GW CSPRI Newsletter

May 16, 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

-May 16, 10:30 a.m. - 12:00 noon, **Cybersecurity Roundtable: Protecting Small Businesses** - The Federal Communications Commission will host an event. The FCC will Webcast this event. Commission Meeting Room, 445 12th St., SW. More information.

-May 17, 6:30 p.m., **Secure Use of Cloud Computing** - This presentation will provide an overview of the Federal Chief Information Officer (FCIOC) Information Security and Identity Management Committee (ISIMC) Network and Infrastructure Security Subcommittee (NISSC) Guidelines for Secure Use of Cloud Computing by Federal Departments and Agencies, a document that presents a set of security guidelines and recommendations for using cloud computing technologies, capabilities and the selection

of deployment and service models. The featured speaker is Earl Crane, director, Cyberspace Strategy Division, U.S. Department of Homeland Security. Government Printing Office, Room A138, 732 N. Capitol St. RSVP and more information.

-May 17, 2:00 p.m., **Protecting Citizen Privacy: The Role of Government** - The Government Business Council will host a Webcast on a new study about how federal managers view privacy in the information age, where responsibility for assuring citizen data practices lies withing government agencies, and roadblocks to federal managers' control of citizen information. Presenters include **Priscilla M. Regan**, professor of government and politics and chair, Department of Public and International Affairs, George Mason University; and **Erin Dian Dumbacher**, associate director of research, Government Business Council. Registration and more information.

-May 19, 11:00 a.m. - 1:00 p.m.: The Department of Homeland Security's Data Privacy and Integrity Advisory Committee will meet by teleconference. More information.

-May 19, 1:00 - 2:00 p.m., **Cyberbullying** - The American Bar Association will host a Webcast panel discussion. More information.

-May 20, 9:00 a.m. - 1:00 p.m., **Cyberinfrastructure Framework for the 21st Century** - This is the second day of a two-day meeting of the National Science Foundation's Advisory Committee for Social, Behavioral and Economic Sciences. NSF, 4201 Wilson Boulevard, Stafford II, Room 555, Arlington. More information.

Announcements

-Student volunteers are needed to provide 3.5 hours of their time during the 2011 Computers, Freedom, and Privacy Conference at Georgetown University Law School. Volunteers are needed to assist with registration (Noon-5 June 13, and 8am-3pm June 14-16) and to attend presentations June 14-16 Noon-4:00 pm to provide logistical support (e.g. water for speakers, make sure AV systems are functioning, Internet access is operational, communicate problems to conference planners, or help direct attendees to workshops, tutorials, etc.)

Those who volunteer for 7 hours for the conference (any two 3.5 hour blocks of time) will be given full registration for the entire conference. If you can only volunteer for 3.5 hours you will have one day's conference registration, not including the day you will volunteer for the conference. Volunteers will be invited to an end of conference reception and be recognized in the program for the event.

Students interested in volunteering should email cfp2011@epic.org.

-The 21st annual Computers, Freedom and Privacy (CFP) 2011 conference will be held on June 14-16, 2011, at the Law Center, Georgetown University, in Washington DC. This conference engages multi-stakeholder experts from technology and policy. The meeting

will have the participation of government officials, the private sector, technologists, policymakers, activists and civil society for discussions about the information society and the future of technology, innovation, and freedom. Keynote speakers at the conference include Cameron Kerry, General Counsel Department of Commerce; Danah Boyd, Microsoft; Sami ben Gharbia, Global Voices; and Bruce Schneier, author and cyber security expert. The theme of CFP2011 (http://cfp.org/2011) is "The Future is Now." Panels scheduled so far include:

> The role of social media in the democracy movement in the Middle East and North Africa;
> A Clash of Civilizations: The EU and US Negotiate the Future of Privacy;
> Cybersecurity, Freedom and Privacy;
> The Global Challenge of Mandatory Data Retention Schemes.

Early registration ends May 20, 2011. Discounts for ACM members, academics, NGOs, and Government. Registration is at http://www.regonline.com/Register/Checkin.aspx?EventID=944943. Conference hotel rates end May 15, 2011 The conference hotel is the Hilton Washington Embassy Row, 2015 Massachusetts Avenue, NW, Washington, DC 20036, 800-695-7460 --- Request the room block for ACM June 14-16, 2011.

Legislative Lowdown

-**Rep. Cliff Stearns** (R-Fla.) last week introduced H.R. 1841, the Data Accountability and Trust Act, which would require entities that collect personal information from consumers to implement security policies to safeguard that data and notify affected consumers if it is breached, writes Ocala.com. The bill is in response to mounting bipartisan calls for national data-breach legislation to supersede the current patchwork of more than 40 state breach disclosure laws.

In the Senate, Commerce Committee **Chairman Jay Rockefeller** (D-W.Va.) and several colleagues wrote to the chairwoman of the Securities and Exchange Commission last week, arguing that firms should be forced to disclose cyber attacks that could affect earnings or give competitors a leg-up in the marketplace, The Hill writes.

Cyber Security Policy News

-A cyber security plan proposed by the Obama administration aims to protect individual privacy, federal computer networks and elements of national critical infrastructure. The proposal includes more stringent penalties for cyber criminals, including a mandatory three-year sentence for hackers who attack critical infrastructure targets. ; mandatory data breach reporting for organizations; placing the responsibility for defending federal agency networks from attack in the hands of the Department of Homeland Security; and improving protection for elements of the country's critical infrastructure.

-The U.S. Justice Department is asking for laws that would require domestic wireless carriers to retain subscriber location data that could be helpful in future criminal investigations in which a person's location is critical to solving a crime, InformationWeek reports. Ironically enough, the DOJ made the request at a hearing of the Senate Judiciary Committee panel hearing over concerns about iPhones storing location data without users' permission.

Meanwhile in Europe, the European Commission's advisory panel on data protection plans this week to urge governments in the European Union to treat the geographic location of cellphone users as personal data deserving of the highest level of privacy protection, The New York Times reports. The panel, which consists of 27 national regulators, plans to adopt the opinion on Friday, the Times notes.

-Federal officials in charge of warning the public in the event of major natural disaster or national security threat have been worrying for years about the waning number of citizens that still using regular telephone lines. In response, emergency alerts will soon come to certain wireless users by text message, according to The New York Times. Federal officials will announce this plan Tuesday, according to the article. Smartphone users will be able to access the alerts by sometime next year, which will require a software update.

-Security experts are warning about a dangerous new software security vulnerability present in many industrial control systems. The Industrial Control Systems Cyber Emergency Response Team issued an advisory last week warning of a flaw in "Iconics Genesis32" and "VizBiz" supervisory control and data acquisition (SCADA) products. The flaw, which lies in a specific component tied to the Microsoft Internet Explorer browser, could be exploited to remotely to allow the installation of malicious software, the group warned.

-Google is close to settling with the Department of Justice over allegations it made hundreds of millions of dollars by accepting ads from online pharmacies that violate U.S. laws, according to The Wall Street Journal. "The Internet company disclosed in a cryptic regulatory filing earlier this week that it was setting aside $500 million to potentially resolve a case with the Justice Department," wrote Thomas Catan and Amir Efrati. "The federal investigation has examined whether Google knowingly accepted ads from online pharmacies, based in Canada and elsewhere, that violated U.S. laws, according to the people familiar with the matter."

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.