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

GW CSPRI Newsletter

April 4, 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

-Apr. 6, 10:00 a.m., **The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age** - The Senate Judiciary Committee will hold a hearing on Internet privacy. The witnesses will include Cameron Kerry, general counsel, Department of Commerce, and Associate Deputy Attorney General James Baker. The hearing also will be Webcast. Location: Room 226, Dirksen Building.

-Apr. 6, 8:30 to 9:30 a.m., **The Establishment of the National Strategy for Trusted Identities in Cyberspace - Jeremy Grant**, national program manager for the NSTIC,

will talk about where things stand with this major initiative in electronic commerce. 1725 Eye Street, NW. More information.

-Apr. 6, 2:00 p.m., **Implementing Continuous Monitoring as Part of Your Cyber Security Strategy** - A free Webinar on practical steps to implement a cyber security continuous monitoring strategy. Moderated by **Tim Hartman**, general manager of Government Executive Media Group. More information.

-Apr. 7, 5:00 p.m., **Can We Make the Internet Safer?** - The University of Maryland has announced the creation of a new cybersecurity seminar series made possible by a sponsorship from Google. The series will feature a diverse group of speakers from industry, academia, and government, addressing a broad range of topics related to cybersecurity, including technology, policy, and economics. Invited speakers will also examine the impact that cybersecurity threats and protective measures are having on privacy, identity, social networks, business and national security. This week's guest will be **Vint Cerf**, chief internet evangelist at Google. University of Maryland's College Park campus at the Jeong H. Kim Engineering Building Rotunda. More information.

-Apr. 13, 12 noon, **Deterring Cyber Threats to U.S. Security** - **Prof. Charles Glaser** of GWU's' Elliot School of International Affairs, will address the national security threats posed by cyber attacks. More specifically, it explores the difficulties and possibilities for deterring cyber attacks, identifying key differences between cyber and conventional attacks. The talk provides a basic framework for evaluating the types of protection that are possible and the technical issues they raise. Room 302, Marvin Center at 800 21st St. NW. Event abstract (PDF).

Announcements

-There will be a special session on "Privacy Protection for Users of Mobile Services," as part of the IEEE 2011 Intelligent Transportation Systems Conference. The conference will be held at GW, on October 5-7, 2011. Privacy experts and those doing research in the field are invited to visit the conference website at http://www.seas.gwu.edu/itsc2011 and to contribute a paper. The deadline for paper submission will be April 30th (the website currently lists an April 10th deadline, but this will be extended). Special session papers will undergo the same review process as regular, and accepted papers will appear in with regular conference papers in the conference proceedings and the IEEE Digital Library.

The description of the session is as follows:

Privacy concerns have been raised as potential obstacles for widespread participation in mobile services. Meanwhile, mobility creates additional privacy protection challenges, as patterns in user movements can be used to link anonymized, location-based data from mobile services to individual users. This session will include new research and reviews of latest research in the area of privacy protection for users of mobile services, including:

• Privacy protection with short-lived pseudonyms: pseudonymous ID generation and management, guaranteeing uniqueness of IDs, synchronization of pseudonym changes, maximizing mix zone effectiveness
• Data obfuscation and degradation for privacy protection: inclusion of spurious or noisy data, injection of data with false trajectories or paths, effect of data obfuscation and degradation on mobile applications
• Using anonomized public-key certificates to protect mobile user privacy while allowing messages to be protected with digital signatures
• Metrics for measuring location-based privacy protection
• De-anonymization attacks on anonymized data in mobile services
• Regulatory mechanisms and privacy policies for privacy protection
• Users' perceptions of and demands for privacy protection in mobile services

Legislative Lowdown

-A bipartisan press conference on Capitol Hill Monday will be the latest sign that years of lobbying on the copyright front by various stakeholders may finally come to fruition in the form of new online piracy laws this year, The Hill reports. According to that publication, lawmakers from both parties and chambers of Congress will gather at the Capitol this week with representatives from industry and organized labor to once again denounce the effects of online piracy and counterfeiting on the U.S. economy.

Cyber Security Policy News

-**The National Security Agency**, has joined a probe of the October cyber attack on **Nasdaq OMX Group Inc.** (NDAQ) amid evidence the intrusion by hackers was more severe than first disclosed, Bloomberg reports.The involvement of the NSA, which uses some of the world's most powerful computers for electronic surveillance and decryption, may help the initial investigators -- Nasdaq and the FBI -- determine more easily who attacked and what was taken. It may also show the attack endangered the security of the nation's financial infrastructure, Bloomberg notes.

-Hundreds of thouands -- possibly more than a million -- legitimate Web pages, were hacked via security vulnerabilities that redirect visitors to sites that try to install rogue antivirus or "scareware," invasive programs that use misleading security alerts in a bid to frighten consumers into installing and purchasing worthless security software. The malicious software also was found on some sites associated with Apple iTunes, but Apple appears to have prevented the malicious code from executing from those domains, MSNBC writes.

-Dozens of Fortune 500 companies have begun warning customers to be especially careful of email scams and targeted phishing attacks, following the theft of customer email addresses and/or names. The disclosures were traced back to a breach at Epsilon, an email marketing firm based in Irving, Texas that discovered on Mar. 30 that a subset

of its clients' customer data was exposed by a break-in. Epsilon is just the latest email service provider to disclose attacks that compromised consumer contact data for customers of some of the largest brands in the world.

-The Pentagon is finalizing a new cyber warfighting strategy that will create a framework for training and equipping forces, as was as call for more international cooperation in the domain, DefenseNews reports. According to the publication, U.S. Defense Secretary Robert Gates is reviewing the document, which could become official in a matter of days, according to Mary Beth Morgan, DoD director for cyber strategy.

Meanwhile, just how much the Defense Department will spend on cybersecurity next year remains hard to pin down, says NextGov. Initially, White House proposed spending $2.3 billion on cybersecurity at the DoD in its 2012 budget request. At the same time, Air Force officials said their budget request would be $4.6 billion for cyber programs. But this appears to be a shifting equation: "On March 21, in response to a query from Nextgov, Pentagon officials said the original $2.3 billion figure covers all Defense components," NextGov's Aliya Sternstein wrote. "On March 23, officials amended that response and provided a higher total -- $3.2 billion -- to reflect the cost of information assurance 'program elements' at individual agencies and services, plus activities typically not defined as information assurance that are critical to the military's overall cyber stance."

At least six servers at NASA exposed to the Internet had critical vulnerabilities that could have endangered the Space Shuttle, the International Space Station, and Hubble Telescope missions, a report (PDF) by the agency's inspector general found. Computerworld writes that the flaws would have been found earlier by a security oversight program the agency agreed to last year but hasn't yet implemented.

-The **FBI** is seeking assistance to help decipher a pair of encrypted notes found in the pockets of a man who was murdered in St. Louis nearly 12 years ago. The notes were thought to have been written by the hand of the victim, who was a noted cryptographic expert. According to the FBI, the media coverage from that public request has generated an outpouring of responses. To accommodate the continuing interest in this case, the FBI has established a Web page where the public can offer comments and theories about the coded messages.

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.