GW CSPRI Newsletter

February 19, 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

-Feb. 19-21, **The 21st National HIPAA Summit** - The HIPAA (Health Insurance Portability & Accountability Act) Summit will provide the most up-to-date information available on new laws and regulations. Comprehensive presentations by leaders from the Centers for Medicare & Medicaid Services, the Office for Civil Rights, the Office of the National Coordinator for Health Information Technology. The Ritz-Carlton, Washington D.C., 1150 22nd St. NW. More information.

-Feb. 20, 8:00 a.m. - 12:30 p.m., **Cyber Resilience Workshop Series** - The International Cyber Center is pleased to announce the second workshop in this series. This week's keynote speaker is Gen. Michael V. Hayden, former director of the National Security Agency and Central Intelligence Agency. Two panels will follow, including experts and academics from Carnegie Mellon University, George Mason University, the Department of Homeland Security, and directors of several sector information sharing and analysis centers. The meeting will be held at "The Hub 3-4-5," George Mason University, Fairfax Campus, VA. More information.

-Feb. 26, 6:00 p.m. - 8:00 p.m., **Linking Disciplines: The Key to Increased Enterprise Security -** The George Washington University Dean's Speaker series event will feature Diana L. Burley, co-chair of the National Academy of Sciences Professionalizing of the Nation's Cybersecurity Workforce Committee; and Kenneth R. van Wyk, an internationally recognized information security expert and author of the O'Reilly and Associates books, "Incident Response and Secure Coding." The guests will discuss their views on linking two historically separate disciplines, information security and software security—as well as taking a holistic view towards developing the cyber security workforce—as being the key to increased enterprise security on our software, networks and services. RSVP requested by Feb. 21. GWU Virginia Science & Technology Campus, Exploration Hall, 20101 Academic Way, Ashburn, VA. More information.

-Feb. 26-28, **AFCEA Homeland Security Conference -** This conference will include a number of tracks on a variety of homeland security issues, including cybersecurity, critical infrastructure protection, biometrics and identity management and information and intelligence sharing. Grand Hyatt Washington - Constitution & Independence Ballrooms. 1000 H St NW. More information.

-Feb. 28, 6:00 p.m. - 7:00 p.m., **The Cyber Domain: Global Digital Commons or Free Fire Zone? -** This event will feature a speech by General Michael Hayden, retired United States Air Force four-star general and former Director of the National Security Agency and the Central Intelligence Agency, and currently a Principal at The Chertoff Group. The lecture is co-sponsored by George Washington University's Cyber Security Policy and Research Institute (CSPRI) and the Computer Science Department. Continental Ballroom (3rd floor), Marvin Center, 800 21st St NW. More information.

Legislative Lowdown

-Two U.S. lawmakers have reintroduced a controversial cyberthreat information-sharing bill over the objections of some privacy advocates and digital rights groups, Computerworld writes. As promised, Representatives Mike Rogers, a Michigan Republican, and C.A. "Dutch" Ruppersberger, a Maryland Democrat, have reintroduced the Cyber Intelligence Sharing and Protection Act (CISPA), a bill that would allow private companies to share a wide range of cyberthreat information with U.S. government agencies.

But according to The Hill, the bill faces tough odds of clearing Congress this year. Privacy groups say the broad language in CISPA would allow companies to send customers' electronic communications—including personal information—to the intelligence community and the secretive National Security Agency (NSA). The bill should include a measure that requires companies to strip personal information from cyber threat data before sending it to the government, the groups argue, adding that a civilian agency, like the Homeland Security Department, should oversee the intelligence sharing process.

-New draft legislation in the House of Representatives is attempting to restrict the private use of drones, making it a misdemeanor to use a UAV to photograph a person or their property without their explicit permission. Fast Company reports that the Preserving American Privacy Act of 2013 (PDF) would see public space use equally limited, requiring a max altitude of just six feet. Law enforcement bodies would have to obtain a warrant or court order to be able collect information on individuals in a private area. Also, it bans the use of armed drones in U.S. airspace--which clarifies the debate on targeting U.S. citizens. Several states are already grappling with how law enforcement should be able to use drones. Charlottesville, VA., passed a law banning drones from its airspace earlier this month. Florida lawmakers are proposing that drone use would have to be authorized by the Department of Homeland Security. The American Civil Liberties Union generally supports such legislation because governments could use drones for domestic surveillance, which raises a host of privacy issues.

