GW CSPRI Newsletter

April 28, 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:

New Blog Post:
"PrEP Model: Cyber Weapons" by Trey Herr

CSPRI Media Appearance:
Allan Friedman (Research Scientist) was interviewed about the Heartbleed computer virus on NewsChannel 8. (**video**)

Cyber(security) Governance?
Click here to read a report from Brazil by Susan Ariel Aaronson. Dr. Aaronson is a Research Professor of the GWU Elliott School of International Affairs.

Events

-Apr. 29, 1:00 p.m. - 5:00 p.m., **NTIA Meeting** - The Department of Commerce's National Telecommunications and Information Administration (NTIA) will hold a meeting on privacy and facial recognition technology. American Institute of Architects, 1735 New York Ave., NW. More information.

-Apr. 29 - May 2, **US Cyber Crime Conference** - This conference covers the full spectrum of topics facing defenders as well as law enforcement responders. All aspects of computer crime will be covered, including intrusion investigations, cyber crime law, digital forensics, information assurance, along with research and development, and testing of digital forensic tools. National Conference Center, 18980 Upper Belmont Pl., Leesburg, Va., 20176. More information.

-Apr. 30, 11:00 a.m. - 11:30 a.m**., PCAST's Big Data and Privacy Report** - The President's Council of Advisors on Science and Technology will hold a public meeting via conference call. Information regarding the call agenda, time, and how to register for the call is available on the PCAST Web site at: http://whitehouse.gov/ostp/pcast. More information.

-Apr. 30, 12:00 noon - 1:30 p.m., **Bitcoin and other Virtual Currencies: Emerging Issues in Regulation and Enforcemen**t - The American Bar Association will host a Webcast panel discussion. The speakers will be Jamal El-Hindi, associate director for program policy & implementation, Office of Foreign Assets Control (OFAC), U.S. Department of the Treasury; Brian Klein, partner, Baker Marquart; Deborah Peden, partner, Pillsbury Winthrop; and Luke Sully, director of intelligence, PriceWaterhouseCoopers. More information.

-Apr. 30, 6:30 p.m. - 7:30 p.m., **InSecurity: Race, Surveillance and Privacy in the Digital Age** - The New America Foundation, Center for Media Justice, and Consumers Union will host a panel discussion. The speakers will be Seeta Peña Gangadharan, senior research fellow, Open Technology Institute; Chris Calabrese, legislative counsel, ACLU; Hamid Khan, campaign coordinator, Stop LAPD Spying; Grace Sheedy, the United Food and Commercial Workers International Union; and Malkia Cyril, founder and executive director, Center for Media Justice. This even also will be Webcast. 1899 L St., NW., Suite 400. More information.

-May 12-14, **GovSec** - GovSec is designed for government, Homeland Security, and law enforcement professionals looking for strategies and cost effective technology to achieve their mission of protecting our critical infrastructures, key assets, communities and the nation. This year’s conference tracks include: counter & anti-terrorism; critical infrastructure & secured cities; cybercrime & cyberterrorism; and campus security & life safety. Washington DC Convention Center, 801 Mount Vernon Place, NW. More information.

Cyber Security Policy News

-An FBI informant directed a series of attacks on websites outside the US in 2012 exploiting a then-undisclosed vulnerability with the knowledge of the FBI agents supervising him, according to a story last week in The New York Times. Among the targeted websites were several operated by the governments of Iran, Syria, Brazil, and Pakistan. NYT's Mark Mazzetti writes that, "the details of the 2012 episode have, until now, been kept largely a secret in closed sessions of a federal court in New York and heavily redacted documents. While the documents do not indicate whether the F.B.I. directly ordered the attacks, they suggest that the government may have used hackers to gather intelligence overseas even as investigators were trying to dismantle hacking groups like Anonymous and send computer activists away for lengthy prison terms."

-President Barack Obama's plan to protect the U.S. from hackers was supposed to allow companies more access to classified data on computer threats so banks, utilities and other targets would be able to boost their cybersecurity. But as Bloomberg reports, that hasn't happened, now 14 months later. "While Lockheed Martin Corp. (LMT), Raytheon Co. (RTN) and 16 other companies have been tentatively approved to participate in the data-sharing program, they remain mired in the red tape of getting government approval to handle the classified data," reporter Chris Strohm writes. "The delay in the Enhanced Cybersecurity Services program comes amid an increase in computer breaches that a recent survey shows could have been prevented. High-profile hacking attacks have included stolen credit-card data from Target Corp. in December and attempts last year to knock the websites offline for JPMorgan Chase & Co. and other banks."

The slow start to Uncle Sam's cyberattack data-sharing plans is bedeviled by a perennial problem: hiring talented cybersecurity experts, and then keeping them from leaving for the more lucrative private sector. Reuters reports that, "in the race to attract cybersecurity experts to protect the government's computer networks, the Department of Homeland Security has a handicap money can't fix. Navigating the federal hiring system takes many months, which is too long in the fast-paced tech world. After a spate of national security leaks and with cybercrime on the rise, the department is vying with the private sector and other three-letter federal agencies to hire and retain talent to secure federal networks and contain threats to American businesses and utilities."

-In the wake of the Heartbleed bug, a dangerous flaw in widely-used cryptography software that jeopardized security for millions of Web sites, major tech companies are teaming up to try to avoid a repeat scenario. NBC News reports that thirteen big tech firms -- including Google, Facebook, Amazon and Microsoft — announced last week that they would join a project called Core Infrastructure Initiative, meant to fund important open-source technology with at least $3.9 million over three years. "That would include OpenSSL, the software that many sites use to encrypt and transmit online data. Researchers discovered a major bug in the system that they dubbed 'Heartbleed.'"

-An unusual number of physicians in several U.S. states are just finding out that they've been victimized by tax return fraud this year. As cybercrime reporter Brian Krebs writes, "an apparent spike in tax fraud cases against medical professionals is fueling speculation that the crimes may have been prompted by a data breach at some type of national organization that certifies or provides credentials for physicians. Scott Colby, executive vice president of the New Hampshire Medical Society, said he started hearing from physicians in his state about a week ago, when doctors who were just filing their tax returns began receiving notices from the Internal Revenue Service that someone had already filed their taxes and claimed a large refund. So far, Colby has heard from 111 doctors, physician assistants and nurse practitioners in New Hampshire who have been victims of tax fraud this year. Colby said he's heard similar reports from other states, including Arizona, Connecticut, Indiana, Maine, Michigan, North Carolina and Vermont."

-Many crucial satellite systems manufactured by some of the world's biggest government contractors contain severe vulnerabilities that could be exploited to disrupt military operations and flight-safety communications, The Guardian reports. "Security consultancy IOActive says it

has uncovered various vulnerabilities in software and ground-based satellite systems manufactured by British suppliers Cobham and Inmarsat," writes Tom Brewster. "US firms Harris Corporation, Hughes and Iridium were also said to have produced vulnerable kits, alongside Thuraya, a UAE provider, and Japan Radio Company. The Computer Emergency Response Team based in Carnegie Mellon University, which is sponsored by the Department of Homeland Security, warned about a handful of the vulnerabilities in January. But...information on more alleged weaknesses was released, amid growing concern the contractors are ignoring the threats. The latest report from IOActive suggested there were some easily hackable systems, many of which were designed for keeping aircraft, ships and army personnel safe."

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.