GW CSPRI Newsletter

February 18, 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:

"The work of security blogger Brian Krebs, who spoke to the GW CyberCorps students last semester on cybercrime, was highlighted in the New York Times. For many of those following data privacy and security breaches closely, the detailed descriptions at http://krebsonsecurity.com/ are required reading."

Read the article here.

CSPRI Event:

-Feb. 26, 6:10 p.m. – 7:15 p.m., **Finding privacy leaks with bulk data analysis -** This talk by Simson L. Garfinkel, Associate Professor at the Naval Postgraduate School, will explore how more data can be recovered from a consumer GPS and other devices by looking below the files and accessing the raw data in unallocated space using bulk_extractor, and open source digital forensics tool developed by the Naval Postgraduate School. More information.

Events

-Feb. 19, 10:00 a.m. - 12 noon, **Mobile Device Tracking** - The Federal Trade Commission will host a workshop. FTC Conference Center, 601 New Jersey Ave., NW. More information.

-Feb. 19, 2:00 p.m. - 3:30 p.m., **Improving Critical Infrastructure Cybersecurity: The Cybersecurity Framework and Beyond** - The Center for 21st Century Security and Intelligence at Brookings will host a panel discussion evaluating the NIST Framework. Panelists will include Patrick D. Gallagher, the director of NIST; Cameron Kerry, a distinguished fellow with Governance Studies at Brookings and former acting secretary and general counsel of Commerce; and Dean Garfield, president and CEO of the Information Technology Industry Council. Ian Wallace, visiting fellow in cybersecurity at Brookings, will moderate the discussion. Brookings Institution, Falk Auditorium, 1775 Massachusetts Avenue, N.W. More information.

-Feb. 19, 4:00 p.m. - 6:30 p.m., **The Ever-Falling Cost of Surveillance: How You Can Be Tracked for Just Pennies a Day, and What It Means for The Future of Privacy** - The New America Foundation will host a panel discussion NAF, Suite 400, 1899 L St., 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.

-Feb. 19, 6:00 p.m. - 8:15 p.m, **NSA Telephonic and Electronic Surveillance Reform: Are the Programs Legal and What is Going to Change?** - The Federal Communications Bar Association's (FCBA) Privacy and Data Security Committee will host an event. Drinker Biddle & Reath, 1500 K 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. 20, 12:30 p.m. - 1:30 p.m, **Booz Allen Cybersecurity Twitter Chat** - Booz Allen will host its first Twitter chat discussion. The session is open to individuals who are interested in cybersecurity trends, technology, and the upcoming RSA Conference 2014. Join the online chat by following @boozallen and using the hashtag #BoozAllenChat. More information.

-Feb. 24-26, **Big Data for Federal Government and Defense** - The amount of data the government faces is at its highest ever and less than 1/3 of federal IT executives believe they have sufficient Big Data strategy. Big Data for Government & Defense will be an opportunity for CIOs, IT directors, program managers and more to express the latest government challenges,

strategies and initiatives relating to federal Big Data. Hear from those closest to these developments as they speak on topics including, advancing data mining processes; increasing server storage capacity; big Data security; cloud-like infrastructure to support big data. Walter E. Washington Convention Center. 801 Mt. Vernon Place NW. More information.

-Feb. 27, 9:30 a.m., **U.S. Strategic Command and U.S. Cyber Command** - The Senate Armed Services Committee will hold a hearing to receive testimony on U.S. Strategic Command and U.S. Cyber Command in review of the Defense Authorization Request for Fiscal Year 2015 and the Future Years Defense Program. Witnesses will include Admiral Cecil D. Haney, USN, commander, U.S. Strategic Command; and General Keith B. Alexander, USA, commander, U.S. Cyber Command. Senate Dirksen Office Bldg., Room SD-G50. More information.

-Mar. 1, 11 a.m. – 5 p.m., **Mobile Hacking on Android,** This workshop will concentrate on the Android platform. Participants will be shown how to perform mobile security testing, starting off by teaching you how to build a proper Android testing environment. Then into the fun stuff - installing and assessing applications for vulnerabilities. More information.

