GW CSPRI Newsletter

January 30, 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.

Cyber Security Scholarship Application Deadline is January 31

Each fall, approximately a dozen students pursue their bachelor's, master's, and doctoral degrees with federal funding from the National Science Foundation, the Defense Department, and the Department of Homeland Security. Federal funding provides two-year full scholarships (tuition, books, stipend, and in most cases room and board) for students to study computer security and information assurance at GW or a partner university. After completing their coursework, students will help protect the nation's information infrastructure by working as security experts in a government agency for two years. Since 2002, 56 students have graduated with help from this program, earning degrees in computer science, electrical engineering, engineering management, forensic sciences, business administration, and public policy. They have gone on to work at 36 governmental organizations.
To find out about the program and to apply (US citizens only), visit www.seas.gwu.edu/cybercorps.

Contents

Events

-Jan. 31, 10:00 a.m., The Subcommittee on Privacy, Technology and the Law will hold a hearing on the "Video Privacy Protection Act," focusing on protecting viewer privacy in the 21st century. Room 226, Dirksen Senate Office Building.More information.

-Feb. 1-3, **Information Security and Privacy Advisory Board Meeting** - Established by the Computer Security Act of 1987, the meeting of this board will examine a broad range of cybersecurity and privacy topics, including economic incentives for medical device cybersecurity, cloud services and data sovereignty, mobile security and information sharing. Residence Inn Washington, DC, 1199 Vermont Avenue NW. More information.

-Feb. 2, 9:00 a.m., **Social Security Administration's Death Records** - The House Committee on Ways and Means Subcommittee on Social Security will hold a hearing about the history, accuracy, use and impacts of the Death Master File along with options for change. The SSA is required to publish the surname, Social Security Number (SSN) and date of death of deceased SSN holders, but incorrect records have lead to financial hardships for many citizens, and easy access to the information has been a boon to identity thieves who use them to submit fraudulent tax returns. The hearing will examine how and if the requirements might be changed to address these problems. Room B-318 Rayburn House Office Building. More information.

-Feb. 2, 7:30 a.m. - 9:30 a.m., **Federal Cybersecurity: What's New in 2012** - Alan Paller, director of research for the Bethesda, Md. based SANS Institute discusses federal efforts to protect the nation from cyber-attacks on civilian, military and contractor databases. Ronald Reagan Building, 1300 Pennsylvania Avenue, NW, 8th Floor (North Tower), The Rotunda. More information.

Announcements

The Systems & Security Group at The George Washington University Computer Science Department is looking for scholars with a desire to advance the field of computer security. It has funded PhD and postdoctoral positions available starting in Fall 2012. The successful applicant will work with Prof. Michael Clarkson and the large cybersecurity community in DC to advance the state of the art in the scientific foundations of computer security. See http://faculty.cs.gwu.edu/~clarkson/positions.php for more information.

Legislative Lowdown

-Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.) said last week that he will take a look at the OPEN Act, an alternative to his highly controversial anti-piracy bill, the Protect IP Act, The Hill reports. Congressional leaders were forced to pull Leahy's Protect IP Act and its House counterpart, the Stop Online Piracy Act (SOPA), last week after a Web protest sparked an explosion of voter anger over the issue. Protect IP and SOPA would empower the Justice Department and copyright holders to demand that search engines delete links to foreign sites deemed “dedicated” to copyright infringement. Ad networks and payment processors would be prohibited from doing business with the sites. But critics of the legislation argue the bills would

stifle innovation and censor free speech. The alternative bill, OPEN, would authorize the U.S. International Trade Commission, rather than the Justice Department, to go after the foreign pirate sites. The bill focuses on a "follow the money" approach by aiming to cut off revenue to the websites instead of requiring other sites to delete links. The OPEN Act was introduced by the leading critics of Leahy's legislation.

