GW CSPRI Newsletter

August 27, 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.

Events

-August 29-30, Takedown Con - This two-day security conference will feature presentations from more than a dozen security researchers on a broad array of topical security concerns, including SCADA exploits, Google hacking, cloud security and dual-channel authentication. More information.

-August 30, 6:00 p.m. - Monthly Cybersecurity Workshop - The Women's Society of Cyberjutsu will hold a free workshop to highlight 10-15 popular tools used in IT security for information gathering, scanning, vulnerability assessments and Web application testing. Participants will have the chance to run commands against live hosts to see how the tools work. The workshop also will be available for remote participation via Teamviewer. 1616 Anderson Rd., Rm E, McLean, VA. More information.

-August 31, **Big Data and the Government Enterprise** - A day-long series of Webcasts that will examine how military, intelligence, and civilian agencies increasingly are able to derive critical and actionable information contained in the “big data” they are receiving. Session seven includes a focus on security, privacy and big data considerations for federal agencies and employees. The presenters will be Oren Falkowitz, director of technology and data science programs, U.S. Cyber Command, National Security Agency, Department of Defense; and Henry Farrell, associate professor of political science and international affairs, George Washington University. More information.

Legislative Lowdown

-Congress is in recess until the second week in September.

Cyber Security Policy News

-A former Obama administration senior director for cybersecurity said last week that Congress's failure to pass cybersecurity legislation this year was a "missed opportunity" that was nonetheless "inevitable given that a significant portion of the private sector and U.S. Congress weren't interested in any new form of regulation." The New York Times featured an interview with Sameer Bhalotra, who left his position as President Obama's senior director for cybersecurity without discussing his next move. "The situation is dire. In many parts of the world, hackers act with near impunity in attacking foreign governments, stealing intellectual property and credit cards, and it's getting worse and worse," Bhalotra said. "The bad guys are extremely agile and it's very difficult for governments and companies to keep up with the next vector of attack."

-Corporate America says data security is now the main concern in the boardroom when it comes to legal considerations, according to a new survey of 11,000 public company directors and 2,000 general counsels. ComputerWorld writes that the results indicate that data security, for the first time, is now the top corporate fear. The research, for the "12th annual Law and the Boardroom Study", from advisory firms Corporate Board Member and FTI Consulting, shows more than half (55 percent) of general counsels rate data security as a major concern, and 48 percent of directors feel likewise. This level of fear has nearly doubled in the last four years. In 2008, only 25 percent of directors and 23 percent of general counsels noted data security as a high area of concern.

-In a draft report (PDF) issued this month, the National Institute of Standards and Technology (NIST) is urging PC and server makers to strengthen the security of the flash hardware and software on computer BIOS chips, warning that attacks against computer BIOS instructions can be used to create extremely resilient and persistent malware that survives reboots. Information Week reports that while previous examples of BIOS-infecting malware are relatively rare, worries over BIOS security have been growing, especially since researchers in 2009 demonstrated a technique for injecting code into any unsigned firmware. Last year, security researchers discovered a BIOS-altering rootkit called Mebromi, which can alter boot-time instructions in the BIOS.

-Security experts say car manufacturers haven't done enough to guard the sophisticated electronic parts on modern cars from cyber attacks. They say hackers who want to steal cars or just eavesdrop on conversations may have an easy time of it. That's according to Reuters, which last week reported about a team of top hackers working for Intel Corp's security division who toil away in a West Coast garage searching for electronic bugs that could make automobiles vulnerable to lethal computer viruses. To date there have been no reports of violent attacks on automobiles using a computer virus, according to SAE International, an association of more than 128,000 technical professionals working in the aerospace and the auto industries. The group of U.S. computer scientists from California and Washington state issued a second report last year that identified ways in which computer worms and Trojans could be delivered to automobiles -- via onboard diagnostics systems, wireless connections and even tainted CDs played on radios systems. They did not say which company manufactured the cars they examined, but did say they believed the issues affected the entire industry, noting that many automakers use common suppliers and development processes.

The criticism comes amid the publication of a report (PDF) from the University of California San Diego and the University of Washington's Center for Automotive Embedded Systems Security, which argued that modern automobiles are pervasively computerized, and hence potentially vulnerable to attack. "A modern automobile is controlled by tens of distinct computers physically interconnected with each other via internal (wired) buses and thus exposed to one another," the paper noted. "A non-trivial number of these components are also externally accessible via a variety of interfaces."

-A new study may be bad news for members of Congress who gauge their social media prowess by their Twitter follower count. The Hill writes about a new study which examined the quality of the Twitter accounts that were signed up to follow the tweets of lawmakers on Capitol Hill, and found that a huge percentage of accounts following legislators appear to be bots or fake accounts. "Jon Tilton, the general manager for digital marketing firm Advocacy Media, ran a follower check last weekend on every member of Congress using StatusPeople, a tool designed specifically to check for fake followers on Twitter, The Hill's Alicia Cohn wrote. "He found that an average of 38 percent of accounts following representatives on Twitter and 42 percent of those following senators are a combination of fake and inactive accounts."

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.