-Mar. 4, **Cybersecurity Summit 2014** - Attendees will have an opportunity to what challenges key DoD and federal cyber leaders are facing today; engage in breakout sessions on critical topics; network with cyber professionals and discuss new ideas and solutions; and hear where agencies are headed and where the budgets are in 2014. Capital Hilton, 1001 16th St. NW. More information.

Legislative Lowdown

-Democrats in the Senate last week introduced a measure to prohibit data broker companies from using deceptive means to collect information about consumers. The bill, the Data Broker Accountability and Transparency Act (PDF), would also require that the data broker companies make the information it has about each consumer available so that consumers can correct the data or opt-out of having their data collected, The Hill reports. Under the proposal, the Federal Trade Commission would be able to impose civil penalties on violators.

-Other senators in Congress offered a bill that would require mobile phones to come with a "kill switch" to make them less appealing to thieves. As the National Journal writes, "the switch, if flipped, would wipe personal data from the phone and render it inoperable, a feature that the bill's backers say would not only protect consumer information but also deter would-be thieves." Apple smart phones have had a similar feature, but the wireless industry has largely declined to embrace the feature. Experts say a universal kill switch might make it simpler for hackers to disable people’s phones, which could have especially damaging consequences for police officers and other public safety officials. Rather, companies have worked with the Federal Communications Commission (FCC) to create a database of stolen phones.

Cyber Security Policy News

-The Obama administration issued voluntary cyber standards aimed at defending key private networks essential to U.S. society last week, but as NextGov observes, it could be years before the benefits are noticeable. "With Wednesday's release, the Commerce Department met a one-year deadline set by President Obama in a Feb. 12, 2013 executive order to develop a pick-and-choose menu of controls understandable to everyone from technicians to corporate boardroom members, who ultimately will determine the rubric's viability in industry," NextGov's Aliya Sternstein writes. "The private sector operates most critical infrastructure. While optional for industry, it is expected that the guidelines -- which encourage reporting data breaches to the government -- will be required for federal contractors."

President Obama's plan to get utilities, banks and other essential services to bolster defenses against hackers is filled with technical standards and guidance on responding to attacks, but it lacks one thing -- financial incentives to help pay for computer and network security upgrades. According to Bloomberg, that could mean many companies decide not to take part in the voluntary program. "While the administration's National Institute of Standards and Technology developed the framework with industry, it left out incentives," Chris Strohm writes. "The Homeland Security Department will develop a program to encourage participation in the framework."

-A new report (PDF) from Kaspersky labs examines what could be the most sophisticated malicious software yet discovered in the wild, The Washington Post writes. "The software, dubbed Careto, is a sophisticated suite of tools for compromising computers and collecting a wealth of information from them. Whoever is behind the malware sends out 'spear phishing' e-mails, with addresses designed to be mistaken for the Web sites of mainstream newspapers, such as The Washington Post or the Guardian. If the user clicks on a link, it takes her to a Web site that scans her system for vulnerabilities and attempts to infect it. There are multiple versions of the malicious software designed to attack Windows, Mac OS X and Linux versions, and Kapersky believes there may be versions that attack iOS and Android."

-NBC reports that a civilian employee at the National Security Agency recently resigned after being stripped of his security clearance for allowing former agency contractor Edward Snowden to use his personal log-in credentials to access classified information. The news outlet said it obtained a memo that says "an active duty member of the U.S. military and a contractor have been barred from accessing National Security Agency facilities after they were 'implicated' in actions that may have aided Snowden: "While the memo's account is sketchy, it suggests that, contrary to Snowden's statements, he used an element of trickery to retrieve his trove of tens of thousands of classified documents. At Snowden's request, the civilian NSA employee, who is not identified by name, entered his password onto Snowden's computer terminal, the memo states."

Meanwhile, legislation aimed at reining in the NSA's sprawling surveillance apparatus appears to have stalled in both the House and Senate, The Hill reports. Nevertheless, supports are optimistic about some kind of legislative curbs passing this year. "Despite the sluggishness, advocates for

sweeping changes to the NSA say they aren't discouraged," The Hill's Julian Hattem writes. "They say it's only a matter of time before something passes through Congress."

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.