GW CSPRI Newsletter

December 3, 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.

Contents

Events

-Dec. 4, 1:00 p.m. - 2:30 p.m., **Building or Sabotaging the Enterprise? Squaring Cyber Security with Technologies that Undermine It** - The American Bar Association will host a webcast and teleconferenced panel discussion. The speakers will be James Bryce Clark, general counsel, Oasis; Charles Palmer, CTO security and privacy, IBM Research; and Candace Jones, counsel and assistant vice president, Federal Reserve Bank of New York. More information.

-Dec. 4, 2:30 p.m. - 3:30 p.m., **Internet Caucus Meeting on Security and Privacy** - The Internet Caucus will host an event at which Alexander Alvaro, vice president of the European Parliament, will speak regarding privacy and security. 1634 I St., NW. More information.

-Dec. 5, 12 noon - 1:00 p.m., **Software Security Growth Modeling** - Security growth modeling, analogous to reliability growth modeling, is an attempt to quantify how the projected security of a system increases with additional detection and removal of software vulnerabilities. Such insights would be crucial in allocating development and assurance resources, as well as making informed release or revision decisions. This Webcast presentation will review assumptions and limitations in such an approach and suggest how it could improve data-driven security management. More information.

-Dec. 5, 1:00 p.m., **Nine Critical Threats Against Mobile Workers** - In this Webinar, FS-ISAC and Marble Cloud look at the 9 critical security threats that are effecting mobile workers today, and the solutions businesses can implement to ensure they're protected. More information.

-Dec. 6, 8:15 a.m. - 3:30 p.m., **Can Trade Policies and Agreements Advance Internet Freedom?** - The Computer and Communications Industry Association and George Washington University's Institute for International Economic Policy will host an event. The discussion is free and open to the public. GWU, Elliot School of International Affairs, Lindner Commons, 6th floor, 1957 E St., NW. More information.

-Dec. 6, 12:00 noon - 2:00 p.m., **Private Attorneys and the War on Terror** - The Federalist Society will host a luncheon and panel discussion on the role of private sector attorneys in the War on Terror. The speakers will include Nitsana Darshan-Leitner, director and founder, Shurat HaDin – Israel Law Center; Steven G. Bradbury, partner, Dechert LLP; and Stephen I. Vladeck, American University Washington College of Law. National Press Club, 13th Floor, 529 14th St., NW. More information.

-Dec. 7-16, **SANS Cyber Defense Initiative 2012** - This event will feature more than 25 courses in IT security, security management, IT audit, software developer, and computer forensics. Hilton Washington, 1919 Connecticut Avenue, NW. More information.

-Dec. 10, 7:00 p.m. - 10:00 p.m., **NoVA Hackers Association Meetup** - This informal group from around the NoVA/DC area coordinates one or two monthly events – an evening meetup with presentations on cybersecurity on the second Monday of the month and various lunch or bar meetup. Champps Americana Bar & Grill, 11091 Sunset Hills Road, Reston, VA. More information.

-Dec. 11-13, **6th Annual Conference on Security Analysis and Risk Management** - This year's conference theme is "Professionalizing Security Risk Management." Specific subject areas will include the following: Community risk, critical infrastructure risk, and cybersecurity risk. George Mason University - Arlington Campus, Founders Hall, 3351 Fairfax Drive, Arlington, Va. More information.

-Dec. 12, 11:00 a.m. - 4:00 p.m., **ISACA Central Maryland Chapter Meeting** - The ISACA Central Maryland Chapter invites you to our annual joint training holiday event with the Associate of Government Accountants (AGA) on Wednesday, December 12, 2012. There are two topics for this training event: Governance and Risk in Cloud Computing and Achieving Data Warehouse Nirvana: The Critical Role of Information Controls. Snyders Willow Grove Restaurant, 841 North Hammonds Ferry Road, Linthicum, MD, United States. More information.

Legislative Lowdown

-The Senate Judiciary Committee took a step on Thursday toward updating the nation's outdated laws related to when law enforcement and other government agencies can access e-mail and other electronic communications, The National Journal reports. As part of legislation to modernize the Video Privacy Protection Act, the committee attached provisions that would update the 1986 Electronic Communications Privacy Act. Senate Judiciary Chairman Patrick Leahy, D-Vt., acknowledged that the bill is unlikely to pass Congress before the end of the year but said it would help advance work on the issue in the 113th Congress.

