GW CSPRI Newsletter

February 10, 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

CSPRI in the News:

Dr. Allan Friedman (CSPRI Visiting Scholar) was quoted in the February 7 *Washington Post* blog article, "No, your phone will not get hacked just by turning it on in Russia."

Dr. Lance Hoffman (CSPRI Director) addressed the federal government's cyber security efforts in a February 4 interview on KOKI (Cox), Tulsa, OK. A portion of the interview also aired on Cox radio.

Events

-Feb. 10, 5:30 p.m. - **NoVA Hackers Association Meetup** - 8:00 p.m., 4350 Fair Lakes Court, Fairfax, 22033. More information.

-Feb. 11, 7:30 a.m. - 9:30 a.m., **The Insider Threat: Protecting Data and Managing Risk** - As recent events have demonstrated, the threats from inside government have the potential to be more harmful than external hacking activities. In this presentation, the speaker will discuss how to manage the risk of an insider threat, signs to look for in order to detect a possible threat as it happens, and what concrete steps agencies and organizations can take to protect sensitive information. The speaker will be Mark A. Nehmer, associate deputy director, cybersecurity and intelligence, Defense Security Service. Ronald Reagan Building, 1300 Pennsylvania Ave NW, Rotunda. More information.

-Feb. 11, 8:15 a.m. - 4:45 p.m., **ISACA NCA Meetup: DoD Training Day, What's Cyber Hot?** - The ISACA National Capital Area (NCA) chapter provides educational seminars and workshops for continuing professional development, networking opportunities at periodic mixers, CISA and CISM review courses, chapter news through newsletters and periodic e-mails, and various online resources. During this one-day conference, speakers will provide the participants information on a variety of cyber topics from their respective organizations across the DoD. There will be two panel sessions that will cover the latest on DoD Cyber Security polices and the biggest challenges for 2014. Rosslyn at Key Bridge, 1900 North Fort Myer Drive, Arlington, VA, 22209. More information.

-Feb. 12, 10:00 a.m., **The Report of the Privacy and Civil Liberties Oversight Board on Reforms to the Section 215 Telephone Records Program and the Foreign Intelligence Surveillance Court** - Dirksen Senate Office Bldg., Room 226. This hearing will be Webcast. More information.

-Feb. 12, Noon – 1:30 p.m., **Writing and Publishing in Cybersecurity** – In this panel discussion, scholars and experts from multiple disciplines, as well as government and industry, will address topics related to research, authorship, and publishing. Gelman Library, Room 702. More information.

-Feb. 12, 10:45 p.m. - 4:00 p.m., **ISACA CM Meetup: Penetration Tests and Why They Are Important** - ISACA Central Maryland Chapter (ISACA-CMC) is a volunteer-led group, offering IT, information systems, security, and audit and financial professionals local educational events, resource sharing, advocacy, professional networking and a host of other benefits at the local level. This session will discuss the various facets of penetration testing, from network to application to physical to social engineering. Tools and examples will be presented. CCMIT, 692 Maritime Boulevard, Linthicum Heights, MD, 21090. More information.

-Feb. 13, 6:30 p.m. – 8:30 p.m., **OWASP DC Meetup: An Introduction to Bitcoin Security within Applications** - Bojan Simic will provide a short background into Bitcoin and how it works. He will then provide some of his firsthand experiences with the state of Bitcoin businesses with regard to security and how many individuals are (insecurely) handling their Bitcoins. Uber, 1200 18th Street NW, Suite 700, Washington, DC, 20036. More information.

-Feb. 13, 6:30 p.m., **Panel to Examine 'Civil Liberties Dead Zone' at U.S. Borders** - The National Press Club's Freedom of the Press Committee will hold a panel to probe the federal government's under-reported practice of examining the electronic devices of individuals crossing into the United States. The moderator will be Marc Rotenberg, executive director of the Electronic Privacy Information Center. Panelist will include: Michael Chertoff, chairman of the

Chertoff Group and former secretary of the Homeland Security Department under President George W. Bush; Frank Smyth, senior adviser for journalist security at the Committee to Protect Journalists; and Neema Guliani, legislative counsel at the American Civil Liberties Union. National Press Club First Amendment Lounge, 529 14th St. NW. More information.

-Feb. 19-21, **Biometrics for Government and National Security 2014** - This three-day conference will feature numerous discussions on the latest challenges and opportunities in government and defense biometrics. Walter E. Washington Convention Center, 801 Mt. Vernon Place NW. More information.

-Feb. 19, 5:30 p.m. - 7:30 p.m., **NovaSEC! Pre-RSA Rally** - This event will take place one week before the annual RSA Conference in San Francisco. This is an opportunity for security professionals to network and discuss current security topics that will be highlighted at the RSA Conference. So whether you are going to RSA or not, this is the place to connect socially with your peers. Wildfire, Tysons Galleria, 2001 International Drive, McLean, Va. 22102. More information.

