GW CSPRI Newsletter

October 9, 2012

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.

Events

-Oct. 9, 1:00 - 2:00 p.m., **Privacy and Information Security Update** - The American Bar Association will host a free webcast and teleconferenced panel discussion. The speakers include Alysa Hutnik, Christopher Loeffler, Sharon Schiavetti and Kristin McPartland, all from the law firm Kelley Drye. More information (PDF).

-Oct. 9, 12:15 - 1:45 p.m., **It's Science and Technology Policy, Stupid** - The New America Foundation will host a panel discussion. The speakers will be Stacy Cline, Republican staff, Senate Health, Education, Labor, and Pensions Committee; Sheri Fink, Konstantin Kakaes, Amanda Ripley, and Robert Wright, from NAF. 1899 L St., NW. More information.

-Oct. 10, 9:30 a.m. - 4:00 p.m.. The Department of Commerce's (DOC) National Telecommunications and Information Administration (NTIA) will hold one in a series of meetings regarding consumer data privacy in the context of mobile applications. Auditorium, Dept. of Commerce, Hoover Building, 14th Street and Constitution Ave., NW. More information.

-Oct. 10, 10:00 a.m. - 11:00 a.m., **Creating Strong Passwords That You Don't Have to Memorize** - The George Washington University will observe National Cyber Security Awareness Month with a primer on password security. Attendees are asked to please bring a laptop connected to GWIX and a pen or pencil. Marvin Center 413/414.

-Oct. 10-12: A 3-day meeting of the National Institute of Standards and Technology's Information Security and Privacy Advisory Board. Courtyard Washington Embassy Row, General Scott Room, 1600 Rhode Island Ave., NW. More information.

-Oct. 15-16, **2nd Annual Cyber Security Finance Forum** - CSFF features combination of expert panels, individual company presentations and networking breaks that focus on the

opportunities, challenges and issues that need to be understood to succeed in the cyber security sector. 1777 F St. NW. More information.

-Oct. 16, **Nuclear Regulatory Commission Cyber Security Conference** - The Nuclear Regulatory Commission is hosting a Cyber Security Conference on October 16, 2012 in Rockville Maryland. This 1-Day Conference will consist of Cyber Sessions in the NRC Auditorium given by government and industry speakers. NRC Auditorium 11545 Rockville Pike Rockville, MD 20852. More information.

-Oct. 16-17, The Cyber Maryland Conference - A two-day conference that includes 28 sessions in three tracks, a cybersecurity showcase and expo, and the national cybersecurity hall of fame inaugural induction ceremony and awards banquet. Baltimore Convention Center, One West Pratt Street, Baltimore, MD 21201. More information.

-Oct. 17, 10:00 a.m. - 11:30 a.m., **Why Should You Care About Protecting Your Privacy and Identity in Cyberspace?** - This panel discussion, hosted by GWU, will include: Dr. Daniel J. Solove, John Marshall Harlan research professor of law, GW Law School; Darrell Darnell, GW senior associate vice president for safety and security; Danielle Lico, GW associate dean of students for student administrative services and senior advisor to the dean; Ashwin Narla, president, GW Student Association; Benjamin Fielden, manager of student technology services, Division of IT. The discussion will be moderated by Dennis Devlin, assistant vice president of information security & compliance services, Division of IT. Jacob Burns Moot Court Room (2000 H Street, NW).

Legislative Lowdown

-An draft executive order from the White House to beef up cybersecurity at some of the nation's most vital information assets is coming under fire from several sides, even as the Obama administration is reaching out for feedback from industry groups most likely to be impacted by the order. The administration floated the idea of an executive order on cybersecurity late last month, after the Cyber Security Act stalled in the Senate. A draft of the order obtained by the Associated Press picks up many of the Cyber Security Act’s pieces, from protections placed on vital infrastructure systems (the definition of which proved a sticking point for the Senate proposal), voluntary standards for private companies, and a Homeland Security Department council with representatives from various departments to assess and report on cyber security threats.
But according to The Los Angeles Times, the idea is now meeting with resistance from key Republicans, including Sen. Susan Collins (R-Maine), who along with Sen. Joe Lieberman (I-Conn.) initially proposed the Cyber Security Act of 2012. "The executive order is a big mistake. First of all, the executive order cannot grant the liability protections that are needed in order to encourage more participation by the private sector, so the executive order simply cannot accomplish what legislation can," Collins said during a discussion at the Wilson Center in Washington, D.C., on Monday. "In addition, an executive order is not lasting, and it doesn’t reflect a consensus by Congress on what should be done." To top it off, a contingent of Republican senators, including John McCain (R-Ariz.), Saxby Chambliss (R-Ga.) and Kay

