# GW CSPRI Newsletter

November 4, 2013

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



# "25 years ago"

This week marks the 25th anniversary of the notorious Internet Worm penned by Robert Tappan Morris. For one analysis and to view old TV news report, click on these links:

**How One Hacker's Mistake Fashioned the Internet You Use Today**

http://mashable.com/2013/11/01/morris-worm/

**Computer Virus TV News Report 1988**

http://www.youtube.com/watch?v=G2i_6j55bS0

# New from the CSPRI Byte:

"**Recent Google Street View Court Decision Threatens to Criminalize Ordinary Wi-Fi Use (Part 1): The Wiretap Act's Collision Course with FCC's Part 15**" by Shane Huang

# Events

**Events in blue are GW-specific.**

***If you missed Prof. Diana Burley discussing her recent report for the National Academy of Sciences on whether the cybersecurity workforce should be professionalized at GW last week, and a panel of experts also discussing that topic, it has been captured on video for you. View the event.**

-Nov. 5, 7:30 a.m. - 5:00 p.m., **Sleuth Kit and Open Source Digital Forensics Conference** - This event is an opportunity to make investigators and developers aware of their tools, get feedback from users, meet fellow developers, and help direct the future of open source digital forensics software.14750 Conference Center Drive, Chantilly, VA, 20151. More information.

-Nov. 5-6, **MirCon 2013** - The annual targeted threat conference put on by Alexandria, Va.-based incident response firm Mandiant. With targeted attacks becoming more prevalent, today's incident responders are faced with the tremendous challenge of accelerating their response times while capturing relevant data from attacks in progress. From analysts and innovators to managers and executives, the Mandiant Incident Response Annual Conference will address new technologies, incident response best practices, and key strategies for managing network security. JW Marriott, 1331 Pennsylvania Ave, NW. More information.

-Nov. 6, 7:30 a.m. - 5:00 p.m., **Fedcyber 2013 Annual Summit** - This event will bring together thought leaders who know the cyber mission in a venue designed to enhance our collective understanding of the threat, build on existing strategies to mitigate challenges, and leverage the nation's greatest technologies to enhance our defense in depth. Crystal Gateway Marriott, Arlington, VA, 22202. More information.

-Nov. 6, 8:30 a.m. - 5:00 p.m., **P0WNAG3 Cyber Security Summit** - This conference will feature panel discussions, live demonstrations and hacks from some of the top professionals in their field. Mingle with the pros, learn some new offensive and defensive techniques. Hilton Garden Inn, Greenbelt, 7810 Walker Drive, Greenbelt, MD, 20770. More information.

-Nov. 6-7, **FOSI 2013 Annual Conference: Family Online Safety Institute** - This year’s conference will bring together the top thinkers in online safety: academics, educators, law enforcement, industry, policy makers, and non-profits. Ronald Reagan Building and International Trade Center (Amphitheater), 1300 Pennsylvania Ave, NW. More information.

-Nov. 6-7, **Security and Privacy Intelligence for Healthcare** - A two conference on some of the most pressing cybersecurity healthcare challenges, including the threat of healthcare data hacking, the business and clinical opportunities of big data, and managing and securing the newest areas of vulnerability in the cloud and mobile spaces. Sheraton Premiere Tyson's Corner, 8661 Leesburg Pike, Tysons Corner, VA 22182. More information.

-Nov. 7, 6:30 p.m. - 8:00 p.m., **OWASP NoVA Meetup** - Meetings are free and open to anyone interested in learning more about application security. 11600 Sunrise Valley Drive, Reston, VA, 20136. More information.

-Nov. 13, 7:00 PM - 9:00 PM, **TeqTalk** – This event is open to the public. Presenters this session include Inno Eroraha, Founder and Chief Strategist of NetSecurity Corporation who will be speaking about "The Erosion of Digital Forensics Artifacts in Cloud-based Environments" and Jason Pubal, Senior Web Application Security Analyst at a large financial services company who will be speaking about "Building a Web Application Security Vulnerability Management Program". Teqcorner, 1616 Anderson Rd., McLean, VA 22102. More Information.

