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

GW CSPRI Newsletter

June 13, 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

-June 13, **Getting IT Right: Protecting Patient Privacy in a Wired World** - A public forum to discuss the future of health privacy in the digital age. Georgetown Law Center, 600 New Jersey Ave., NW. More information.

-June 14-15, **The Workshop on the Economics of Information Security** - Prior workshops have explored the role of incentives between attackers and defenders, identified market failures dogging Internet security, and assessed investments in cyber-defense. This workshop will build on past efforts using empirical and analytic tools to not only understand threats, but also strengthen security through novel evaluations of available solutions. George Mason University, Fairfax Campus, Mason Inn Conference

Center and Hotel, 4352 Mason Pond Drive, Fairfax, Va. More information and registration.

-June 14-16, **Association for Computing Machinery's "Computers, Freedom, and Privacy" Conference** - The theme of the 21st annual conference is Computers Freedom and Privacy: "The Future is Now." Georgetown University Law Center (Hart Auditorium), 600 New Jersey Avenue NW. More information.

-June 16, 8:00 a.m. - 5:00 p.m., **Workshop on Cybersecurity Incentives** - This workshop will discuss the history, present, and future of societal mechanisms and institutional designs that leverage incentives to bring an acceptable balance between security and other priorities in cyberspace. The agenda will focus on illustrating cyberspace as an ecosystem of actors and discuss their roles and responsibilities, and the dynamics of their interaction and interconnectivity. Scholarship in law, economics and other fields within the behavioral sciences inform stakeholders about how markets, incentives and legal rules affect each other and shed light on determinations of liability and responsibility. George Mason University, Fairfax Campus, Mason Inn Conference Center and Hotel, 4352 Mason Pond Drive, Fairfax, Va. More information.

-June 16, 7:30 a.m. - 10:30 a.m., **Defending the Digital Infrastructure: Building Trust through Public/Private Partnerships** - Ronald Reagan Building ~ Hemisphere Suite A 1300 Pennsylvania Avenue, NW. More information.

-June 20-23, **Gartner Security & Risk Management Summit** - Topics to be covered include governance risk compliance; cloud computing and recovery; security architecture; mobile applications and security; and security threats and vulnerabilities. Gaylord National, 201 Waterfront Street, National Harbor, MD. More information.

-June 21, 7:30 a.m. - 9:30 a.m., **Will 2011 be the Year of Cyber? -** Join a panel of federal cyber experts on June 21 to explore the changing federal landscape. What are the White House cyber bill's chances of passage? How are CIOs partnering with CISOs to lead federal cyber strategy? What new measures are being used to gauge the effectiveness of agencies' efforts? Speakers include **John Gilligan**, former chief information officer for the U.S. Air Force and **Tommy Ross**, senior defense and intelligence adviser, Sen. Harry Reid (D-Nev.). Ronald Reagan Building ~ The Rotunda 8th Floor (North Tower)?1300 Pennsylvania Avenue, NW. More information.

-June 21, 8:30 a.m. - 11:00 a.m., **Controlling Cyber Conflict? Arms Control, International Norms, and Strategic Restraint** - This panel discussion brings together expert panelists to discuss and explore how cyber conflict can be mitigated. Is the cyberspace domain amenable to arms control solutions, and what would such solutions look like, or are the development of international norms more appropriate? Speakers include Prof. Martha Finnemore, George Washington University; Robert J. Butler, deputy assistant secretary of defense for cyber policy, Office of the Secretary of Defense; James A. Mulvenon, Defense Group Inc.; Christopher A. Ford, Hudson Institute. National Press Club, 529 14th St. NW, 13th Floor. More information.

-June 23, 7:45 a.m. - 9:30 a.m., **NERC: Cyber Status, Trends and the Future - Mark Weatherford**, vice president and chief security officer of the North American Electric Reliability Corporation (NERC), will discuss cybersecurity trends as they relate to the bulk power system, the current cyber threat landscape, the status of ongoing NERC efforts and recent initiatives, and legislative matters related to NERC's activities. ICF International, 1725 Eye St NW, Suite 1000. More information.

Legislative Lowdown

-A bill drafted by **Rep. Jason Chaffetz** (R-Utah) and **Sen. Ron Wyden** (D-Ore.) would make it a crime to intercept or disclose an individual's location data and require a warrant for government to obtain that information, NexGov writes. The Geolocational Surveillance and Privacy Act would prohibit police and federal law enforcement from tracking citizens' location through cellphones, GPS devices and other electronic items without first getting a warrant, according to a draft version of the bill provided by Chaffetz's office.

