GW CSPRI Newsletter

July 1, 2013

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

-July 5, 10:00 p.m., **2600 Arlington Meetup** - An informal gathering of security enthusiasts and specialists. The meetings are open to anyone who has a general interest in technology, though the discussion can be technical and dive into technospeak at times. Champs Pentagon Row, 1201 South Joyce St., Arlington, Va. 22202. More information.

-July 10, 8:00 - 9:30 a.m., **Secured Space: What It Is, Who Has It and Who Needs It? -** The Howard County Chamber of Commerce and GovConnects will host a discussion on the technologies available to protect your intellectual property from cyber theft. University of Maryland University College, Dorsey Station, 6865 Deerpath Rd., Elkridge, Md. 21075. More information.

-July 10, 6:00 p.m. - 9:00 p.m., **NovaInfosec Meetup, East** - An informal gathering of security professionals. NoVA Infosec is dedicated to the community of Northern Virginia-, Washington, DC-, and southern Maryland-based security professionals and whitehat hackers involved in the federal government and other regulated verticals like critical infrastructure, financial, and healthcare. Velocity Five, 8111 Lee Highway, Fall Church, Va 22042. More information.

-July 16, 12 noon - 1:00 p.m., **The Growing Importance of Trade Secrets** - The D.C. Bar Intellectual Property Law Section will present a luncheon program which will explore the policies in place for using trade secrets to protect intellectual property values. Faculty experts Walter D. Davis Jr. of Axinn, Veltrop & Harkrider LLP and Jia Lu of Finnegan, Henderson, Farabow, Garrett & Dunner, LLP will highlight some of the most relevant policy changes and recent court decisions and provide participants with vital information to make better decisions about using trade secrets to protect intellectual property. D.C. Bar Conference Center, 1101 K Street NW, first floor. More information.

Legislative Lowdown

-Telcos and ISPs that serve European customers will have to come clean on data breaches within 24 hours under new EU regulations. ZDNet reports that under the regulations, telecoms operators and ISPs operating in Europe will have to notify national data protection authorities within 24 hours where personal data has been lost, stolen or "otherwise compromised". Under the new rules, companies will have to disclose the nature and size of the breach within 24 hours, but where this isn't possible they must submit "initial information" within this time before providing full details within three days. Affected firms will be required to spell out which pieces of information have been compromised and what measures have been, or will be, applied by the company to put this right.

-Revelations involving the extent of the National Security Agency's domestic surveillance activities are putting a serious crimp in any plans to pass cybersecurity legislation this year, The Hill reports. Speaking at a panel hosted by the publication last week, Greg Nojeim, senior counsel with the Center for Democracy and Technology, noted that the prognosis doesn't look bright. "I think that the recent disclosures about the NSA's conduct have put back the [cybersecurity] debate and they've changed it," Nojeim said, arguing that the intelligence agencies would likely exploit vague language in cybersecurity legislation to gain access to new troves of private data. "They've made it harder to pass cybersecurity legislation that has an information-sharing component." The most prominent cybersecurity measure in Congress -- the Cyber Intelligence Sharing and Protection Act (CISPA) -- would remove legal barriers that prevent companies from sharing information about cyber attacks with each other. It would also allow them to share that information with the government. Its supporters argue that it is critical for combating hackers that steal sensitive information and wreak havoc on computer systems.

Cyber Security Policy News

-Britain's spy agency GCHQ has secretly gained access to the network of cables which carry the world's phone calls and internet traffic and has started to process vast streams of sensitive personal information which it is sharing with its American partner, the National Security Agency (NSA), The Guardian writes. The U.K. publication cited information shared by NSA whistleblower Edward Snowden describing the ability to tap into and store huge volumes of data drawn from fibre-optic cables for up to 30 days so that it can be sifted and analyzed. That operation, codenamed Tempora, has been running for some 18 months. GCHQ and the NSA are consequently able to access and process vast quantities of communications between entirely innocent people, as well as targeted suspects.