# Legislative Lowdown

-The Senate Intelligence Committee last week moved to advance legislation that would tweak -- but not terminate -- the National Security Agency's program to gather call records on all U.S. phone calls. According to The Hill's Brendan Sasso, "the move sets up a showdown with the Senate Judiciary Committee, which will soon take up legislation to end the controversial program." The chairman of that committee, Sen. Patrick Leahy (D-Vt.), and Rep. Jim Sensenbrenner (R-Wis.), the original author of the Patriot Act, introduced the USA Freedom Act earlier this week to end the bulk phone data collection and toughen other privacy protections.

Meanwhile, a bevy of tech heavyweights have come out against Feinstein's measure and in favor of stronger restrictions on the NSA, The Hill writes. Business networking site LinkedIn has joined Google, Facebook and other tech giants in supporting the USA Freedom act.

-Although still stung by the extent of U.S. telephone and cyber surveillance on European leaders abroad, lawmakers in Brussels are looking for ways to delay legislation designed to prevent privacy violations at home. "Two days after Chancellor Angela Merkel of Germany telephoned President Obama to complain about the monitoring of her cellphone by the United States, she joined fellow European leaders at a summit meeting in Brussels last week in agreeing not to rush into a new data privacy law, perhaps putting it off until 2015, after elections next May for a new European Parliament," The New York Times reports.

# Cyber Security Policy News

-The National Security Agency quietly broke into overseas communications links that connect Google and Yahoo data centers, according to documents provided to The Washington Post by Edward Snowden. By tapping those links, the agency has positioned itself to collect at will from hundreds of millions of user accounts, many of them belonging to Americans," wrote Barton Gellman and Ashkan Soltani for The Post. "The NSA does not keep everything it collects, but it keeps a lot." The Post reportedly obtained a top secret document which shows that the NSA's acquisitions directorate sends millions of records every day from internal Yahoo and Google networks to data warehouses at the agency's headquarters at Fort Meade, Md. In the preceding 30 days, the report said, field collectors had processed and sent back 181,280,466 new records —

including “metadata,” which would indicate who sent or received e-mails and when, as well as content such as text, audio and video.

Asked about the Post's revelations, National Security Agency Director Keith Alexander said he hadn't seen the paper's report, but he denied that the NSA has direct access to Google and Yahoo servers. The Hill notes, however, that the official response from the NSA's spokesperson was more nuanced, noting that the NSA is a foreign intelligence agency and that the agency is "focused on discovering and developing intelligence about valid foreign intelligence targets only."

A major thoroughfare in Israel suffered a cyberattack earlier this year, knocking out key operations for two days in a row and causing hundreds of thousands of dollars in damage, the Associate Press reports. The AP cites anonymous sources saying that attackers got in using a Trojan horse which compromised a security camera apparatus in the Carmel Tunnels toll road on Sept. 8. "The expert said investigators believe the attack was the work of unknown, sophisticated hackers, similar to the Anonymous hacking group that led attacks on Israeli websites in April," the AP's Daniel Estrin wrote. "He said investigators determined it was not sophisticated enough to be the work of an enemy government like Iran."

Authorities in Finland are investigating the infiltration of the foreign ministry's data network by cyberspies, Bloomberg reported last week. "The data breach was an extensive attempt to spy on an entire network,” Tuomioja told reporters in Helsinki yesterday after broadcaster MTV3 reported the ministry’s network was the target of intelligence gathering for as long as four years. "It seems to have been going on for an extended period of time." The hacking was discovered early this year based on a tip from outside the country, and the government has discussed it on several occasions, Tuomioja said.

-Even as Congress scrutinized delays and malfunctions in the Obama administration's health insurance Web site, new security concerns surfaced in a government memo that "posed a potentially high security risk for the Web site." The AP obtained a copy of a memo shared with lawmakers that called for a six-month "mitigation" program, including ongoing monitoring and testing. The memo "recommended setting up a security team to address risks and conduct daily tests, and said a full security test should be conducted within two to three months of the website going live."

*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.*