THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE
Thoughtful Analysis of Cyber Security Issues

GW CSPRI Newsletter

June 6, 2011

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

Upcoming Events

-June 7, 2:00 p.m., **Securing the Federal Agency: Reaction to Growing Cyber Threats** - This free Webinar focuses on the results of a new study of federal managers reporting how they have identified and responded to cyber threats. Speakers Rick Doten, chief scientist, Center for Cyber Security Innovation, Lockheed Martin, and Nicko van Someren, chief security architect at Juniper, will discuss federal managers' confidence in their agencies' detection and prevention of threats, and what information sharing would do to combat the external and internal breaches. More information and registration.

-June 8, 9:30 a.m. - 11:00 a.m., **Global Security Forum 2011: Vulnerability Assessment, Lesson from Four Cyber Events** - The Center for Strategic and International Studies will host a discussion, which also will be streamed live. Speakers

include **Robert L. Deitz**, former senior councilor to the director of the Central Intelligence Agency; **Judith Miller**, former general counsel for the U.S. Department of Defense; **Franklin Miller**, former special assistant to the president and senior director for defense policy and arms control, National Security Council; and **Robert J. Giesler**, former director of information operations and strategic studies, Office of the Secretary of Defense. CSIS, 1800 K. St. NW. More information.

-June 9, 2:00 p.m., Continuous Monitoring from the Front Lines of Cybersecurity: A Department of Justice Case Study - Cybersecurity strategists from the Department of Justice and IBM will present a case study detailing the Department of Justice's implementation of an endpoint management architecture that provides associated cost savings and efficiency gains. Speakers include **David Otto**, program manager, Department of Justice, and **Branden Wood**, technical sales manager, IBM, Tivoli Endpoint Manager, Federal. More information.

-June 9, 8:00 a.m. - 9:00 a.m., **Pyschological Profile of Hackers** - **Dr. Terry Gudaitis**, cyber intelligence director at Cyveillance, will try to bring the audience inside the mind of known hackers. AFEI, 2111 Wilson Blvd., Suite 400, Arlington, Va. More information.

-June 14-15, **The Workshop on the Economics of Information Security** - Prior workshops have explored the role of incentives between attackers and defenders, identified market failures dogging Internet security, and assessed investments in cyber-defense. This workshop will build on past efforts using empirical and analytic tools to not only understand threats, but also strengthen security through novel evaluations of available solutions. George Mason University, Fairfax Campus, Mason Inn Conference Center and Hotel, 4352 Mason Pond Drive, Fairfax, Va. More information and registration.

-June 14-16, **Association for Computing Machinery's "Computers, Freedom, and Privacy" Conference** - The theme of the 21st annual conference is "Computers Freedom and Privacy: The Future is Now." Georgetown University Law Center (Hart Auditorium), 600 New Jersey Avenue NW. More information.

Legislative Lowdown

-**Reps. Michael McCaul** (R-Texas) and **Dan Lipinski** (D-Ill.) last week introduced the "Cybersecurity Enhancement Act of 2011," a bill the sponsors said would help harden federal networks; spur research and development; build the cyber workforce; and enable the government, universities, and the private sector to collaborate more easily. According to the sponsors, the bill would give the National Institute of Standards and Technology the authority to set security standards for federal computer systems and develop checklists for agencies to follow; create a federal-university-private-sector task force to coordinate research and development; establish cybersecurity research and development grant programs; and create scholarship programs at the National Science Foundation that

can be repaid with federal service. **Sen. Bob Menendez** (D-N.J.) is expected to offer a companion bill in the Senate. The bill is similar to a measure passed by the House in 2010.

Cyber Security Policy News

-The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force, reports *The Wall Street Journal*. The Pentagon's first formal cyber strategy, unclassified portions of which are expected to become public next month, represents an early attempt to grapple with a changing world in which a hacker could pose as significant a threat to U.S. nuclear reactors, subways or pipelines as a hostile country's military, the WSJ reporters said. In part, the Pentagon intends its plan as a warning to potential adversaries of the consequences of attacking the U.S. in this way. "If you shut down our power grid, maybe we will put a missile down one of your smokestacks," said a military official.

The Washington Post has taken a look at the Pentagon's list of cyber weapons and tools, including viruses that can sabotage an adversary's critical networks. "The framework clarifies, for instance, that the military needs presidential authorization to penetrate a foreign computer network and leave a cyber-virus that can be activated later," the Post's Ellen Nakashima writes. "The military does not need such approval, however, to penetrate foreign networks for a variety of other activities. These include studying the cyber-capabilities of adversaries or examining how power plants or other networks operate. Military cyber-warriors can also, without presidential authorization, leave beacons to mark spots for later targeting by viruses."

All this talk of cyberweapons and trading missile attacks for virus infections came as officials at Google warned that hundreds of people, including senior U.S. government officials and military personnel -- were tricked into giving away their Gmail credentials, in a cleverly-disguised targeted phishing campaign. Google said it shut down the attack, which appeared to have happened in January and to have emanated from the Jinan province of China. The Chinese government vociferously denied any involvement in the attacks, even as it launched a counter allegation that the U.S. is launching a global "Internet war" to bring down Arab and other governments. At the same time, an essay by a pair of military officers from the People's Liberation Army Academy of Military Scientists urged China to make mastering cyber-warfare a military priority as the Internet becomes a crucial battleground for opinion and intelligence, Reuters reports.

Meanwhile, a number of major U.S. defense contractors appear to be dealing with quite sophisticated intrusions of late. Lockheed Martin said last week that it was the recent target of a "significant and tenacious" hack in May, although the defense contractor and the Department of Homeland Security insist the attack was thwarted before any critical data was stolen. The effort highlighted the fact that some hackers, including many working for foreign governments, set their sights on information that has the potential to

be far more devastating than accessing credit cards. Fox News reported that Northrop Grumman Corp. may also have been hit by a serious cyber assault, and that the company shut down remote access to its network on May 26 in response to the incident. Wired.com's Kevin Poulsen reported last week that defense contractor L-3 also warned employees that hackers were targeting the company using inside information on the SecureID keyfob system freshly stolen from an acknowledged breach at RSA Security.

-The White House and Department of Homeland Security last week announced new reporting metrics for federal chief information officers that requires agencies to report on their progress in automating the continous measurement of the most critical security risks. The new metrics, available here (PDF), assess agency progress in implementing the sensors and systems needed for continuous monitoring of cyber threats and vulnerabilities. **Alan Paller**, research director for the SANS Institute, a cybersecurity training group, called the step "a huge improvement in federal cybersecurity - one that will result in rapid risk reduction and potentially allow the government to lead by example in showing how to manage cyber security effectively."

-The US Department of Health and Human Services (HHS) has proposed changes to the Health Insurance Portability and Accountability Act (HIPAA) that would allow patients to see the names of every person who accesses their electronic health records, MSNBC reports. The updated rules would give patients the right to see the name of any person who accessed their electronic health records, and what he or she did with them. The so-called "access report" would be available from some health care providers as soon as Jan. 1, 2013. It would function much like a free credit report -- consumers would have the right to ask for one such report for free every year.

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.