For those who were unable to attend CSPRI's related debate last week "Resolved: The Internet's Domain Name System (DNS) Should Be Utilized to Try to Control Bad Behavior Such As Copyright and Trademark Infringement", the video of it should be up soon at the CSPRI website. A follow-on discussion ***"The End of K Street Deals?: Is Netizen Direct Lobbying the New Norm?"*** *will take place on Wednesday, February 15 at noon in GW's Marvin Center Room 302.*

Panelists will include:

> *Mitch Glazier, Senior Executive Vice President of the Recording Industry Association of America;*
>
> *Michael R. Nelson, Adjunct Professor, Internet Studies, CCT Georgetown University and Research Associate, CSC Leading Edge Forum;*
>
> *Dean Garfield, President and CEO of the Information Technology Industry Council; and*
>
> *Susan Aaronson, Associate Research Professor of International Affairs, George Washington University*

A web page with more details and a link to register will be up later this week.

Cyber Security Policy News

Last week marked the annual observance of Data Privacy Day, but the day came during a week full of an unusual number of developments that have privacy and security experts on edge.

For starters, the federal government's plan to expand computer security protections into critical parts of private industry is raising concerns that the move will threaten Americans' civil liberties, the Associated Press writes. The Constitution Project warned that as the Obama administration partners more with the energy, financial, communications and health care industries to monitor and protect networks, sensitive personal information of people who work for or communicate with those companies could be improperly or inadvertently disclosed. The group observed that while the government may have good intentions, it "runs the risk of establishing a program akin to wiretapping all network users' communications."

Also last week, Google is forging ahead with changes to its search engine and its privacy policy despite the risk of a crackdown by government regulators, The Hill writes. Earlier this month, Google began highlighting content from its social networking site Google+ in search results. Critics argue that by giving a preference to its own service over competitors like Facebook and

Twitter, Google ran afoul of antitrust laws that ban anticompetitive behavior. Rep. Edward Markey (D-Mass.) last week said he will ask the Federal Trade Commission (FTC) to probe whether Google's recent privacy changes violate the company's settlement with the agency.

Security and legal experts are warning that Internet privacy protections that the European Commission introduced this week could undermine American investigations into stateside data breaches, and pose serious complications for Internet companies doing business in Europe. The proposed rules, which focus on safeguarding data in the cloud, would require U.S.-based cloud computing providers with European Union customers to notify EU authorities of a data breach within 24 hours of detection. Speaking at a George Washington University Law School panel last week, AT&T's Chief Privacy Officer Bob Quinn called the proposed changes "unworkable." Meanwhile, many businesses are worried that the changes could result in costly burdens and large fines for errant companies, the Financial Times reports.

-President Obama uttered the term "cyber" only once in his 7,200-word State of the Union address last Tuesday night, but that fleeting moment about an hour into the speech could prove significant, writes GovInfoSecurity. The brief nod toward the need to pass comprehensive cybersecurity legislation "received scattered applause from the senators and representatives, not nearly as intense as other remarks the president gave. Still, the fact that Obama mentioned cyberthreats signals to Congress, the nation and the world that cybersecurity is an administration priority, though how much of a priority isn't clear," reporter Eric Chabrow writes.

In related news, Obama is directing the Departments of State and Homeland Security to develop a plan to protect the $14.6 trillion U.S. economy from interruptions in the international supply chain. The White House released last week a National Strategy for Global Supply Chain Security that gives officials from those departments six months to make recommendations on how to spot risks and make commercial infrastructure more resilient.

-The FBI has charged a former contractor at the Federal Reserve Bank with stealing the proprietary software code to a $9.5 million program. The Justice Department says Bo Zhang admitted he copied the Government-Wide Accounting and Reporting Program code onto his hard drive. He then allegedly used the program in his personal computer training business.

-A problem with Symantec's Veritas Storage Foundation software caused the shutdown of a clinical data repository that stores almost 10 million records for active-duty and retired military personnel and their families, according to NextGov. The Defense Information Systems Agency also acknowledged it played a key role when the AHLTA -- or Armed Forces Health Longitudinal Technology Application -- CDR shut down last week. The outage occurred during a technology upgrade at the site, when a fix for an issue in the previous version of operating system that powered the CDR wasn't included in the current CDR operating system.

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.