Bailey Hutchison (R-Texas), sent a letter to Obama on Tuesday asking for the president to work through Congress, not the White House, to improve cyber security protocols, The Times reports. At the same time, House Intelligence Committee Chairman Mike Rogers (R-Mich.) blasted the White House on Thursday for failing to consult with him on a potential executive order to enhance cybersecurity, The Hill's Brendan Sasso writes. "I don't get it. I don't understand it," Rogers said at a cybersecurity summit at the Chamber of Commerce headquarters. "I think it's irresponsible." Rogers argued that his committee researched cybersecurity issues for two years and that administration officials should seek the input and expertise of congressional Republicans. He also charged that the White House has failed to reach out to the business community. Not so, says the White House. The White House claims it is reaching out to the private sector and Congress for input on a potential executive order designed to boost cybersecurity, National Journal reports. National Security Council spokeswoman Caitlin Hayden said in an e-mailed statement on Friday that the order is still being developed. "The process of developing an Executive Order will take time, as we believe that it must take into account the views of our partners in the private sector and the Congress," she said.

Cyber Security Policy News

-A report to be released this week by a House of Representatives panel will recommended that U.S. companies avoid doing business with ZTE or Huawei, two of China's largest hi-tech firms. According a draft of the report, obtained by the National Journal, the assessment said that a nearly year-long review of the issue by the House Intelligence Committee was met with a lack of cooperation and "inadequate and unclear" answers from the companies. "Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems." It also calls for Congress to block any mergers or other acquisitions by the companies in the U.S. The Journal writes that both Huawei and ZTE are hoping that public relations campaigns will help overcome what their executives say are "myth and innuendo" they see as coming from the committee. Huawei has run ads in Politico's Playbook, for example, and ZTE has brought on the PR firm of Ogilvy. But the committee's report explicitly rejected the companies' main policy suggestion: to have third-party auditors ensure the security of all devices and software sold in the U.S.

-An international gang of cyber crooks is plotting a major campaign to steal money from the online accounts of thousands of consumers at 30 or more major U.S. banks, security firm RSA warned. In an advisory Thursday, RSA said it has information suggesting the gang plans to unleash a little-known Trojan program to infiltrate computers belonging to U.S. banking customers and to use the hijacked machines to initiate fraudulent wire transfers from their accounts. Computerworld writes that, if successful, the effort could turn out to be one of the largest organized banking-Trojan operations to date, Mor Ahuvia, cybercrime communications specialist with RSA's FraudAction team, said today. The gang is now recruiting about 100 botmasters, each of whom would be responsible for carrying out Trojan attacks against U.S. banking customers in return for a share of the loot.
In a related post following up on the RSA report, independent investigative reporter Brian Krebs delved deeper into the proposed collaborative effort, which the fraudsters orchestrating the

scheme are calling "Project Blitzkrieg." The first part of the piece attempts to gauge the underground community's reactions to the project, which so far has been mostly suspicion and skepticism. The latter half of the story examines a service offering in the cyber underground that is marketed as an insurance scheme to help hackers in Russia and Eastern Europe bribe their way out of criminal charges for cybercrime. Such services may go a long way toward explaining why U.S. law enforcement agencies often have trouble obtaining cooperation from authorities in those regions.

-Acting on a Federal Trade Commission complaint, a federal court has imposed a $163 million judgment on a woman who allegedly helped run a scareware ring that tricked over one million consumers across six countries into purchasing fake security software. That decision, announced by the FTC Tuesday, came after a two-day bench trial last month. U.S. District Judge Richard D. Bennett, who presided over the case, also wrote in his related judgment that the defendant, Kristy Ross, "shall be permanently restrained and enjoined from the marketing and sale of computer security software and software that interferes with consumers' computer use as well as from engaging in any form of deceptive marketing." The fake software in question--often referred to as scareware, fake antivirus, or fake AV--is part a social-engineering scam designed to trick users into thinking their PC contains viruses, system errors, spyware, or pornography. The software then advertises information security software to help, which is available for immediate download. But in reality, the results of the system scan, as well as security software's cleaning power, is fake.
-Many of the country's largest companies lashed out at Microsoft this week, claiming that its decision to turn on the "Do Not Track" privacy feature in Internet Explorer 10 would "harm consumers, hurt competition, and undermine American innovation." In a letter addressed to three top Microsoft executives, including CEO Steve Ballmer and the company's top lawyer, Brad Smith, companies ranging from McDonalds and General Motors to Intel and Visa demanded a sit-down with Microsoft to discuss Internet Explorer 10 (IE10). Computerworld writes that IE10 is slated to ship alongside the Windows 8 operating system on Oct. 26. Although Microsoft has promised to also release a version of the browser suitable for Windows 7, it has consistently refused to give a timetable.

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.