GW CSPRI Newsletter

April 30, 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

-May 1, 1:00 p.m. - 2:00 p.m., **Privacy and Information Security Update** - A discussion hosted by the American Bar Association on privacy and information security legislative, regulatory, enforcement and litigation developments during the months of March and April. Speakers include Reed Freeman, Julie O'Neill and Nicholas Datlowe of Morrison Foerster. More information (PDF).

-May 1-2, **Military Smart Grids & Microgrids** - This conference brings together the key planners and technical experts who are leading the way in developing military smart and microgrid systems. The event includes several discussions about preparing for and responding to cybersecurity threats to grid infrastructure. Sheraton National Hotel Arlington, 900 S. Orme Street, Arlington, VA. More information.

-May 3, 9:00 a.m. - 12:00 noon, **State of the Mobile Net Conference** - There will be a panel titled "Complex Devices / Complex Privacy Questions: Grappling with Privacy in the Mobile Space". At 10:15 AM, Jason Weinstein, deputy assistant attorney general in the Justice Department's Criminal Division will address "Location Tracking by the Government After Jones:

What Jones Tells Us About Mobile Phone and App Tracking". At 10:45 a.m. - 12:00 noon, there will be a panel titled "Megabytes by the Morsel and Data by the Dollop: How Will New Mobile Data Plans Affect Consumers, Innovation and the Mobile Marketplace?". Reserve Officers Association Building, 5th Floor, One Constitution Ave., NE. More information.

-May 9, 12:00 noon, **Federal Cyber-Security Regulation: Critical Safety Measure, or Privacy Nightmare?** - This discussion will include viewpoints from Jim Harper, director of information policy studies, Cato Institute; Michelle Richardson, legislative counsel, American Civil Liberties Union; Ryan Radia, associate director of technology studies, Competitive Enterprise Institute. Luncheon to follow. The Cato Institute, 1000 Massachusetts Avenue, NW. More information.

Announcements

-Please join us at 12 noon on May 16 for a discussion about the security of electronic voting machines titled, "Is America Ready to Vote on the Internet? Concerns for National Security."

There are at least two major forces tugging at the success of new, modern electronic systems that will take advantage of all society knows about technology. One is the desire for an easy system with convenient access for all, minimal administrative barriers and allowing voters to participate in new ways that expand participation and bring people who could not or would not participate in the traditional election cycles. The other is the growing awareness of the almost remarkable ease with which systems can be hacked from near or (important to some) abroad, and the technology "fix" for this insecurity is not yet defined to every one's satisfaction. In addition, other concerns about the massive transition costs for procuring new, secure systems and training the primarily volunteer work force that administers elections may at times sideline or ignore strong opinions about the use of new technology. These conflicting forces will be unveiled and explored in the upcoming CSPRI seminar, cosponsored by the Verified Voting Foundation.

The program will be moderated by Prof. Lance Hoffman, Director, GW Cyber Security Policy and Research Institute. The expert panelists will include Prof. Alex Halderman, University of Michigan Dept. of Electrical Engineering and Computer Science (who, with his students, carried out what some have called "a totally epic hack of the DC Internet voting system pilot program"); Costis Toregas, Assistant Director, George Washington University Cyber Security Policy and Research Institute and an advisor to local, national and global organizations; and Matt Masterson, Deputy Elections Administrator, Office of the Ohio Secretary of State.

The discussion will be held in Room 302, Marvin Center at 800 21st St. NW. A hot buffet lunch will be provided, but registration is required. Please visit http://www.cspri.seas.gwu.edu/internetvoting.html to RSVP and find more information.

Legislative Lowdown

-The House of Representatives wasted no time in approving the controversial Cyber Information Sharing and Protection Act (CISPA), even as the White House and several previous backers of the bill withdrew their support, calling for a more measured debate on the proposal. The measure passed at 6:30 p.m. last Thursday by 248 to 168, boosted by a Republican majority (206 Republicans voted for it, along with 42 Democrats). Debate on the bill was expected Thursday, but the vote was a surprise because it had been scheduled for Friday.

