THE GEORGE WASHINGTON UNIVERSITY
CYBER SECURITY POLICY
AND RESEARCH INSTITUTE

Thoughtful Analysis of Cyber Security Issues

GW CSPRI Newsletter

January 17, 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

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.

Upcoming Events

-Jan 17-18, **State of the Net Conference** - The 7th annual State of the Net Conference will include featured discussions with Internet policy experts and panel tracks focusing on privacy, security, telecommunications regulation, and intellectual property. The conference will host keynote speakers including Congresswoman Marsha Blackburn, Congressman Bob Goodlatte, Dr. Ed Amoroso, Chief Cybersecurity Officer with AT&T and Tony Melone, Executive Vice President and Chief Technology Officer, Verizon. Hyatt Regency DC, 400 New Jersey Ave. NW. More information.

-Jan. 18, 10:00 a.m. - 12:00 noon, **Government Mandated DNS Blocking and Search Takedowns: Will It End the Internet as We Know It?** - The House Oversight and Government Reform Committee will hold a hearing. 2154 Rayburn House Office Building. More information.

-Jan. 19, 11:45 a.m., **Unintended Consequences of the Rogue Website Crackdown: SOPA, PIPA and OPEN Legislation** - A roundtable discussion featuring Larry Downes, senior adjunct fellow, TechFreedom, author, "The Laws of Disruption"; Julian Sanchez, research fellow, Cato Institute; James Gattuso, senior research fellow in regulatory policy, Heritage Foundation; Allan Friedman, research director, Center for Technology Innovation, Brookings Institution; and Dan Kaminsky, security researcher. Live streaming of the event will begin at 12:00 p.m. Reserve Officers Association of the United States, Minuteman Ballroom A&B, One Constitution Avenue, NE. More information.

-Jan. 25, 12 noon, **Debate--Resolved: The Internet's Domain Name System (DNS) Should be Utilized to Try to Control Bad Behavior Such as Copyright and Trademark Infringement** - A ten-minute warmup, "DNS addressing explained for non-techies," will start the event at noon, followed by the debate. Lunch will be provided at 1 p.m. to accompany a roundtable discussion. Please RSVP to lunch and/or the seminar at http://debateinternetdns.eventbrite.com. GW Marvin Center, 800 21st St. NW, Room 309. 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.

-Prof. Michael Clarkson (GW Computer Science) has been awarded an Air Force Office of Scientific Research Young Investigator Research Award for his research proposal, “Making Cybersecurity Quantifiable.” The objective of this three-year, $610,000 grant is to make it possible to quantify, and consequently to compare, the security of computing systems. Instead of merely declaring a system to be secure or not, Prof. Clarkson seeks to enable measurement of security. His work will focus on constructing mathematical models and metrics for cybersecurity in three important areas: privacy, access control, and availability.

Cyber Security Policy News

-On Saturday, the White House outlined its opposition to two similar bills pending in the House and Senate that would crack down on the sale of pirated American movies, music and other goods on foreign-based websites, the Wall Street Journal reports. The bills would require Internet companies to hobble access to foreign pirate websites, bar search engines from linking to them and prevent U.S. companies from placing ads on them.

The measures have generated unprecedented pushback from technology firms and privacy and security experts, who claim the approach could hurt innocent companies and undermine cybersecurity. A number of groups have promised high-profile demonstrations against the measures: Wikipedia is expected to go dark on Jan. 18 in protest, as are tech-heavy news aggregation sites Reddit and BoingBoing.

In response, the lead sponsor of the House measure, Rep. Lamar Smith (R-Texas), said he would remove a major provision of his bill that would force changes to internet infrastructure to fight online copyright and trademark infringement, writes Wired.com. The announcement from the chairman of the House Judiciary Committee came a day after Sen. Patrick Leahy (D-Vt.), the main sponsor of similar legislation in the Senate, announced the same move. For the time being, that means if the bills become law, ISPs won’t have to perform DNS redirecting of sites the attorney general concludes are facilitating online copyright and trademark infringement.

-The Defense Department intends to beef up spending on computer network protections and satellite intelligence systems while targeting troops for cuts under a global strategy released last week. Funding levels, which were not specified, will be detailed in next month’s federal budget proposal. The Washington Post reports that the plans may ease the blow for defense contractors such as Northrop Grumman and Lockheed Martin that are facing cuts in other programs.

-Privacy advocates are calling on the Federal Trade Commission to initiate an investigation into whether Facebook's new "Timeline" feature is legal. In a letter to the FTC, the Electronic Privacy Information Center warned that "with Timeline, Facebook has once again taken control over the user's data from the user and has now made information that was essentially archived and inaccessible widely available without the consent of the user." As The Hill notes, EPIC says Timeline might violate a settlement that Facebook reached with the FTC last year. In that agreement, Facebook settled charges with the FTC in November that it failed to follow its own privacy policies. The FTC complaint accused Facebook of sharing its users’ personal information with advertisers and changing its privacy policies without obtaining its users' consent.

-The Department of Energy and the Department of Defense have teamed up to create a cybersecurity model that can be tested and applied across the utility industry to provide insight into how to better protect the U.S. electricity grid, Dark Reading reports. The Electric Sector Cybersecurity Risk Management Maturity Model pilot project aims to work with experts in both the public and private sector to use existing cybersecurity strategies to develop a so-called "maturity model" that can identify how secure the electricity grid currently is from cyber threats, according to a White House blog post by White House cybersecurity coordinator Howard Schmidt. It will then test that model with participating utility companies to see how well it works, Schmidt said. The initiative was outlined by the White House last week.

-Internet policymakers are moving forward a plan to dramatically expand the number of new top-level domains for Web sites, despite warnings that doing so could pose a significant threat to consumers, PCWorld writes. The Internet Corporation for Assigned Names and Numbers (ICANN) will open up applications for new generic top-level domains this week, even with continued objections to the plan, the group's CEO said. In a letter to ICANN last month, the Federal Trade Commission urged the group to table the plan. The commission worried that under ICANN's plan, “ABC Bank” could have the website “ABC.com,” but a scammer could set up “ABC.bank,” and another scammer could set up “ABC.finance” ad infinitum.

-The United States last week expelled the Venezuelan diplomat who last month was implicated in an alleged Iranian plot to launch cyber attacks against nuclear power plants. The diplomat, Livia Antonieta Acosta Noguera, is currently Venezuela's consul in Miami. The State Department on Sunday said it has declared the diplomat persona non grata and that it had notified the Venezuelan government of the decision on Friday that it was investigating a "very disturbing" report that implicates a U.S.-based Venezuelan diplomat in an alleged Iranian plot to launch cyber attacks against U.S. nuclear plants. Livia Antonieta Acosta Noguera, currently Venezuela's consul in Miami, Florida, is described in a report by New York-based Hispanic television network Univision as an accomplice in the plot.

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.