Legislative Lowdown

-Lawmakers on the House Homeland Security Committee last week approved legislation aimed at helping better secure the federal government and critical infrastructure systems from cyberattacks. The measure, H.R. 3696 (PDF) -- also known as the National Cybersecurity and Critical Infrastructure Protection Act - directs DHS to "strengthen and codify its cybersecurity standards for the federal government and critical infrastructure networks," The Hill reports.

Cyber Security Policy News

-Given greater leeway in revealing more information about what kind of user data they provide to the government in response to Foreign Intelligence Surveillance Act (FISA) requests, several companies including Facebook, Google, LinkedIn, Microsoft, and Yahoo are revealing the first information about the amount of user data they're handing over in FISA requests. Ars Technica breaks it down, noting that “all of the companies received fewer than 1,000 total requests in this time frame, suggesting that many of the requests are for large numbers of accounts. If Microsoft had 500 requests for information, for instance, and shared content on 15,000 accounts in response, that would be an average of 30 accounts per info request.”

The data comes amid revelations that the National Security Agency's much criticized efforts to hoover up data on domestic phone calls made by Americans is far less voluminous that most reports have made out. The Washington Post and the Wall Street Journal both report that while the program had been described as collecting records on almost every phone call placed in the U.S., in practice "it doesn't collect records for most cellphones, the fastest-growing sector in telephony and an area where the agency has struggled to keep pace. The WSJ's Siobhan Gorman explains: "The agency's legal orders for data from U.S. phone companies don't cover most cellphone records, a gap the NSA has been trying to address for years. That effort has been slowed by the NSA's need to fix a host of problems that it uncovered in the program and reported to the U.S. court that oversees NSA surveillance in 2009, people familiar with the matter say."

Meanwhile, the FISA Court announced last week that it has approved President Obama's request to change to the NSA's section 215 metadata collection program. "Obama did not choose to end the controversial metadata collection program outright -- as his own review panel suggested -- but rather to employ a few safeguards to prevent data that was not part of a terrorist investigation from being accessed, like spying on loved ones," NextGov reports.

-The federal government was once again awarded low marks for protecting its systems from hackers and malicious software. A report by the Republican staff of the Senate Homeland Security and Governmental Affairs Committee released last week says that federal agencies are ill-prepared to defend networks against even modestly skilled hackers. The report draws on previous work by agency inspectors general and the Government Accountability Office to paint a broader picture of chronic dysfunction, citing repeated failures by federal officials to perform the unglamorous work of information security," writes The Washington Post. "That includes installing security patches, updating anti-virus software, communicating on secure networks and requiring strong passwords. A common password on federal systems, the report found, is 'password.' Obama administration officials quibbled with elements of the report but acknowledged that getting agencies to secure their systems against attack has been difficult."

-State authorities in Florida on Thursday announced criminal charges targeting three men who used the site localbitcoins.com to allegedly run illegal businesses moving large amounts of cash in and out of the Bitcoin virtual currency, KrebsOnSecurity reports. Experts say this is likely the first case in which Bitcoin vendors have been prosecuted under state anti-money laundering laws, and that prosecutions like these could shut down one of the last remaining avenues for purchasing Bitcoins anonymously. "The biggest problem that Bitcoin faces is actually self-imposed, because it’s always hard to buy Bitcoins, said Nicholas Weaver, a researcher at the International Computer Science Institute (ICSI) and at the University of California, Berkeley and keen follower of Bitcoin-related news. " The reason is that Bitcoin transactions are irreversible, and therefore any purchase of Bitcoins must be made with something irreversible — namely cash. And that means you either have to wait several days for the wire transfer or bank transfer to go through, or if you want to buy them quickly you pay with cash through a site like localbitcoins.com." One very popular method of quickly purchasing Bitcoins — BitInstant — was shuttered last year. Last month, BitInstant CEO Charlie Shrem was arrested for money laundering, following allegations that he helped a man in Florida convert more than a million dollars in Bitcoins for use on the online drug bazaar Silk Road.

The Florida action comes as Russia's prosecutor general warned that the use of Bitcoins and other cryptocurrencies carries the risk of violating citizens' property rights, and therefore cannot be used in Russia. "The monitoring of the use of virtual currencies shows an increasing interest in them, including for the purpose of money laundering, profit obtained through illegal means,” ITAR-TASS quoted the Prosecutor General’s Office as saying in a story by RT. "Russia’s official currency is the ruble. The introduction of other types of currencies and the issue of money surrogates are banned,” the statement says, meaning that cryptocurrencies - the most popular of which is Bitcoin - cannot be used by Russian citizens or corporations."

At the same time, the United States should lead the way in Bitcoin regulation, says Sen. Tom Carper (D-Del). According to The Hill, a new study commissioned by Carper found that most countries do not have rules in place to address virtual currencies. "The study looked at 40 countries and asked whether they recognize Bitcoin as legal tender; what negative impacts Bitcoin could have on national currencies; what concerns they have about fraud; and how tax authorities view Bitcoin transactions," The Hill's Tim Devaney writes. "According to the study, there is 'widespread concern' about the negative impact Bitcoin could have on national currencies and how it could be used to fund criminal operations and tax fraud."

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.