Mr. Snowden also has been sharing information about spying activities with the German press. America's NSA intelligence service allegedly targeted the European Union with its spying activities, placing bugs in the EU representation in Washington and infiltrating its computer network, Germany's Der Spiegel reported last week. Cyber attacks were also perpetrated against Brussels in New York and Washington. The publication said information it obtained showed that not only had the NSA conducted online surveillance of European citizens, but also appears to have specifically targeted buildings housing European Union institutions. "The information appears in secret documents obtained by whistleblower Edward Snowden that Spiegel has in part seen," Der Spiegel wrote. "A 'top secret' 2010 document describes how the secret service attacked the EU's diplomatic representation in Washington. The document suggests that in addition to installing bugs in the building in downtown Washington, DC, the European Union representation's computer network was also infiltrated. In this way, the Americans were able to access discussions in EU rooms as well as emails and internal documents on computers."

-The most secretive court in the nation, which has been criticized for authorizing domestic surveillance by the National Security Agency, has taken a tiny step toward openness in lawsuits brought by Google and Microsoft, CNet reports. Both firms were left reeling after a pair of articles last month, based on one of Snowden's disclosures, alleged that they provided the NSA with "direct access" to their servers through a so-called PRISM program. By the next day, however, CNET reported that was incorrect, and the Washington Post backtracked from its original story on PRISM, eventually concluding there is no evidence that "the privacy of any American was illegally or improperly invaded." Google's filing before the surveillance court said the initial news coverage was "misleading," and Microsoft's lawyers called it "inaccurate." The two companies, which have flatly denied providing any government agency with direct access to their servers, filed the lawsuits to try to clear their names. They say they respond to government requests for individual account data only when they're legally compelled to do so -- in cases ranging from kidnapping to missing persons to terrorist investigations -- and want permission to divulge more information publicly.

-In the wake of damaging revelations and accusations by Snowden, the chief of the NSA says the agency will be introducing new measures to decrease the likelihood that such a leak would ever occur again. As Wired.com observed, the NSA plans to institute a two-person rule to government activities of system administrators at the agency. "This would presumably involve requiring a shadow for every sysadmin to ensure that no one operator can download the kind of data Snowden obtained without authorization from another operator, or change auditing and logging instructions on the system to hide their tracks," Wired's Kim Zetter wrote. "Alexander noted that Snowden, as a systems administrator, had great authority to access parts of the network that are not accessible to regular analysts. The sysadmin also has the ability to set the auditing conditions on a portion of the network. 'This is a huge problem,' Alexander said. 'We’re coming up with a two-person rule to make sure we have a way to block' someone from taking information out of the system.'"

-In other cyber-spy leak news, former second ranking officer in the U.S. military is now the target of a Justice Department investigation into a politically sensitive leak of classified information about a covert U.S. cyber attack on Iran’s nuclear program, NBC News reported last week. According to NBC, Retired Marine Gen. James “Hoss” Cartwright, the former vice chairman of the Joint Chiefs of Staff, has received a target letter informing him that he’s under investigation for allegedly leaking information about a massive attack using a computer virus named Stuxnet on Iran’s nuclear facilities. Gen. Cartwright, 63, becomes the latest individual targeted over alleged leaks by the Obama administration, which has already prosecuted or charged eight individuals under the Espionage Act. Last year, the New York Times reported that Cartwright, a four-star general who was vice chairman of the Joint Chiefs from 2007 to 2011, conceived and ran the cyber operation, called Olympic Games, under Presidents Bush and Obama. The Times said President Obama ordered the cyber attacks sped up, and in 2010 an attack using the Stuxnet worm temporarily disabled 1,000 centrifuges that the Iranians were using to enrich uranium.

-If all of this news about allegations of government snooping on personal phone calls and emails has you thinking about encrypting more of your communications, consider that doing so is more likely to ensure your data is stored longer by government security agents, The Register writes regarding two more explosive documents which set out what sort of information the NSA is allowed to harvest from foreign targets, as well American citizens. "The documents clearly state that surveillance should cease the minute a target is on US soil or is deemed to be an American – but there are exceptions to this which allow spooks to store communications from American citizens," The Register reports. "If someone's location cannot be clearly established, then they "will not be treated as a United States person", that is, unless other evidence becomes apparent. This would mean that anyone using anonymity software like Tor, which deliberately masks their location, is liable to have their communications stored. Spies are also told they can retain 'all communications that are enciphered or reasonably believed to contain secret meaning' for up to five years, giving them another way to keep American citizens' communications data."

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.