Cyber Security Experts Set Research Priorities At NIST Workshop To Secure Cyber-Physical Systems

Cyber Security Research Alliance Initiates Next Step to Define Key Research Topics with Government, Academia, and Industry to Address Cyber Security Vulnerabilities

GAITHERSBURG, Md., April 9, 2013 /PRNewswire/ -- Leading industry, government, and academic cyber security experts convened at the National Institute of Standards and Technology (NIST) for a workshop to establish a research agenda to address threats and vulnerabilities across multiple domains for a wide array of cyber-physical systems that are increasingly targeted by cyber attackers.

The industry-led Cyber Security Research Alliance (CSRA) and NIST hosted the two-day event focused on identifying and addressing threats and vulnerabilities for Cyber-Physical Systems (CPS), which includes industrial controls, data communications, and other IT systems that support critical infrastructure operations such as utilities, communications networks and security-sensitive government operations.

"Securing CPS is a top concern because of the potential for widespread physical and economic collateral damage that could result from a targeted and well-executed cyber attack," said Lee Holcomb, president of the CSRA and vice president of strategic initiatives, Lockheed Martin Information Systems & Global Solutions. "The research agenda developed collaboratively by researchers at NIST, leading academic institutions, and CSRA member companies, is designed to mitigate cyber threats to CPS and better secure our nation's critical infrastructure."

Workshop participants explored CPS research opportunities for several of the most complex areas in cyber security such as IT supply chain, government-industry information sharing on vulnerabilities, approaches to product assurance and trustworthy operational readiness. The group identified a specific set of research priorities that will appear in public documents to be published in the next several weeks. The documents will include key research objectives to inform industry, government and academic research activity in CPS.

"Cyberphysical systems – self-driving cars, smart buildings, advanced manufacturing systems, intelligent medical devices, and much more – are becoming central and essential to our everyday lives," said Chuck Romine, Director of NIST's Information Technology Laboratory. "These complex, IT-driven systems pose unique security challenges that will only be met through the combined effort of the commercial, academic and government sectors. This meeting brought together experts from all sectors to join forces in pursuing our shared goals."

About the CSRA: The CSRA is a private, non-profit research consortium formed in response to the growing need for increased public-private collaboration to address complex problems in cyber security. The founding members of the CSRA are Advanced Micro Devices (AMD), Honeywell, Intel Corporation, Lockheed Martin, and RSA/EMC. CSRA seeks to achieve coordinated industry participation to address national cyber security research and development strategic imperatives and bridge the gap between government-funded R&D and commercially available products and solutions in cyber security.

To learn more about CSRA, please visit our website athttp://www.cybersecurityresearch.org/

SOURCE Cyber Security Research Alliance

---

https://news.lockheedmartin.com/2013-04-09-Cyber-Security-Experts-Set-Research-Priorities-at-NIST-Workshop-to-Secure-Cyber-Physical-Systems