-Senate Judiciary chairman Patrick Leahy re-introduced a bill Tuesday that would establish a national standard for data breach reporting and make it a crime to conceal a data breach that could result in financial harm to consumers. According to The Hill, the legislation would make it a crime to intentionally conceal a data breach that could cause economic damage to consumers, punishable by up to five years in jail. The bill would require data brokers to disclose to consumers what sensitive personal information they have about them and allow consumers to make corrections to that data.

Cyber Security Policy News

-**The International Monetary Fund** was hit by what experts described as a large and sophisticated cyberattack whose dimensions are still unknown, *The New York Times* reported Saturday. Several senior officials with knowledge of the attack said it was both sophisticated and serious. “This was a very major breach,” said one official, who said that it had occurred over the last several months, even before Dominique Strauss-Kahn, the French politician who ran the fund, was arrested on charges of sexually assaulting a chambermaid in a New York hotel.

-Citigroup Inc. suffered a cyber attack on its systems last week, when hackers managed to break into the company's network and get data on roughly 200,000 credit-card holders in North America, Reuters reports. The Citigroup breach is the largest direct attack on a major U.S. bank to date, security experts said. It has already prompted banking regulator **Sheila Bair** to call on banks to "strengthen their authentication when a customer logs onto online accounts."

-Defense contractor **Lockheed Martin** has confirmed that a recent attack on its network was aided by the theft of confidential data relating to RSA SecurID tokens employees use

to access sensitive corporate and government computer systems. Lockheed Martin said last week that it had proof that hackers breached its network two weeks ago partly by using data stolen from a vendor that supplies coded security tokens to tens of millions of computer users. In a note to its customers last week, RSA said it would expand a program to help customers replace their SecurID tokens. A spokesman for the company said it would consider the cost of replacing those tokens on a case-by-case basis.

-**Facebook** stoked fresh concerns from privacy advocates and lawmakers in the U.S. and Europe by rolling out technology that uses facial recognition to identify people in photos on its website, according to The Wall Street Journal. The technology was designed to help Facebook users mark friends in photos as they upload them to the social-networking site. Facebook first introduced the tool to U.S. users in December, and added it to most of the rest of the world this week, prompting privacy officials in Europe to open investigations. The company said the face-recognition tool is enabled for all users by default.

-Public companies must disclose cyber attacks or risk factors that may be relevant to investors, according to Securities and Exchange Commission chairman **Mary Schapiro**, The Hill reports. The SEC chief responded this week to a letter last month from Senate Commerce chairman **Jay Rockefeller** (D-W.Va.) and several Senate Democrats asking the SEC to clarify that firms must disclose any network breach that could jeopardize the firm's intellectual property or trade secrets.

-The United States and foreign countries should broker a code of conduct for offensive cyber actions that bans knocking out banking, power, and other critical infrastructure networks except when nations are engaged in war, writes NexGov. Their recommendation follows the White House's release of an international cybersecurity doctrine that states the country "will respond to hostile acts in cyberspace as we would to any other threat to our country" and "use all necessary means . . . in order to defend our nation." In recent years, the sophistication of network attacks has sparked debate about the nature of cyberwar -- specifically over those "means" and how they should be deployed.

-A closely-watched court battle over how far commercial banks need to go to protect their customers from cyber theft is nearing an end. Experts said the decision recommended by a magistrate last week — if adopted by a U.S. district court in Maine — will make it more difficult for other victim businesses to challenge the effectiveness of security measures employed by their banks. The court laid out what experts said would be the first legal precedent defining what constitutes "commercially reasonable" security for commercial online transactions. The 2005 guidance from banking regulators said banks should employ "multi-factor authentication," including two of the three following components: Something the customer has (a token), something they know (as password), and/or something the user is (a biometric component). This case would be the first to add legal precedent to banking industry guidelines about what constitutes 'reasonable' security. The tentative decision is that a series of passwords + some device fingerprinting is enough to meet the definition of 'something you know' + 'something you have.' The

case has generated enormous discussion over whether the industry's 'recommended' practices are anywhere near relevant to today's attacks, in which crooks usually have complete control over the victim's PC.

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.