

Ensuring a Secure Supply Chain for Trusted Systems and Networks

Paul Popick (The Aerospace Corporation) - Paul.popick.ctr@osd.mil

Kristen Baldwin (Office of the Deputy Assistant Secretary of Defense for Systems Engineering) - Kristen.baldwin@osd.mil

Mitchell Komaroff (DoD CIO) - Mitchell.Komaroff@osd.mil

Barry Nutter (Lockheed Martin) - Barry.Nutter@LMCO.com

Mark Koehnke (Raytheon Corporation) - Mark_A_Koehnke@raytheon.com

Copyright © 2013 by Popick, Baldwin, Komaroff, Nutter, Koehnke. Published and used by INCOSE with permission

Abstract. The panel discussion will focus on the role of government and industry to secure the supply chain from malicious insertion and alteration of components and systems, and the notion that government would like industry to share in the risk, in tension with industry's inability to assume open-ended liability. System security challenges facing major programs include the increasing reliance on commercially available technology, complex supply chains that include thousands of suppliers across the globe, system interconnectedness and the identification and exploitation of system vulnerabilities. The threats to the supply chain include counterfeit for financial gain, malicious insertion, exfiltration of data, denial of service and compromise of mission effectiveness. International standards and industry standards to address these concerns are just emerging and do not yet provide a basis for resolution. Many of the commercial-off-the shelf (COTS) products have complex supply chains that are not secured to prevent alteration and malicious insertion. Open source is often incorporated into COTS and the COTS tools used to develop DOD subsystems and other COTS. These COTS and open source products are widely available for study, reverse engineering and exploitation of vulnerabilities. The complex supply chains and development processes of major acquisition programs (prime contractors, subcontractors, suppliers, and sub-suppliers) make it difficult for anyone to truly know what is in the system and where it came from. Systems engineering has to consider the vulnerabilities of the COTS products, the supply chain, the development environment, development process, and the system maintenance process, as well as the operational system. The system engineer must now not only worry about the performance of the system components during design trade-off but must also consider the security of the supply chain, the COTS products used in the system, and the information incorporated into the system where much of the development and manufacturing exist outside of traditional controls. Government needs industry to share the technical and cost risk and liability of securing the supply chain to ensure a competitive incentive to develop trusted systems. Industry needs to limit risk and liability, and cannot assume open ended liability for supply chains and component integrity that are outside of their control.

Biography

Paul Popick (The Aerospace Corporation) - Paul.popick.ctr@osd.mil

Paul Popick has 40 years experience as a program manager, systems engineering manager, systems engineer, and software development manager. In his current assignment he is supporting the program protection policy, methodology and review of major acquisition programs for the Office of the Deputy Assistant Secretary of Defense for Systems Engineering. Mr. Popick was one of the organizers of the May 2012 NDIA Program Protection Workshop, one of the instructors of the Oct 2012 NDIA program protection tutorial and a co-chair of the INCOSE System Security Engineering working Group. . In previous assignments, Mr Popick has led portions of major commercial and defense system integration programs for IBM Global Services and IBM Federal Systems Division. Mr. Popick has been an Adjunct Professor in project management at George Washington University, and in Systems Engineering at Johns Hopkins University. Mr. Popick is a Project Management Institute (PMI) certified Project Management Professional (PMP), and an IBM Certified Executive Project Manager. Mr. Popick is one of the originators of the IBM Global Services systems engineering method and has a patent pending for this work. Mr Popick received a Master of Science in Applied Mathematics from New York University and a Bachelor of Science from Southern Methodist

University.

Kristen Baldwin (Office of the Deputy Assistant Secretary of Defense for Systems Engineering) - Kristen.baldwin@osd.mil

Kristen Baldwin is the Principal Deputy in the Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD(SE)). Ms. Baldwin acts on behalf of the DASD and is responsible for engineering and technical workforce, policy, and acquisition program implementation across the Department of Defense (DoD). She is also overseeing the DoD's strategies for Engineering Resilient Systems and Trusted Systems Design. A member of the Senior Executive Service, Ms. Baldwin is also the acting Director for Systems Analysis. She leads modeling and simulation activities across DoD, system assurance, program protection, systems engineering for systems of systems, and SE research and development initiatives. She oversees the DoD Systems Engineering Research Center, a University Affiliated Research Center dedicated to advancing systems engineering methods, processes, and tools, and the MITRE National Security Engineering Center, a DoD Federally Funded Research and Development Center. Ms. Baldwin received a bachelor's degree in mechanical engineering from the Virginia Polytechnic Institute and a master's degree in systems management from the Florida Institute of Technology.

