Defense Acquisition University

Cybersecurity and Modular Open Systems Approach

October 26, 2017

Bill Decker
Defense Acquisition University
7115 Old Madison Pike
Huntsville, AL 35806
724-612-0999
For further info: tim.denman@dau.mil

Defense Acquisition University

www.DAU.mil

Approved for Public Release

Ground rules

- This is a discussion, not a lecture
- Your opinions and viewpoints are welcomed
- There are no right/wrong answers

Agenda

- Introduction
- Modular Open Systems Approach
  - What is it?
  - Why do we want (or have) to do it?
  - What does it mean to the SE?
- Cybersecurity
  - Critical requirement, often not clearly stated
- Discussion
  - How can we serve both masters?
- Conclusion

Introduction

- Assumptions (remember what they do)
  - MOSA – open means publically available technical data and software
  - Cybersecurity means no vulnerability to cyber attack

FY17 NDAA MOSA Definition
Sec. 805, §2446a (b)(1) p.253

- Congressional MOSA Definition – FY17 Legislation
- An integrated business and technical strategy that:
  - (A) Employs a modular design that uses major system interfaces between a major system platform and a major system component, between major system components, or between major system platforms;
  - (B) Is subjected to verification to ensure major system interfaces comply with, if available and suitable, widely supported and consensus-based standards;
  - (C) Uses a *system architecture that allows severable major system components at the appropriate level to be incrementally added, removed, or replaced throughout the life cycle of a major system platform to afford opportunities for enhanced competition and innovation while yielding*-
    - (i) Significant cost savings or avoidance; (ii) schedule reduction; (iii) opportunities for technical upgrades; (iv) increased interoperability, including system of systems interoperability and mission integration; or (v) other benefits during the sustainment phase of a major system;
  - (D) complies with the technical data rights set forth in Sec 2320, title 10.

MOSA Community Definitions

- Current MOSA Terminology – OSA Contract Guidebook
  - “Modular Open Systems Approach or MOSA” is the DoD’s implementation of Open Systems. Within the MOSA context, programs should design their system based on adherence to the following five MOSA principles: Establish an Enabling Environment., Employ Modular Design, Designate Key Interfaces, Use Open Standards, Certify Conformance. *[A Modular Open Systems Approach (MOSA) to Acquisition, OSJTF]*
  - “Open Systems Approach” means an integrated business and technical strategy that employs a modular design and, where appropriate, defines key interfaces using widely supported, consensus-based standards that are published and maintained by a recognized industry standards organization. [*A Modular Open Systems Approach (MOSA) to Acquisition, OSJTF*]

https://www.dau.mil/cop/mosa/Pages/Topics/Terms-and-Definitions.aspx

SE activities

- Identify modules in the system
  - May be hardware or software or combination
  - DoDAF architectural artifacts may be used
  - Internal to system, as well as system to system
- Identify key interfaces
  - Specify standards to be employed
- Work with PM to identify and ensure delivery of needed technical data/software
- Manage technical risk for PM

Cybersecurity Implementation into Acquisition Programs – 3 Sub-processes

- **Requirements Generation**
  - The PM team and requirements developers must be cognizant of the mandatory System Survivability KPP, which includes cyber survivability requirements
  - PMs will need to deliver systems that are able to operate and complete their missions in cyber-contested environments.

- **Acquisition and Program Management**
  - PMs must address cybersecurity in program reviews, including Deep Dives, In-Process Reviews, and Overarching Integrated Product Team (OIPT) meetings
  - The PM needs to build an IPT structure that includes cybersecurity expertise.

- **Systems Engineering and Test and Evaluation**
  - Implementation of a disciplined systems engineering process that includes cybersecurity is required from requirements analysis through design, test and evaluation, fielding, sustainment, and decommissioning.
  - The PM must develop a cybersecurity Test and Evaluation (T&E) strategy, allocate resources for cybersecurity T&E, and ensure they are described in the TEMP.

DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle , May 2015, Version 1.0

SE Role in Cybersecurity

- Cybersecurity strategy
  - Identify cyber risks
  - Work with IPTs to determine controls that are appropriate
  - Implement controls/reporting
  - Integration with Program Protection Plan (PPP)
  - A multi-disciplined Systems Security Engineering (SSE) WG can provide an integrated PPP that includes the Risk Management Framework (RMF), Supply Chain Risk Management (SCRM) and protection of Critical Program Information (CPI).

- Work with internal/external cyber assets
  - DoD and Service CIOs, NSA, DISA, etc.
  - Authorizing Officials (AO) and Security Control Assessors (SCA)

Discussion

- Pros vs Cons of public interfaces

Pros	Cons
Identified early	Identified early
Controls applied from start	Exploitation has more time
Benefits of MOSA	One exploit approach works for many applications
More open evaluation of the interfaces	Monocultures: Same vulnerabilities
??	

Conclusion

- Challenge is to implement MOSA without compromising security
  - Must be planned from start
  - Shortcuts lead to risk
- PMs should be intimately involved