THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY AND RESEARCH INSTITUTE

Thoughtful Analysis of Cyber Security Issues

GW CSPRI Newsletter

November 21, 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.

Contents

Upcoming Events

- December 5, 9:00 a.m. - 3:30 p.m. Personal Information: The Benefits and Risks of De-Identification. The Future of Privacy Forum, with CSPRI as its academic co-sponsor, is hosting leading academics, advocates, Chief Privacy Officers, legal experts and policymakers as they discuss and debate the benefits and risks of de-identification, the definition of personal information and whether anonymization still matters. The National Press Club, Murrow Room, 529 14th Street, NW, Washington, DC 20045. More information.

-Dec. 6, 8:30 a.m. - 5:00 p.m., **Securing Supply Chains in the Cyber Domain** - Speakers include Brett B. Lambert, deputy assistant secretary of defense, manufacturing and industrial base policy, Department of Defense; Larry Clinton, president and CEO, Internet Security Alliance; Steven R. Chabinsky, deputy assistant director, Cyber Division, Federal Bureau of Investigation; Jeffrey W. Irvine, deputy assistant director, Office of Investigations, US Secret Service. The Ritz-Carlton Pentagon City, 1250 South Hayes Street, Arlington, VA. More information.

Announcements

CSPRI Researchers Diana L. Burley, Lance J. Hoffman and Costis Toregas have a new report out, *Thinking Across Stovepipes: Using a Holistic Development Strategy to Build a Cybersecurity Workforce*, available on the CSPRI website at http://www.cspri.seas.gwu.edu/Publications,%20Papers,%20and%20Research/Stovepipes%20GW%20CSPRI%20Report%202011%208.pdf, it proposes a holistic approach to developing the cybersecurity workforce based on careful integration of workforce development strategies into a plan that involves educators, career professionals, employers, and policymakers. First, it motivates this by describing how other fields such as medicine have successfully done this and arguing that cyber security is, like medicine, inherently cross-disciplinary at multiple levels of expertise and performance, making it similar in complexity to the medical profession and thus a good candidate for some of the solutions developed there. The article then focuses on one element of a holistic strategy – education -- and discusses the findings of a recent workshop on cybersecurity education. It then places those findings in the context of the broader discussion and suggests some practical steps. They encourage computer science educators, human resources professionals, and the functional experts from disciplines that will attract computer science graduates to think beyond their "stovepiped" fields and collaborate so that holistic, integrated solutions can be developed, accepted, and implemented.

Legislative Lowdown

-It's looking likely that lawmakers will punt action on a raft of cybersecurity bills until the next session of Congress. NextGov reports that the Senate plans to hold a vote on comprehensive cybersecurity reforms during the first work period of 2012. The scheduling came in a letter sent late Wednesday. Majority Leader Harry Reid (D-Nev.) informed Senate Republicans of his decision to bring legislation to the floor early next year, according to members of the Homeland Security and Governmental Affairs Committee. Reid's bill is expected to include measures proposed by the committee that would automate federal information security practices and charge the Homeland Security Department with regulating safeguards for civilian public and private networks.

-Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.) filed amendments to the National Defense Authorization Act on Thursday that would increase the penalties for cybercrimes and make it a felony to damage a computer that controls systems critical to national security, according to The Hill. The amendment clarifies that only serious misconduct such as hacking

should be prosecuted under the Computer Fraud and Abuse Act, as opposed to relatively innocuous actions such as lying in an online profile or violating a site's terms-of-use agreement. It would increase the criminal penalties for computer hacking and conspiracy to commit hacking.

-The controversial Stop Online Piracy Act appears to be dead in the water in the face of significant opposition. The bill would require ISPs to block access to sites determined to be infringing on copyrights and trademarks. But House Oversight and Government Reform Committee Chairman Darrell Issa (R-Calif.) said the original co-sponsors of the legislation are wavering in their support after hearing more last week about the bill's potential impact on efforts to secure the Internet. House Minority Leader Nancy Pelosi (D-Calif.) also announced via Twitter that she opposes the bill.

Cyber Security Policy News

-Hackers gained remote access into the control system of the city water utility in Springfield, Illinois, and destroyed a pump last week, according to a report released by a state fusion center and obtained by a security expert, Wired.com reports. The hackers were discovered on Nov. 8 when a water district employee noticed problems in the city's Supervisory Control and Data Acquisition System (SCADA). The system kept turning on and off, resulting in the burnout of a water pump. The disclosure came at the same time an anonymous security researcher hacked into a water SCADA system in Texas and posted screen shots of the attack, prompting the city of South Houston to shut down online access to its SCADA system.

The events have helped to re-focus attention on pervasive weaknesses surrounding SCADA networks, which hundreds of companies use to manage far-flung facilities, from power utilities to chemical production plants. Security researchers at Pike Research estimated last week that $14 billion will be pumped into the smart grid from now through 2018, with 63 percent of that money for control system security. The company found that a "$60 piece of software can bypass an entire defense-in-depth implementation," ComputerWorld writes.

-A computer virus attack disabled an ambulance dispatch system in New Zealand, leaving drivers in the dark and forcing employees to adjust their emergency procedures for two days. MSNBC reports that the Nov. 9 malware attack hit the communication centers of St. John, an ambulance company serving nearly 90 percent of New Zealand's population. For two days, the computer systems that allow call center employees to alert drivers via on-board mobile data terminals (MDT) were disabled.

-New research from Russian antivirus firm Kaspersky Lab suggests that the hacker group behind the "Duqu" Trojan may have been working on its attack code for more than four years. Kaspersky published some findings today from a recent rooting through Duqu samples provided by researchers in the Sudan, saying that one driver included with the attack payload was compiled in August 2007, extending the timeline of the gang's work. The malware has been compared in stealth and complexity to Stuxnet, a highly targeted malicious software strain that experts say was designed to sabotage Iran's nuclear ambitions.

-Facebook is nearing a landmark settlement with the Federal Trade Commission over its privacy practices, the LA Times reports. The social networking giant could announce a deal as early as Monday over charges that it violated users' privacy when it changed default settings to make more of their information public. The Times writes that the potential settlement is sending a strong message to Internet companies that regulators are getting serious about protecting the privacy of consumers.

Investigators probing the hacker attack at NASDAQ have found lax security practices that enabled the attackers, Reuters reports. The investigators found that NASDAQ's basic computer architecture was sound, which kept its trading systems safe from the hackers, according to four people who were briefed on the FBI probe or had knowledge of NASDAQ's efforts to improve its security with the help of external consultants. The sources, however, said the investigators were surprised to find some computers with out-of-date software, misconfigured firewalls and uninstalled security patches that could have fixed known "bugs" that hackers could exploit.

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.