Some states are turning to the threat of criminal prosecution to deter would-be drone enthusiasts from potentially peeping on others. Under a bill being considered in Oregon, anyone owning a drone fitted with a camera could be jailed for six months, or a year if it's caught flying, if a new state law is passed. The rules were proposed to tackle, among other things, peeping toms gazing into bedroom windows.

Cyber Security Policy News

-The Department of Homeland Security's civil rights watchdog has concluded that travelers along the nation's borders may have their electronics seized and the contents of those devices examined for any reason whatsoever — all in the name of national security. Wired.com reports that the DHS, which secures the nation's border, in 2009 announced that it would conduct a "Civil Liberties Impact Assessment" of its suspicionless search-and-seizure policy pertaining to electronic devices "within 120 days." More than three years later, the DHS office of Civil Rights and Civil Liberties published a two-page executive summary of its findings. "We also conclude that imposing a requirement that officers have reasonable suspicion in order to conduct a border search of an electronic device would be operationally harmful without concomitant civil rights/civil liberties benefits," the report's executive summary said (PDF).

-Hackers in several U.S. states gained access to local broadcasters' Emergency Alert Systems and issued phony warnings about a zombie invasion. Experts say the pranks, carried out in California, Michigan, Montana and New Mexico, expose widespread security weaknesses in the EAS devices, which are configured to automatically interrupt programming. Reuters reports that while broadcasters said poor password security paved the way for the bogus warning, security experts said the equipment used by the Emergency Alert System remained vulnerable when stations allow it be accessed via the public Internet. The fear is that hackers could prevent the government from sending out public warnings during an emergency or attackers could conduct a more damaging hoax than a warning of a zombie apocalypse.

-The cybersecurity order President Obama introduced last week sets up some new ways for Washington to share threat information with the private sector. For now, it'll be a one-way relationship: the government can notify private businesses if they've been targeted for cyberattack, but the businesses won't be giving anything to the government in return, National Journal's Brian Fung writes. The White House hopes Congress will change that through legislation this year. Bills like the perennially controversial Cyber Intelligence Sharing and Protection Act (CISPA) would open the floodgates of information in the other direction. Privacy groups aren't a fan of those efforts, as they worry companies won't be held accountable if personally identifiable data gets handed over and abused. But at least when it comes to the executive order, some have only praise. "Greasing the wheels of information sharing from the government to the private sector is a privacy-neutral way to distribute critical cyber information," National Journal quotes Michelle Richardson, legislative counsel for the American Civil Liberties Union.

-Malware from China has inundated the Internet, targeting Fortune 500 companies, tech startups, government agencies, news organizations, embassies, universities, law firms, and anything else with intellectual property to protect. A recently prepared secret intelligence assessment described this month in the Washington Post found that the U.S. is the target of a massive and prolonged computer espionage campaign from China that threatens the U.S. economy. With the possible exceptions of the U.S. Department of Defense and a handful of three-letter agencies, the victims are outmatched by an enemy with vast resources and a long head start. The cover story for the latest issue of Businessweek tracks the computer sleuthing of two U.S. based security experts who track several large scale attacks back to individual hackers in China. Also, today's New York Times has a lengthy front page article on the Chinese Army's involvement in cyber attacks against U.S. targets—including many in critical infrastructure.

-Large-scale, distributed-denial-of-service attacks against U.S. banks and credit unions could resume soon. GovInfoSecurity reports that the hacktivist group Izz ad-Din al-Qassam Cyber Fighters announced in a Feb 12 posting that the attacks were likely to resume. The announcement comes just two weeks after the group had declared a suspension of its attacks. Security experts warned, even before the latest posting, that more DDoS attacks against banking institutions were likely, saying the hacktivist group's reasons for suspending the attacks seemed suspicious. Evidence also suggests the botnet used in the attacks continues to grow.

-In August of 2011, while in the middle of upgrading its network security monitoring, the Federal Communications Commission discovered it had already been hacked. Over the next month, the commission's IT staff and outside contractors worked to identify the source of the breach, finding an unspecified number of PCs infected with backdoor malware. After pulling the infected systems from the network, the FCC determined it needed to do something dramatic to fix the significant security holes in its internal networks that allowed the malware in. The organization began pulling together a $10 million "Enhanced Secured Network" project to accomplish that. But as Ars Technica puts it, things did not go well with ESN. In January, a little less than a year after the FCC presented its plan of action to the House and Senate's respective Appropriations Committees, a Government Accountability Office audit of the project, released publicly last week, found that the FCC essentially dumped that $10 million in a hole.

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.