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

GW CSPRI Newsletter

March 28, 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

-Mar. 28-29, **National Science Foundation's National Science Board's Task Force on Data Policies** - The agenda for the meeting features discussion of high-performance cyber infrastructure and data-intensive science. NSF, 4201 Wilson Blvd., Room 1235, Arlington, VA. More information.

-Mar. 29, **Economic Ramifications of Cyber Threats and Vulnerabilities to the Private Sector** - The Senate Commerce Committee will hold a hearing featuring Gordon Snow of the FBI's Cyber Division; Harriet Pearson, chief privacy officer at IBM; Sara Santarelli, chief network security officer at Verizon; and Tom Kellerman, vice president

of security at Core Security Technologies. Room 253, Russell Senate Office Building. More information.

-Mar. 30, 7:30 - 9:30 a.m., **GovExec: WikiLeaks: Lessons Learned** - A complimentary discussion of what lessons the WikiLeaks incident has offered about information-sharing and cybersecurity. Ronald Reagan Building, The Rotunda, 8th Floor (North Tower), 1300 Pennsylvania Avenue, NW. More information.

-Mar. 30, **National Defense Industrial Association's Cyber Division Meeting** - At this inaugural meeting of the division, the appointed co-chairs will lead discussions and solicit recommendations designed to develop an organizational structure composed of leadership positions and standing committees, and build and execute a program of activities designed to fulfill the objectives set forth in the organization's charter. A key action will be identifying a set of standing committees and designating committee leaders. Northrop Grumman Information Systems, 7575 Colshire Drive, McLean, VA. More information.

--Mar. 30, 12 noon, **Security and Privacy: Clinical Case Studies** - Dr. Neal Sikka, of the GW School of Medicine and Health Sciences, will discuss clinical case studies that highlight the dual challenges for medical practitioners. Room 302, Marvin Center, 800 21st St. NW. More information.

-Apr. 1, 2:00 - 4:00 p.m., **Advisory Committee for Cyberinfrastructure Meeting** -- This National Science Foundation panel will meet, on site and by teleconference. 4201 Wilson Blvd., Room 1160, Arlington, VA. More information.

Announcements

-This year's **Computers, Freedom and Privacy Conference**, June 14-16 at the Georgetown University Law Center in Washington, will feature a research showcase in the form of a research poster session on June 16 as well as a research panel that includes the authors of the best research posters. CFP focuses on topics such as freedom of speech, privacy, intellectual property, cyber security, telecommunications, electronic democracy, digital rights and responsibilities, and the future of technologies and their implications. Researchers who work in any of these areas are invited to submit research abstracts at the submission site. The deadline is April 3.

-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

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 week after the Senate held a hearing on the state of online consumer privacy, **Sen. John Kerry** (D-Mass) has published a draft of the "Commercial Privacy Bill of Rights Act of 2011." The Act, co-sponsored by **Sen. John McCain** (R-Ariz.), directs the FTC to make rules requiring certain entities that handle information covered by the Act to comply with a host of new requirements protecting the security of the information as well as the privacy of the individuals to whom information pertains, writes **Nicole Friess**, in an analysis of the bill at Information Law Group. She states that "The Act aims to enhance individual privacy protections "in a balanced way that establishes clear, consistent rules," and "will stimulate commerce by instilling greater consumer confidence at home and greater confidence abroad."

-Sen. Ron Wyden (D-Oregon) has offered a bill that would require the government to obtain warrants before using geo-location information to track individuals. According to NextGov, the bill specifies emergency exceptions, including when someone's life or safety is in danger, when there are immediate risks of danger to others, activities that threaten national security, or activity indicative of organized crime. Critics of the bill say the exceptions are so narrow that federal law enforcement agents might be wary of ever using geo-location information to track people.

Cyber Security Policy News

-**Comodo**, a New Jersey based company that is a leading provider of Web site security products, said last week that attackers had compromised a reseller of its services in an apparent bid to obtain security digital certificates that would allow them to impersonate Google, Yahoo, Skype and other major Web services. Comodo said nine "secure sockets layer" (SSL) certificates were fraudulently obtained, including one for Microsoft's Live.com. Experts warned that the certificates would be useful to anyone in control over a large network, such as an ISP, and could allow the attacker to intercept encrypted communications sent to and from the domains in the SSL certs, such as Google.com and Live.com. Comodo maintained that the attackers were from Iran, based on the fact that the Internet addresses used in the attack traced back to Tehran, although experts note that the attackers may have been located elsewhere and simply routed their connections through hacked systems or open relays in Iran.

-Security researchers have released information on 45 vulnerabilities in the software used to control facilities such as nuclear plants and oil refineries, The Register reported. Security bugs were found in programs by Siemens, Iconics, 7-Technologies, Datac and Control Microsystems that could allow attackers to remotely execute code, access sensitive data, and disrupt physical equipment by targeting supervisory control and data acquisition software (SCADA) installed on Internet-connected machines. “SCADA is a critical field but nobody really cares about it,” Luigi Auriemma, one of the researchers, said in explaining why he and other researchers decided to release their findings publicly.

-**The Department of Homeland Security** on Wednesday rolled out its much-anticipated white paper (PDF) on the ecosystem of cybersecurity. The document explores technical options for creating a safer, more secure and resilient network of networks, and calls for networks where computers and devices work together in near-real time in its own defense. The paper presents three building blocks as foundational for a "healthy cyber ecosystem": automation, interoperability, and authentication.

In other DHS news, the department has launched its first cybersecurity internship programs, GovInfoSecurity reports. The planned 10-week summer internship, open to cybersecurity students who are attending or have just completed college and graduate school, will provide students with the opportunity to work with experts in cybersecurity, focusing on mission areas such as identification and analysis of malicious code, forensics analysis, incident response, intrusion detection and prevention, and software assurance.

-Russian anti-virus firm Kaspersky said last week that the number of smartphone threats has doubled in the past year, TG Daily writes. According to Kaspersky, at least 514 variants and 107 families of mobile malware were registered in August 2009. By the end of 2010 (14 months later), the number had jumped to 1,000 variants and 153 families - an increase of 94% and 44% respectively.

-U.S. Cyber Command is now up and running, InformationWeek reports. Cyber Command chief General Keith Alexander has outlined a series of next steps to be pursued by the six-month-old unit, including development of a "defensible architecture" that's better suited for the latest generation of cyber threats. Alexander identified five strategic priorities to be pursued by U.S. Cyber Command going forward, including the need to treat cyberspace as a "domain" within DoD; employ active cyber defenses and other new defense approaches; team with other federal agencies and the private sector on a national cybersecurity strategy; strengthen relationships with international partners; and recruit a cybersecurity workforce.

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.