GW CSPRI Newsletter

May 21, 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

Events

-May 23, 8:30 a.m. - 1:00 p.m., **Building a Secure Cyber Future: Attacks on Estonia, Five Years On -** This conference will draw upon the lessons from planning in the Estonian experience, to ensure a more effective response to a similar major cyber incident in the future. The conference will feature representatives from Estonia, technical experts, the private sector, and both current and former US government officials. Each panel will focus on planning in different time periods: the successes and failures of planning prior to Estonia, planning and preparedness today, and finally, how states will adapt to challenges five or ten years down the road. The Madison Hotel, 1177 15th St. NW. More information.

-May 23, 9:00 a.m. – 11:00 a.m., **Cyber Security 2020: Is there a Better Way to Protect the Internet?** – This panel discussion, featuring Eric Burger (Georgetown Center for Secure Communications), Simson Garfinkel (Naval Postgraduate School), Thomas Fuhrman (Booz, Allen, Hamilton), Zach Tudor (SRI International's Computer Science Lab), and Mark Rasch (CyberSecurity and Privacy Consulting, CSC), will evaluate current approaches to cybersecurity and seek ideas for future improvement. The panelists will examine the political barriers to cybersecurity reform with a particular focus on new technologies, better business practices, and

the people and organizations that will implement new strategies. 28th floor, 1100 Wilson Blvd., Arlington, VA. More information.

-May 31, 8:30 a.m. - 4:00 p.m., **Cyber Security Conference & Expo** - The Digital Government Institute's 5th annual Cyber Security Conference, which is free for government professionals to attend, will explore today's cyber threats and offer an opportunity for those supporting government security initiatives to collaborate on how to detect, protect, and respond to these challenges. Ronald Reagan Building, The Pavilion Room, 1300 Pennsylvania Ave., NW. More information.

Legislative Lowdown

- A spate of cybersecurity bills have stalled in Congress, but one lawmaker thinks he has found a way to move forward on regulations. Rep. Jim Langevin (D-R.I.) has proposed attaching two cybersecurity amendments to the defense bill in the House, Federal News Radio writes. The first would set up a White House office to coordinate agencies' responses to cyber threats. A similar measure passed the House two years ago but died in the Senate. The second amendment would set minimum cybersecurity standards for critical infrastructure like power grids and water systems.

-A House Judiciary subcommittee appeared sympathetic last week to calls for Congress to set standards for when law enforcement can gain access to geolocation information generated by cell phones and other devices, according to NextGov. The Crime, Terrorism and Homeland Security Subcommittee debated legislation offered by Rep. Jason Chaffetz, R-Utah., that would require the government to show probable cause and obtain a warrant before requesting geolocation information from cell phones or other devices. The bill includes some exceptions for bypassing the standard such as for emergencies involving possible death or serious harm and national security.

Cyber Security Policy News

-Twitter, whose popular services lets people trade and subscribe to receiving short messages from friends and acquaintances, recently confirmed that it supports the Do Not Track header, a user privacy tool originally created by Mozilla that is in the process of becoming a web standard, according to Wired.com. That means if you visit Twitter in any web browser that supports the Do Not Track header, you can opt out of the cookies Twitter uses to gather personal information, as well as any cookies set by third-party advertisers.

-The White House's cybersecurity coordinator said Thursday that he is stepping down at the end of this month after a 2 1 / 2-year tenure in which the administration has increased its focus on cyber issues but struggled to reach agreement with lawmakers on the best way to protect the

nation's key computer networks from attack, The Washington Post reports. Howard Schmidt, who oversaw the creation of the White House's first legislative proposal on cybersecurity, said he is retiring to spend more time with his family and to pursue teaching in the cyber field.

-The Christian Science Monitor carries a provocative piece analyzing the various ways the U.S. utilities passed up government-backed chances to protect their networks from cyberattacks in the wake of 9-11. It was a race that seemed winnable. "After five years of intense effort, a 35-member team of industrial-control-system wizards from the gas, water, and electric utilities industries had created a powerful new encryption system to shield substations, pipeline compressors, and other key infrastructure from cyberattack," reporter Mark Clayton wrote. "But just weeks before it was to be finalized in 2006, the funding plug was pulled on the encryption system, called AGA-12, by the American Gas Association and its partners at the electric power and water utility industries, some who worked on the project recall."

-A start-up Internet registry has applied for the ambitiously named .secure top-level domain, which organizers say would enforce high security standards for organizations operating in that name space, says Government Computer News. Those operating subdomains within .secure would be individually vetted, required to abide by acceptable use and security control policies, and subject to disconnection, said Alex Stamos, chief technology officer of Artemis Internet Inc. At the same time Artemis announced its bid for a new generic TLD, it also announced an industry effort to develop technical and policy standards that would enable enforcement of minimum security controls for websites at the browser level.

-Hackers have compromised a number of prominent foreign policy and human rights group Web sites, configuring them to serve spyware by exploiting newly patched flaws in widely used software from Adobe and Oracle. The latest reports of this apparent cyberspy activity come from security experts at Shadowserver.org, a nonprofit that tracks malware attacks typically associated with so-called "advanced persistent threat" (APT) actors. Shadowserver uncovered Flash exploits waiting for visitors of the Web sites for Amnesty International Hong Kong and the Center for Defense Information, a Washington, D.C. think-tank. The home page for the International Institute for Counter-Terrorism was found to be serving up malware via a recent Oracle Java vulnerability (CVE-2012-0507), while the Cambodian Ministry of Foreign Affairs site was pointing to both Flash and Java exploits. According to Shadowserver, other sites that were compromised by remarkably similar attacks but since cleaned include those belonging to the American Research Center in Egypt, the Institute for National Security Studies, and the Center for European Policy Studies.

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.