The Electronic Privacy Information Center (EPIC) notes that the bill generally requires law enforcement to obtain a warrant before accessing email or other electronic communications and allows for blanket consent of video viewing information. An amendment by Senator Feinstein, adopted by the Committee, limited the opt-in to two years or till whenever the user withdraws consent.

-Sen. Leahy's committee is expected to mark up another important privacy bill at 10:00 a.m., Dec. 6, when the Senate Judiciary Committee is expected to consider S. 1223, the "Location Privacy Protection Act of 2011", sponsored by Sen. Al Franken (D-Minn.). The meeting will be held in Room 226 of the Senate Dirksen Office Building.

Cyber Security Policy News

-Amid intensified armed skirmishes in Syria, more than 90% of the Internet access in that nation was shut down late last week, according to the Internet monitoring group Renesys. It was not clear who was behind the latest event, but the government has intermittently cut off Internet access several times in the past two years, CNN reported. Renesys also posted a thought-provoking analysis showing how easy it would be for other nations to hit the Internet kill switch inside their borders.

-The United Nations' International Atomic Energy Agency has admitted that data from a retired server at its Vienna headquarters was stolen and posted to a hacker website, Ars Technica reports. A group calling itself Parastoo allegedly stole the data in an effort to draw attention to Israel's nuclear weapons program and as a protest against attacks on Iran's nuclear efforts—including the use of the Stuxnet worm and assassinations of Iranian nuclear researchers. IAEA spokeswoman Gill Tudor told Reuters that the server the data was stolen from was "an old server that was shut down some time ago," and that the agency regretted the breach.

-In a case watched closely by banks and their commercial customers, a financial institution in Maine has agreed to reimburse a construction company $345,000 that was lost to hackers after a court ruled that the bank’s security practices were "commercially unreasonable," Wired.com reports. People’s United Bank has agreed to pay Patco Construction Company all the money it lost to hackers in 2009, plus about $45,000 in interest, after intruders installed malware on Patco’s computers and stole its banking credentials to siphon money from its account. Patco had argued that the bank’s authentication system was inadequate and that it failed to contact the customer after its automated system flagged the transactions as suspicious. But the bank maintained that it had done due diligence because it verified that the ID and password used for the transactions were authentic.

-Military cybersecurity experts this month will undertake a mission to protect the six-foot-by-eight-foot NetWars CyberCity scale model just off the Jersey Turnpike that has its own hospital, cybercafe, bank, and power plant, from its first round of cyberattacks, Dark Reading's Kelly Jackson Higgins reports. CyberCity is the brainchild of Ed Skoudis, director of NetWars CyberCity and an instructor with SANS, which runs the newly constructed, small-scale city that on the surface looks more like a hobbyist's collector's item. The goal of the project is to help the military's so-called "cyberwarriors" simulate how cyberattacks affect both the logical and physical worlds.

- The number of Americans whose identities have been stolen for the purpose of filing fraudulent tax returns has risen exponentially in just the last several years. But the IRS' tight budgets and inefficient business resources have stymied its efforts to fight the problem. According to Federal News Radio, in 2008, there were 51,700 confirmed cases of tax-refund identity theft in the United States. By 2011, the number was 1.1 million, and those are just the cases the IRS knows about. An audit by the Treasury Inspector General for Tax Administration (TIGTA) earlier this year estimated another 1.5 million potential cases in which thieves stole identities for the purpose of getting fraudulent refunds. And IRS could give out $21 billion dollars in fraudulent refunds in just the next five years if the agency doesn't find a way to crack down, TIGTA found.

- Earlier this month, a federal judge held that the Fourth Amendment does not prevent the police from using tracking software to determine the location of a person who is tapping into an unsecured Wi-Fi connection, the Inside Privacy blog writes. In 2010, a Pennsylvania state police officer began investigating distribution of child pornography over a peer-to-peer file-sharing network. The officer traced the IP address of one distributor to a home in Allegheny County. The officer obtained a warrant and searched the residence, but he did not find any evidence of child pornography. Because the home’s Wi-Fi connection was unsecured, the officer suspected that the child pornography distributor was using the home’s Wi-Fi connection for its activities and thus was located nearby. The resident agreed to cooperate with police to identify the person who was accessing and using his Internet connection.

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.