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

GW CSPRI Newsletter

July 5, 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 1
Legislative Lowdown 2
Cyber Security Policy News 2

Upcoming Events

-July 4-9, **The 9th International Conference on Web Services, IEEE Conference on Cloud Computing** - This week-long conference on cloud computing challenges includes a number of tracks dedicated to cybersecurity. Washington Marriott, 1221 22nd St. NW. More information.

-July 11-12, **Industrial Security Conference** - As the threat of terrorism and cyber attacks increases, so does the need to ensure your industrial security compliance program is up to date, robust and comprehensive. This Summit will provide proven-effective strategies for implementing strong security and compliance measures. The Westin Washington D.C. City Center, 1400 M. St. NW. More information.

-July 12, 10:00 a.m., **Cybersecurity Best Practices & Lessons for Enterprises Under Persistent Threat** - 'Night Dragon' and 'Stuxnet' attacks have unleashed a flurry of media coverage. As cybersecurity threats escalate and the level of process automation increases, the oil and gas industry is taking lessons from downstream plants and the utility industry. Nation state attackers are the biggest threat to the industry, but many unknown threats also exist worldwide. This Webcast will address best practices from other Process Industries that are proactively addressing regulatory mandates, protecting the most sensitive enterprise data and industrial controls. More information.

-July 15, 8:00 a.m. - 5:00 p.m., **DC Cybersecurity Symposium** - This conference will focus on the state of U.S. cyber protection one year after the stand-up of U.S. Cyber Command. The gathering also will explore CYBERCOM's interface with the five military services, the Unified Commands/COCOMs, DHS, Civilian Agencies, Industry, and Coalition Partners - as these enmeshed interrelationships unfold, and the framework for collaboration strengthens. Capital Hilton, 1001 16th St. NW. More information.

Legislative Lowdown

-Members of the Senate Commerce Committee expressed broad agreement on the need for a national data breach reporting standard but were less unified with regards to the prospect of comprehensive privacy legislation at a hearing last week, The Hill reports. **Chairman Jay Rockefeller** (D-W.Va.) said his Do Not Track Online Act focuses on forcing companies to give consumers a clear picture of what information they're collecting and allowing those users a single easy way to stop the collection process. The senator also voiced support for a comprehensive privacy bill from Sens. **John Kerry** (D-Mass.) and **McCain** (R-Ariz.), calling it "a very good piece of legislation." But ranking member **Pat Toomey** (R-Pa.) was less convinced of the need for comprehensive privacy legislation, saying there didn't appear to be a clear picture of the potential harms to consumers that would be addressed by any privacy bill along with the potential cost to industry.

Cyber Security Policy News

-Federal banking regulators last week released a long-awaited supplement to the 2005 guidelines that describe what banks should be doing to protect e-banking customers from hackers and account takeovers, KrebsOnSecurity.com writes. Experts called the updated guidance a step forward, but were divided over whether it would be adequate to protect small to mid-sized businesses against today's sophisticated online attackers. The updated guidance recognizes the need to protect customers from newer threats, but stops short of endorsing any specific technology or approach. Instead, it calls on banks to conduct more rigorous risk assessments, to monitor customer transactions for suspicious activity, and to work harder to educate customers — particularly businesses — about the risks involved in banking online. A copy of the new guidelines is here (PDF).

-A federal judge has found that Google can be held liable for damages for secretly intercepting data on open Wi-Fi routers, Wired.com reports. The ruling is a serious legal setback for the search giant over activity it has engaged in across the United States for years. That decision, the first of its kind, was handed down late last month by a Silicon Valley federal judge presiding over nearly a dozen combined lawsuits seeking damages from Google for eavesdropping on open Wi-Fi networks from its Street View mapping cars. The vehicles, which rolled through neighborhoods across the country, were equipped with Wi-Fi–sniffing hardware to record the names and MAC addresses of routers to improve Google location-specific services. But the cars also secretly gathered snippets of Americans' data.

In related news, the U.S. Supreme Court will review the constitutionality of surreptitiously placing GPS devices on suspects' vehicles without a warrant. Wired.com's David Kravets argues that the petition, which will not be decided until the new term begins in October, is arguably one of the biggest Fourth Amendment case in a decade — one weighing the collision of privacy, technology and the Constitution.

-The Homeland Security Department unveiled a new system of guidance on Monday intended to help make the software behind Web sites, power grids and other services less susceptible to hacking, according to The New York Times. The system includes an updated list of the top 25 programming errors that enable today's most serious hacks. It adds new tools to help software programmers eliminate the most dangerous types of mistakes and enable organizations to demand and buy more secure products. The effort to improve software security has been three years in the making, according to **Robert A. Martin**, principal engineer at Mitre, a technology nonprofit organization that conducts federal research in systems engineering.

-Cyber crooks are outwitting national and international legal systems that fail to embrace technological advances, the Department of Homeland Security warned last week. DHS Secretary **Janet Napolitano** said that prominent cyber attacks of late -- including those targeting the International Monetary Fund, the U.S. Central Intelligence Agency and the U.S. Senate, as well as companies such as Citigroup and Lockheed Martin Corp -- have raised questions about the security of government and corporate computer systems and the ability of law enforcement to track down hackers. "Right now there needs to be some sort of international legal framework to address those and that does not yet exist," said Napolitano last week in her address to an international security conference in Vienna.

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.