill that would put Texas far ahead of the rest of the country when it comes to protecting consumers' electronic privacy." Unless Perry takes action to veto it, the legislation would fix a legal loophole that currently lets law enforcement seize opened emails (or unopened emails older than 180 days) with little more than an administrative subpoena. Under the new law, which passed the state House on Monday and the state Senate on Tuesday, investigators would need to get a search warrant before asking businesses to hand over consumer records.

Cyber Security Policy News

-The United States and China have agreed to hold regular, high-level talks on how to set standards of behavior for cybersecurity and commercial espionage, the first diplomatic effort to defuse the tensions over what the United States says is a daily barrage of computer break-ins and theft of corporate and government secrets. The New York Times reports that the talks will begin in July. Next Friday, President Obama and President Xi Jinping of China, who took office this spring, are scheduled to hold an unusual, informal summit meeting in Rancho Mirage, Calif., that could set the tone for their relationship and help them confront chronic tensions like the nuclear threat from North Korea. American officials say they do not expect the process to immediately yield a significant reduction in the daily intrusions from China. The head of the United States Cyber Command and director of the National Security Agency, Gen. Keith B. Alexander, has said the attacks have resulted in the “greatest transfer of wealth in history.” Hackers have stolen a variety of secrets, including negotiating strategies and schematics for next-generation fighter jets and gas pipeline control systems.

The Hill writes that news of the planned talks come as congressional pressure is mounting for President Obama to talk tough this week to his Chinese counterpart Xi Jinping on cybersecurity. House Intelligence Chairman Mike Rogers (R-Mich.) is calling on Obama to explicitly warn the Chinese president that cyberattacks waged by the country's government and military against the U.S. "will not be tolerated."

-Former CIA Director R. James Woolsey said Tuesday that the United States is at risk of a devastating cyber attack delivered by North Korea, The Wall Street Journal reports. Such an attack would use electromagnetic radiation to potentially wipe out 70% of the U.S. electric grid and cripple U.S. defenses, he said. Iran could also soon possess this capability. However, others say the chances of such an attack are low, citing more traditional cyber threats as the primary danger to U.S. interests.

-The Obama administration is skipping a proxy war of munitions and missiles in favor of a more devastating strike: sending iPads and anti-virus software directly to Tehran. Writing for Quartz, Tim Fernholz says the US government did an abrupt about-face today, announcing that it would allow American companies to sell laptops, cell phones and software in Iran. The move is an attempt to ensure that Iranians have a chance to communicate among themselves—and with the world—before and after the country's June 14th presidential election.

-The Federal Trade Commission (FTC) has filed fresh documents asking a U.S. District Court in New Jersey to reject a hotel chain's motion to dismiss a complaint filed against it following multiple data breaches. Wyndam argues that the FTC wants to turn a statute designed to protect consumers from unscrupulous businessmen into a tool to punish businesses victimized by criminals. As SC Magazine notes, the outcome of the case could decide whether the FTC can continue to punish companies that have been breached.

-The General Services Administration and the Pentagon are seeking industry feedback on how to incorporate cybersecurity standards into government buying requirements, The Washington Post writes. The GSA's request for information, issued earlier this month, stems from a February executive order meant to improve cyber protection for critical infrastructure. Now, the GSA and Defense Department's request suggests they are weighing many options, from putting in place an accreditation program to making certain acquisitions exempt from federal cybersecurity standards.

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.