According to ABC News, CISPA was designed to offer private companies new ways to protect themselves from potential economic cyberspies hailing from countries such as Russia and China. To accomplish this, the bill amends the National Security Act of 1947 (which contains no cyberthreat provisions) to increase information-sharing permission between U.S. businesses and the federal government. Supporters say information regarding cyberthreats will be more quickly and easily disseminated under CISPA. Critics of the measure say they're concerned about the scope of sharing and privacy issues. Under CISPA, companies will be permitted to share information with entities such as the Department of Homeland Security and the National Security Agency and won't be required to protect Internet users' personal data. The shared information is supposed to be related to cyberthreats, but many opponents argue that term is too broad and offers too many exemptions to current privacy laws.

The quick action on the bill turned off some lawmakers who had supported it from the beginning. Five Democratic and two Republican co-sponsors of the Cyber Information Sharing and Protection Act (CISPA) reversed course and voted against the bill on the House floor on Thursday evening, the Hill reports. In addition, President Obama has threatened to veto the bill if it should pass in the Senate, where the measure is expected to face much tougher chances of passage, according to The Guardian.

The Hill notes that the House passed two other cybersecurity measures last week, neither of which are anywhere near as controversial as CISPA. The first was H.R. 2096, the Cybersecurity Enhancement act. The bill would coordinate federal research and development on cybersecurity, and establish a program for training federal cybersecurity experts. The bill also authorizes the National Institute of Standards and Technology to set security standards for federal computer systems. The second was H.R. 3834, the Advancing America's Networking and Information Technology Research and Development act. This bill would update and modernize the High-Performance Computing Act of 1991, which established what is now a $4 billion federal research program on computing and networking systems.

Cyber Security Policy News

-VMware last week acknowledged that hackers obtained access to some of its source code and posted it online, but the firm downplayed the impact of the breach. The documents in question date back to 2003 and 2004, said Iain Mulholland, director of VMware's Security Response Center. "The fact that the source code may have been publicly shared does not necessarily mean

that there is any increased risk to VMware customers," Mulholland said. The breach, which covered VMware's ESX virtualization product, was reportedly the work of a hacker known as Hardcore Charlie, who claims to have about 300MB of VMware source code, according to security firm Kaspersky Lab.

-Dozens of websites offering credit card details and other private information for sale have been taken down in a global police operation, according to the BBC. Britain's Serious Organised Crime Agency says raids in Australia, Europe, the UK and US are the culmination of two years of work. Two Britons and a man from Macedonia were arrested, with 36 sites shut down. Some of the websites have been under observation for two years. During that period the details of about two-and-a-half million credit cards were recovered - preventing fraud, according to industry calculations, of at least a half billion British pounds.

-Defense Department officials said a pilot program that lets them share cyber threat information with the private sector has been a success story, and more firms are clamoring to join, Federal News Radio reports. Within a few months, the program will be significantly expanded and made permanent. DoD started the pilot program nearly a year ago based on a simple premise: since foreign hackers weren't having much luck stealing information from Defense Department systems, they had turned their sights on systems owned and operated by companies in the defense industrial base. The sharing would involve both classified and unclassified data and would let information flow in both directions — private firms would share information about the attacks they're seeing with the National Security Agency, and NSA would provide its own information about current threats to companies who meet the program's requirements.

-A Canadian company that makes equipment and software for critical industrial control systems planted a backdoor login account in its flagship operating system, potentially allowing attackers to access the devices online, writes Wired.com. The backdoor, which cannot be disabled, is found in all versions of the Rugged Operating System made by RuggedCom, according to independent researcher Justin W. Clarke, who works in the energy sector. The login credentials for the backdoor include a static username, “factory,” that was assigned by the vendor and can’t be changed by customers, and a dynamically generated password that is based on the individual MAC address, or media access control address, for any specific device. Clarke, who is based in San Francisco, says he discovered the backdoor after purchasing two used RuggedCom devices – an RS900 switch and an RS400 serial server – on eBay for less than $100 and examining the firmware installed on them.

-Iran said last week it was investigating a suspected cyber attack on its main oil export terminal and on the Oil Ministry itself, Reuters reports. A virus was detected inside the control systems of Kharg Island, the country's largest crude oil export facility, but the terminal remained operational, a source told the publication. Officials said the attack had not corrupted vital information at NIOC, although it had damaged general information, an oil ministry official told the semi-official Fars news agency, which has some ties to the government.

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.