GW CSPRI Newsletter

January 6, 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

Events 1

Cyber Security Policy News 2

Events

-Jan. 6, 2:00 p.m. – 4:00 p.m., **Cybersecurity and Cyberwar: What Everyone Needs to Know...and How to Talk About It** - The Center for 21st Century Security and Intelligence and Governance Studies at Brookings will launch the new book *Cybersecurity and Cyberwar: What Everyone Needs to Know*. The first panel will feature co-authors Peter W. Singer and Allan Friedman discussing their book and the key questions of cybersecurity – how it all works, why it all matters and what we can do. A second panel will then feature some of the leading journalists on the cybersecurity beat today, exploring the challenges of reporting on a new domain and explaining its complexities to the public. Following the panel discussions, participants will take questions from the audience. This event will be webcast live. The Brookings Institution, 1775 Massachusetts Ave, NW, Washington, DC 20036. More information.

-Jan. 8, 7:30 a.m., - 4:30 p.m., **ISACA CM Meetup** - The ISACA – Central Maryland (CM) chapter is based in Baltimore, MD. It is led by a group of dedicated volunteers 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. 692 Maritime Boulevard, Linthicum Heights, MD, 21090. More information.

-Jan. 8, 9:00 am. - 3:00 p.m., **National Cybersecurity Center of Excellence (NCCoE) Proposed Federally Funded Research and Development Center (FFRDC)** - The National Institute of Standards and Technology (NIST), National Cybersecurity Center of Excellence will be hosting an Industry Day for parties interested in the proposed Federally Funded Research and Development Center to engage vendors and federal employees in a discussion about the proposed requirement, the NCCoE, and the forthcoming Draft Request for Proposals (RFP) for the requirement. The Universities at Shady Grove, Building I Auditorium, 9630 Gudelsky Drive, Rockville, MD 20850. More information.

-Jan. 11, 9:00 a.m. - 7:00 p.m., **DC Internet Freedom Hackathon** – OpenITP will host this event, being held to help improve open source privacy and anonymity tools used by communities throughout the world which face online censorship or surveillance. The hackathon will have a special focus on improving the user interface of these tools, which must be localized for different languages and cultures, and thus present unique design challenges. A bad interface can put end-users living under oppressive regimes at risk. UX designers and regional experts are highly encouraged to attend, in addition to developers, activists, and other interested folks. “1776”, 1133 15th St NW. More information.

-Jan. 15, 3:00 p.m., **Cyber Risk Wednesday: Cyber Resilience Through Measurement** – The Atlantic Council will host this discussion that will feature panelists discussing a data-driven methodical and systematic understanding of cyber risks and solutions. 1030 15th Street, NW, 12th Floor. More information.

-Jan. 16, 6:30 p.m. - 8:30 p.m., **OWASP VA Local Chapter Meeting** - The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Their mission is to make application security “visible,” so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of their materials are available under an open source license. Living Social, 11600 Sunrise Valley Drive, Reston, VA, 20136. More information.

Cyber Security Policy News

-The Obama administration is moving on two fronts to preserve the National Security Agency's controversial domestic surveillance programs, despite setbacks in the courts and recommendations by a presidential commission to place some checks on the NSA's spying powers.

In mid-December, a group reviewing the NSA's surveillance and cyber command operations recommended broad changes that would permit most of the NSA's surveillance programs to continue but shift ownership of the government's large inventory of telephone records and restrict spying on allied nations. The review panel's meetings were not public, but the group did meet with various business and privacy groups, and tidbits of their recommendations leaked to the media. For example, The Wall Street Journal reported that the panel proposed shifting control of sought-after phone records from the government to individual phone companies, while The

New York Times wrote that the panel urged the White House to rein in U.S. spying on foreign leaders.

Meanwhile, courts reviewing legal challenges brought against the NSA's policies have produced contradictory rulings, setting the stage for a set of appeals by the administration. On Dec. 16, Judge Richard J. Leon in Washington ruled that the program was "almost Orwellian" and likely unconstitutional. The, late last month, a federal judge ruled that the NSA's phone records collection program was legal, a decision that the New York Times quoted George Washington University Law professor Orin S. Kerr observing as "the exact opposite of Judge Leon's in every way, substantively and rhetorically."

Last week, the Justice Department appealed Leon's Dec. 16 ruling, The Washington Post reports. According to The Post, Leon, who was nominated by President George W. Bush and appointed to the bench in 2002, stayed his decision to allow the Justice Department time to appeal.

As the debate rages in the courts, Sen. Rand Paul (R-Ky.) said he is pushing forward with a planned class-action lawsuit against the NSA in a bid to show the administration's surveillance policies are "too broad and unconstitutional," The Hill writes. Appearing on ABC's 'This Week,' Paul said that the suit would allow regular people to object to having a single generalized warrant cover large numbers of cell phones, and that the government should be forced to specifically seek the records of individuals. "That's what we fought the Revolutionary War over," Paul said about generalized warrants.

Tech industry groups, still reeling from disclosures by former NSA contractor Edward Snowden that they largely acquiesced to the NSA's surveillance demands, have been scrambling to publish what information they can on the volume of surveillance-related requests from the U.S. government. Verizon said it will soon publish the number of government requests it receives for customer data, a shift that The Washington Post says sets "a significant precedent for the telecommunications industry, which has kept that information private."

In related news, CNet reports on Google's latest "transparency report," published late last year. This report is intended to offer insight on the number of requests the search giant gets from the government to remove content from its services. Google says it received 3,846 government requests to remove 24,737 pieces of content during the first half of 2013, a 68 percent increase over the same period in 2012.

-Individuals already wary of the government's ability to spy on their communications have long turned to encryption to keep their conversations secret. But new research published last month shows that computer scientists have devised an attack that reliably extracts secret cryptographic keys by capturing the high-pitched sounds coming from a computer while it displays an encrypted message. Ars Technica writes that the technique, "outlined in a research paper published Wednesday, has already been shown to successfully recover a 4096-bit RSA key used to decrypt e-mails by GNU Privacy Guard, a popular open source implementation of the OpenPGP standard."

-Cyber crooks were the grinches that stole Christmas, at least for nationwide retailer Target and its customers. On Dec. 18, KrebsOnSecurity.com broke the story that hackers had broken into Target's network in the days leading up to Black Friday, and stolen credit and debit card data on millions of customers. On Dec. 19, Target confirmed that a data breach extending from Nov. 27 to Dec. 15 resulted in the compromise of some 40 million credit and debit cards, making it one of the largest data breaches ever. The company now finds itself the target of at least four class-action lawsuits, and the breach has sparked calls for federal action. According to The Hill, "the government is facing increased pressure to institute data security protections after the high-profile breaches of Target and social networking app Snapchat. While some argue that the companies' security standards are ripe for an investigation from the Federal Trade Commission (FTC) — which has brought data security cases as part of its mission to protect consumers from deceptive business practices — the agency's ability to intervene is anything but certain."

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.