GW CSPRI Newsletter

June 16, 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 CSPRI Blog Post:
"Event Report: Computers, Freedom, and Privacy Conference 2014"
By Jonathan Berliner

CSPRI in the News:
CSPRI Research Scientist, Dr. Allan Friedman discusses personal data use and the recent request that telecom giants create cybersecurity plans.

Events

-June 17, 6:30 p.m. - 8:00 p.m., **ISSA DC Meetup: The Five Stages of Grief** - How to Implement a Software Assurance Program - Presenters will share some of the challenges we encountered while implementing a software assurance program. We will discuss the various stakeholders, and their varying goals, expectations, and fears. The speakers will present suggestions based on our experience that may help your program gain acceptance and produce more secure software. In addition, the discussion will briefly describe Continuous Integration/DevOps and discuss some of the security benefits – and risks –

that come from this software development approach. Government Printing Office, 732 North Capitol Street, Washington, DC, 20401. More information.

-June 17-19, **NIST's Identity Ecosystem Steering Group (IDESG) 9th Plenary Meeting** - The National Strategy for Trusted Identities in Cyberspace (NSTIC), signed by the President in April 2011, states, "A secure cyberspace is critical to our prosperity." This powerful declaration makes clear that securing cyberspace is absolutely essential to increasing the security and privacy of transactions conducted over the Internet. The Identity Ecosystem envisioned in the NSTIC is an online environment that will enable people to validate their identities securely, but with minimized disclosure of personal information when they are conducting transactions. The IDESG is the private sector led organization created to achieve this mission by administering the development of policy, standards, and accreditation processes for the Identity Ecosystem Framework. Red Auditorium, NIST, 100 Bureau Drive, Gaithersburg, MD, 20899. More information.

-June 18, 7:30 a.m. - 1:30 p.m., **MeriTalk's Cybersecurity Brainstorm** - The second annual Cyber Security Brainstorm on Wednesday, June 18, 2014 at the Knight Conference Center at the Newseum in Washington, D.C. The event will bring together savvy Federal cyber security experts to share best practices, collaborate on challenges, and discuss what is needed for the future of cyber security. As cyber security is front and center in 2014 for Federal IT management professionals, this half day program will examine the evolving dialogue on issues including continuous monitoring, information sharing, cloud security, and cyber threats. Knight Conference Center at the Newseum, 555 Pennsylvania Ave., N.W. More information.

-June 18, 6:00 p.m. – 9:00 p.m., **NovaInfosec Meetup** - If you are in the IT security business, like the idea of meeting to discuss the foibles of the industry, demo your recent discovery and conquest, or just drink a beer with like minded folks, then this meeting is for you. Velocity Five, 19286 Promenade Drive, Leesburg, VA, 20176. More information.

-June 19, 5:30 p.m. – 8:30 p.m., **ISSA NoVA Meetup** - This talk will be an introduction to dynamic malware analysis, and should be useful for anyone in a technical role in the information security field. Oracle Reston, 1910 Oracle Way, Reston, VA, 20190. More information.

-June 23-26, **Gartner Security Risk and Management Summit** – A look into the full spectrum of security and risk management emerging trends and market scopes within five role-based programs and a dedicated technical insights track. This year's summit features new coverage on chief information security officer (CISO) programs; risk management and compliance; and business continuity management. Gaylord National, 201 Waterfront Street, National Harbor, MD 20745. More information.

-June 24-25, **Cyber Awakening: Protecting a Nation's Security** – The AFCEA Cyber Symposium will explore the aspects of operational security of U.S. Government, DoD and industry networks, cyber cooperation among joint and coalition partners, and discuss

the training and development of the cyber workforce. Baltimore Convention Center, 1 W Pratt St, Baltimore, MD 21201. More information.

Legislative Lowdown

-The head of the House Intelligence Committee thinks the odds are good that the Senate will pass a long-delayed cybersecurity bill this year, writes The Hill. After a meeting with leaders of the Senate Intelligence panel on Wednesday, Rep. Mike Rogers (R-Mich.) said his hopes for action soon have returned. The House last April passed legislation to allow companies to share information about possible cyber threats with each other and the government, which advocates have said is necessary to make sure that possible hackers and online terrorists do not go unnoticed.

Cyber Security Policy News

-In a move bound to stir up some controversy given the company's reach and scale, Facebook said last week that it would not be honoring the do-not-track setting on web browsers. According to a story in Ad Age, "a Facebook spokesman said that's 'because currently there is no industry consensus.' Social-media competitors Twitter and Pinterest do honor the setting. Google and Yahoo do not. Facebook will honor the settings to limit ad tracking on iOS and Android devices, however."

-The The Federal Aviation Administration (FAA) is ordering Boeing to modify the technology aboard late-model 737 aircraft to prevent computer hackers from damaging the planes, U.S. Today writes. "The order published Friday in the Federal Register is effective immediately, although the agency allowed a comment period until July 21. The special conditions are urgent because the FAA is trying to avoid slowing down design and delivery of new planes, according to the agency."

-Telecom giant Vodafone disclosed last week that a small number of governments have direct access to communications flowing over its networks. In most countries where Vodafone operate, a warranted is needed to intercept communications, but in some countries police have a direct link to customers' phone calls and Web communications, reports the BBC.

-In other telecom news, the Federal Communications Commission (FCC) is pressing telecommunications industry providers to take the lead on improving cybersecurity -- or else. Reuters reports that. "The FCC in coming weeks will ask communications companies to report how, measurably, they are adopting the various voluntary best practices and codes of conduct they previously helped draft through a multi-stakeholder FCC advisory group. Another such advisory group is now also working on a review of industry best practices in cybersecurity." According to Reuters, the FCC will "begin to incorporate cybersecurity considerations into its routine regulatory work and will also help evaluate how the communications sector is adopting the minimum cybersecurity

standards that the government drafted with the industry's help in February." A copy of the FCC chairman's recent remarks on the targeted cybersecurity improvements is here (PDF).

-Cyber-intelligence sharing, as well as oversight of third parties, should be priorities for banking institutions, according to a new report published by the Financial Stability Oversight Council. The organization, chaired by the Secretary of the Treasury, "recommends that the Treasury Department work with banking regulators and other appropriate government agencies, such as the **Federal Financial Institutions Examination Council**, as well as private financial firms, to improve information sharing about cyber-threats and other risks facing the U.S. financial system." The council also warned about the dangers of insecure third-party systems, pointing to the break-in at Target, which exposed the personal and financial information of 110 million people and started with a phishing attack against one of the retailer's contractors.

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.