GW CSPRI Newsletter

June 23, 2014

From the **Cyber Security Policy and Research Institute** of **The George Washington University**, www.cspri.seas.gwu.edu.

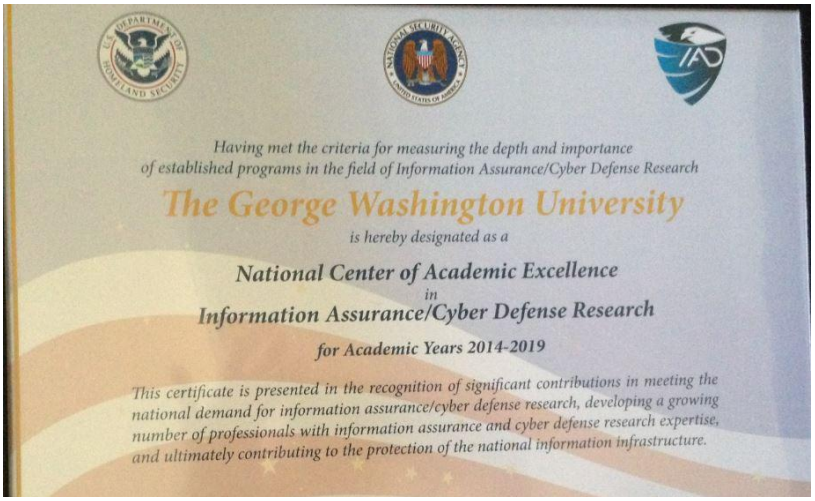
This newsletter is a weekly summary of events related to cyber security policy and research, with a special focus on developments and events in the Washington, DC area.

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

Announcements

CSPRI Director, Dr. Lance Hoffman traveled to the CISSE conference in San Diego, CA to accept GWU's extension to 2019 as a National Center of Academic Excellence in Information Assurance/Cyber Defense Research (CAE-R).



Events

-June 23-26, **Gartner Security Risk and Management Summit** – A look into the full spectrum of security and risk management emerging trends and market scopes within five role-based programs and a dedicated technical insights track. This year's summit features new coverage on chief information security officer (CISO) programs; risk management and compliance; and business continuity management. Gaylord National, 201 Waterfront Street, National Harbor, MD 20745. More information.

-June 24-25, **Cyber Awakening: Protecting a Nation's Security** – The AFCEA Cyber Symposium will explore the aspects of operational security of U.S. Government, DoD and industry networks, cyber cooperation among joint and coalition partners, and discuss the training and development of the cyber workforce. Baltimore Convention Center, 1 W Pratt St, Baltimore, MD 21201. More information.

-June 24, 10:00 a.m. - 11:30 a.m., **The Future of Global Technology, Privacy, and Regulation** - The Brookings Institution will host a speech by Microsoft's General Counsel Brad Smith. The event will be Webcast. Free. Open to the public. 1775 Massachusetts Ave., NW. More information.

-June 24, 1:00 p.m. - 5:00 p.m., **Privacy and Facial Recognition Technology** - The Department of Commerce's National Telecommunications and Information Administration (NTIA) will host one of its series of meetings. American Institute of Architects, 1735 New York Ave., NW. More information.

-June 25, 11:00 a.m., **How Data Mining Threatens Student Privacy** - The House Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will hold a hearing. Room 311, Cannon Building. More information.

-June 25, 5:00 p.m. – 7:00 p.m., **ISSA Baltimore Meetup: Inside an IT Outsourcing from the Perspective of a Service Provider's Security, Audit, and Risk Professional** - Professionals in information security, audit, risk, and internal control, and their Managers, will benefit from this event. Parsons, 7110 Samuel Morse Drive, Suite 200, Columbia, MD, 21046. More information.

-June 25, 7:00 p.m. – 10:00 p.m., **CharmSec Meetup** – CharmSec is an informal, all-ages, citysec-style meetup of information security professionals in Baltimore. Heavy Seas Alehouse, 1300 Bank Street, Baltimore, MD, 21231. More information.

