GW CSPRI Newsletter

January 13, 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:

Profs. Azim Eskandarian (CEE) and **Lance Hoffman (CS)** and their former student **Jeremy Blum** have had their paper, "Challenges of intervehicle ad hoc networks" selected as one of the Top Ten Best Research Papers for the *IEEE Transactions on Intelligent Transportation Systems* for the decade 2000-2009. Part of the paper dealt with security against hacking and communication failures in vehicles.

CSPRI Visiting Scholar Allan Friedman's new book, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014), was launched last Monday. A video of the book launch including a discussion of the issues by him, his co-author P. W. Singer, and various journalists was broadcast live by CSPAN on January 6. It is viewable here.

New Blog Post:

Cyberinsurance: At What Cost? by Nicolas Zahn

New CSPRI Publication:
Insurance for Cyber Attacks: The Issue of Setting Premiums in Context by Dr. Costis Toregas, Associate Director of CSPRI and Nicolas Zahn

Save the Date! On January 29, 2014 at 6 p.m. in the Marvin Center Betts Theater, David Medine, Chairman of the Privacy and Civil Liberties Oversight Board, a bipartisan independent federal agency, will discuss the Board's report and recommendations, to be issued on January 23, on the NSA telephony metadata program and reform of the operations of the Foreign Intelligence Surveillance Court. He will also discuss the role of the Board going forward overseeing federal counterterrorism programs to ensure they strike the right balance between national security and privacy and civil liberties. More details will be given next week.

Events

-Jan. 15, 1:00 p.m., **What does the FFIEC Guidance on Social Media Risk mean to your Security Operations?** - The FFIEC has issued "Social Media: Consumer Compliance Risk Management Guidance" effective immediately. Prepare your Security Operations teams with the information they require to successfully plan and implement a winning, balanced approach, to the new Guidance. On December 12, 2013, the FFIEC provided significant and important guidance to financial institutions on the rapidly changing character and complexity of reputational and operational risk resulting from social media activity. Join FS-ISAC Affiliate Board Advisor, BrandProtect, for a Webinar on just what the FFIEC guidance on Social Media Risk means to your security operations, and how you can best prepare to meet the suggested operational requirements for future threat detection and risk mitigation. More information.

-Jan. 15, 3:00 p.m., **Cyber Risk Wednesday: Cyber Resilience Through Measurement** - This discussion, sponsored by the Atlantic Council's Cyber Statecraft Initiative, 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, 9:00 a.m., **Healthcare.gov: Consequences of Stolen Identity** - The House Science, Space and Technology Committee will hold a hearing. The witnesses will include David Kennedy, chief executive officer, TrustedSEC, LLC; Waylon Krush, co-founder and CEO, Lunarline, Inc.; Michael Gregg, chief executive officer, Superior Solutions, Inc.; and Lawrence Ponemon, chairman and founder, Ponemon Institute. Rayburn House Office Bldg., Room 2318. More information.

-Jan. 16, 9:30 a.m., **HHS' Own Security Concerns about HealthCare.gov** - The House Committee on Oversight and Government Reform will hold a hearing. Rayburn House Office Bldg., Room 2154. 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.

-Jan. 21, 6:30 p.m. - 9:00 p.m., **ISSA DC Meetup: Social Engineering to Improve Security Awareness** - While many organizations perform Social Engineering assessments to test their security, they end up being useless games of "gotchas", with results that prove the obvious. Rarely, do they provide recommendations that could not have been found through less expensive, overt methodologies. This presentation provides guidance on performing penetration tests in a systematic way that tests levels of security awareness. The results allow for a very tailored awareness program that is specific to the organization's employee base. As the level of awareness increases, the number and severity of incidents can dramatically decrease. Center for American Progress, 1333 H Street, NW. More information.

Legislative Lowdown

-Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.) reintroduced legislation last week designed to protect Americans' data from cyber thieves on Wednesday. Leahy proposed the bill, which was first offered almost a decade ago but which has never made it to a vote on the Senate floor, after a headline-grabbing hack at nationwide retailer Target exposed the personal and financial information on more than 110 million people. According to The Hill, the legislation "would impose criminal penalties for people who hide security breaches that damage consumers, require companies that maintain databases with personal information to protect them and establish a nationwide standard for notifying consumers after a data breach."

-On Jan. 15 at 2:00 p.m., the House Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will hold a markup of HR 3696 (PDF), the National Cybersecurity and Critical Infrastructure Protection Act of 2013. According to InsidePrivacy.com, the bill focuses primarily on the authorities of the Department of Homeland Security and information-sharing, while preserving and enhancing the role of private parties in interfacing with DHS.

Cyber Security Policy News

-President Obama is expected to reveal his plan for reforming the National Security Agency in a speech Jan. 17, according to a statement from the White House. *Government Executive* reports that the speech will come in the wake of a report issued last month by the president's review group calling for sweeping changes to the government's surveillance practices, including forcing the NSA to give up its database of records on all U.S. phone calls. "We will not harm our national security," White House press secretary Jay Carney said Friday, announcing the date of the speech, but providing no other details about its time or location.

Meanwhile, the president met last week with senior lawmakers on both sides of a debate about whether to end the National Security Agency's collection of Americans' phone data. According to The Washington Post, the 90-minute meeting came in the wake of that report that concluded that the program, which gathers billions of phone call toll logs, "was not essential" to preventing terrorist attacks. The group recommended that the data be held instead by the phone companies or a private third party.

Some states are not waiting for action from The White House. In California, two lawmakers last week introduced legislation that would prohibit state agencies and corporations from providing material support to the National Security Agency. *ComputerWorld* writes that the "Fourth Amendment Protection Act" would bar state and locally-owned utilities from providing water and electricity to NSA facilities in California. Under the proposal, any data collected without a warrant by the NSA and given to California law enforcement authorities would be inadmissible in state courts.

With federal courts issuing conflicting rulings over the constitutionality of the NSA's telephone bulk metadata collection program, many pundits have opined that this debate will only be settled by the U.S. Supreme Court. But according to GW Professor Orin Kerr, one of the nation's prominent Fourth Amendment scholars and a member of CSPRI's Advisory Board, high court intervention is "certainly possible, but it's not at all a sure thing." Writing for the blog The Volokh Conspiracy, Kerr observes: "We pay them the big bucks to step in and decide the big cases. Perhaps. But that view hinges on a notion of the Supreme Court's role that four or more Justices may or may not share. We don't know how eager the Justices may be to step in, and the arguments above will give them reasons to stay out for now."

Agencies should expect new guidance this year from the Office of Management and Budget (OMB) on how soon they should report data breaches to the Homeland Security Department, Federal News Radio reports. The expected guidance is being informed in part by a Government Accountability Office (GAO) report, which found that the OMB's requirement to submit information about data breaches to DHS's U.S. Computer Emergency Readiness Team (US-CERT) within an hour after discovering the breach was of little value.

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.