Mitchell Komaroff (DoD CIO) - Mitchell.Komaroff@osd.mil

Mitchell Komaroff serves as the Director, Trusted Mission Systems and Networks (TMSN), for the DoD Chief Information Officer (DoD CIO). He is primarily responsible for developing and implementing a strategy for mitigating national security risks to DoD arising from the increasing globalization of the information and communications technology (ICT) sector, and the telecommunications infrastructure. TMSN is the DoD CIO focal point for: transactional risk management in Committee on Foreign Investment in the US (CFIUS) and Federal Communications Commission Licensing matters, and developing policies and procedures for implementing the Department's Trusted Systems and Networks strategy for reducing global supply chain risk. Since coming to the Office of the DoD CIO, Mitchell Komaroff has worked to implement software and systems assurance across the Department of Defense. Before coming to the Office of the DoD CIO, Mitchell Komaroff was a Computer Scientist with the Defense Information Systems Agency (DISA) and with industry, where he worked network quality of service (QoS), IA Architecture and Information Management issues. Mitchell Komaroff holds a Masters of Science degree in Mathematics from George Mason University and a Juris Doctor degree from the University of Maryland, School of Law.

Barry Nutter (Lockheed Martin) - Barry.Nutter@LMCO.com

Mr. Barry C. Nutter Lockheed Martin Fellow for Cyber Security Lockheed Martin Information Systems & Global Solutions Barry Nutter has 38 years experience as a cyber security subject matter expert, information system architect, systems engineer, systems security engineer, and intelligence officer. In his current assignment as a Lockheed Martin Fellow, he provides cyber security and solutions architecture technical leadership and support to intelligence community, federal government, and commercial customers. As a Lockheed Martin corporate cyber security domain advocate, he remains abreast of cyber security threat trends, offensive tools and tradecraft, and defensive security solutions and best practices. In previous Lockheed assignments, Mr. Nutter was the chief security architect for several major multi-year architectural transformation programs for intelligence community and government customers. He is a Certified Information System Security Professional and Advanced Information System Architect. His earlier career as a CIA intelligence officer spanned two decades and three directorates. His assignments included management and line roles in all-source intelligence analysis and production, as well as human and technical clandestine overseas collection operations. Mr. Nutter received a Master of Arts in International Relations from the University of Southern California and a Bachelor of Arts from the Ohio State University.

Mark Koehnke (Raytheon Corporation) - Mark_A_Koehnke@raytheon.com

Mark Koehnke has 35 years of experience as a microwave design engineer, program manager and system anti-tamper engineering since joining Raytheon in 1978. He has held roles of increasing responsibility over the years as a design engineer of ultra low noise microwave oscillators and radar exciter subsystems, as a section manager for Low Noise RF Technology and holds two patents in the field of low noise microwave

technology. With the emergence of the new DoD AT policy, as an annex to a Program Protection Plan (PPP) in 1999, his career took a hard turn from microwave design and into the protection of DoD critical technology. Mark is currently the manager of the Cyber Solutions and Integration Department within the Systems Architecture, Design and Integration Directorate at Raytheon's Integrated Defense Systems business unit. In this role, Mark is responsible for providing solutions to program Anti-Tamper, Information Assurance and Cyber Security needs which all fall under the expanding scope of PPP requirements. The responsibility of his department has expanded to keep pace with the expanding scope of the DoD's Program Protection Planning requirements to also include addressing Supply Chain Risk Mitigation and Software Assurance requirements, methodologies and solutions. Mr. Koehnke received a Bachelor of Science in Electrical Engineering from Penn State University.