Legislative Lowdown

-A bill that would require the government to obtain a search warrant to rifle through people's emails and other online communications now has majority support in the House

of Representatives, according to Computerworld. The Email Privacy Act now has 218 co-sponsors -- the number needed for the bill to pass if it is brought up for a vote in the House. Under existing law, police and federal law enforcement can often gain access to citizen emails stored by a third part without a warrant. “Cloud providers and other technology vendors have been pushing for changes to how the government can ask for customer data amid signs that the Snowden revelations have scared some overseas customers away,” writes Jaikumar Vijayan. “The proposed Email Privacy Act would amend ECPA to prohibit a third-party service provider from divulging a customer's communication records to law enforcement officials without a warrant obtained under the Federal Rules of Criminal Procedure or state warrant procedures.”

At the same time, the federal court overseeing the country’s spy agencies renewed an order Friday allowing the National Security Agency to collect phone records of people in the United States, reports The Hill. “Some privacy advocates have urged the Obama administration not to ask for reauthorization while Congress debates a measure to effectively end the program,” writes Julian Hattem. “Administration officials have said that the program is necessary to track terrorists and foreign agents and have rejected calls to end or significantly reform the program without legislation from Congress.”

Cyber Security Policy News

- UK intelligence service GCHQ can legally snoop on British use of Google, Facebook and web-based email without specific warrants because the firms are based abroad, the BCC reports. Classified as "external communications", such activity can be covered by a broad warrant and intercepted without extra clearance, the BBC quotes GCHQ Chief Charles Farr. It is the first time the UK has commented on how its legal framework allows the mass interception of communications, as outlined by US whistleblower Edward Snowden in his leaks about global government surveillance. “Facebook, Twitter, YouTube and web searches on Google - as well as webmail services such as Hotmail and Yahoo - were classified as ‘external communications’, which meant they could be intercepted without the need for additional legal clearance,” the BBC writes. “It is the first time the UK has commented on how its legal framework allows the mass interception of communications, as outlined by US whistleblower Edward Snowden in his leaks about global government surveillance.”

Like the United States, Canada is struggling to bring its communications privacy laws into the 21st century. But a recent ruling by the country’s Supreme Court seems to have turned a corner. “Canadian ISPs can no longer simply hand over customer information without a warrant after the country’s Supreme Court ruled that internet users were entitled to a ‘reasonable’ expectation of privacy,” writes Brid-Aine Parnell with The Register. “The decision means that internet service providers can no longer disclose the names, addresses and phone numbers of their customers to law enforcement voluntarily, and cops will instead be required to get a warrant for the data.”

-Bloomberg this week carries an in-depth piece that looks closer at "UglyGorilla," the code name for one of the alleged Chinese hackers who was charged by the FBI last month with espionage attacks and stealing intellectual property from U.S. corporations. According to Bloomberg, this attacker was more interested in information that could be useful should the Chinese become locked in a cyberwar with the United States. "The hacker called UglyGorilla invaded the utility on what was probably a scouting mission, looking for information China could use to wage war," reports Michael Riley and Jordan Robertson. "UglyGorilla is one of many hackers the FBI has watched. Agents have recorded raids by other operatives in China and in Russia and Iran, all apparently looking for security weaknesses that could be employed to disrupt the delivery of water and electricity and impede other functions critical to the economy, according to former intelligence officials with knowledge of the investigation. The incursions spurred a debate in the Obama administration over whether and how to respond, and raised alarms among lawmakers briefed on the incidents."

Meanwhile, Business Week looks at recent discovery of a sophisticated software attack that allows hackers to access internal airport computer systems and manipulate data as if they were authorized employees. BW cites Boston digital security firm Trusteer, which says it uncovered malware hidden in the private network of a major non-U.S. international airport. Michael Dolgow writes: "The company says the threat could have compromised everything from employees' personal information to the safety of passengers. The airport VPN was immediately disconnected after officials there were made aware of the breach and authorities are investigating, Tubin says. A spokesman for the U.S. Transportation Security Administration, Dave Castelveter, says his agency was made aware of the breach by *Bloomberg Businessweek*'s inquiries but declined to comment further, citing a policy of not discussing security protocol." Read more here.

-Forbes asked nearly a dozen security experts for their views on ideas to help better secure the Internet and to "fix cybersecurity." Their answers, boiled down into a couple of sentences each, offer a range of responses and perspectives on why cybersecurity is hard.

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.