Building the Case for Secure MOSA Using Systems Thinking Methodologies

Sponsor: OUSD(R&E) | CCDC

By
Ms. Giselle M. Bonilla-Ortiz

7th Annual SERC Doctoral Students Forum
November 18, 2019
FHI 360 CONFERENCE CENTER
1825 Connecticut Avenue NW, 8th Floor
Washington, DC 20009

www.sercuarc.org

Agenda

- Introduction
- Perspectives: Identifying Secure MOSA Stakeholders
- Secure MOSA System Boundary
- Inputs to Secure MOSA
- Value Adding Processes: Identifying the benefits of a Secure MOSA
- Secure MOSA Shaping Forces
- Telling the Story: Visualizing Secure MOSA Relationships Using Systemigrams
- Conclusion
- Ongoing Research
- References

Introduction

- Modular Open Systems Approach (MOSA) is the Department of Defense (DoD) method to designing composable systems that follow open standards and can be acquired from independent vendors

- Equally as important is the DoD's desire to mitigate the risks of losing critical program information and to maintain operability of their systems during potential cybersecurity attacks

- This presentation introduces the concept of a Secure MOSA and utilizes Systems Thinking methodologies to understand the complex relationships contained in this system

Perspectives: Identifying Secure MOSA Stakeholders

Government

- Congress
- Warfighter
- Department of Defense
  - OSD and DASD (SE)
  - Program Management Office
  - Acquisition Officers
  - Logistics
  - Systems Engineers
  - Systems Security Engineers
  - Contracting Officers
  - Chief Development Testers
  - ATEA
- Intelligence and Counterintelligence
- JAPEC
- JFAC
- NIST

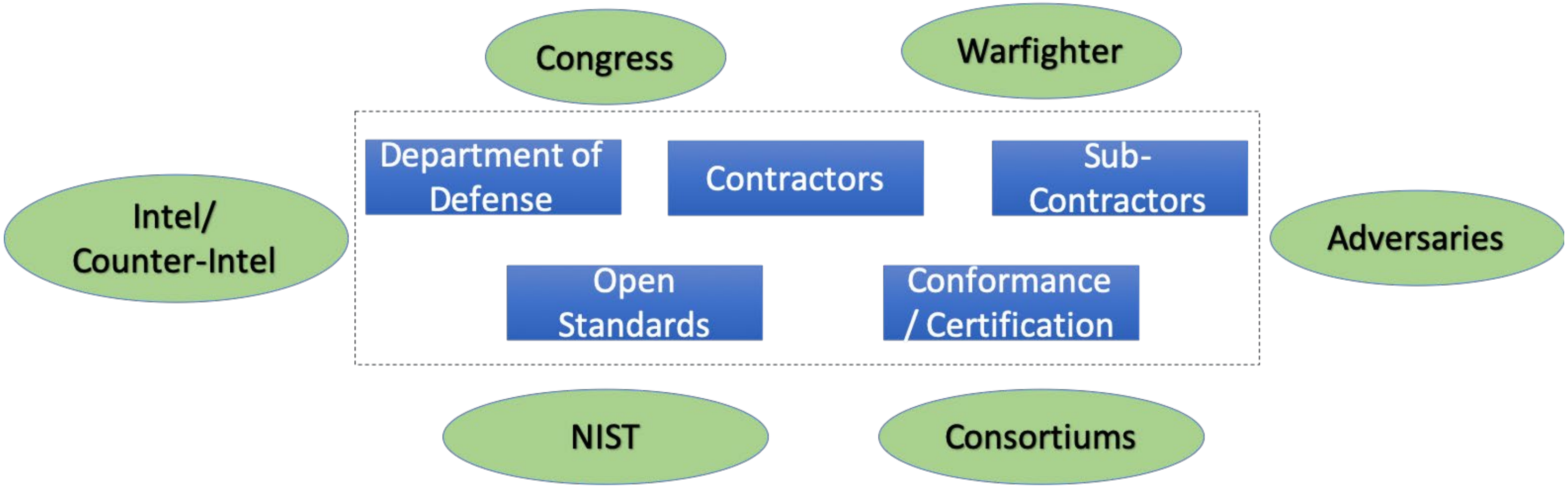
Industry

- Contractors
  - Program Managers
  - Systems Engineers
  - Systems Security Engineers
  - Training
  - Security
  - Production and Operations
- Sub-contractors / suppliers

Other organizations

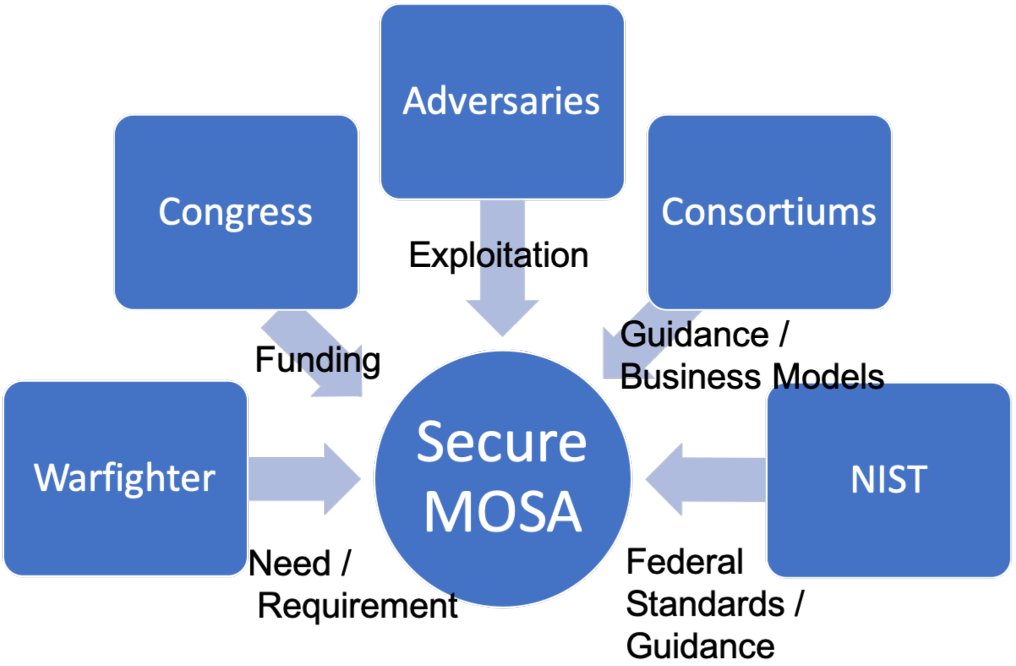
- Open Standards
- Consortiums
- Conformance and Certification Agencies
- Adversaries and Exploiters

Secure MOSA System Boundary



- Determine the system boundary to scope analysis
- Entities outside the boundary influence decisions and design – see inputs, next slide
  - These relationships may cross the boundary

Inputs to Secure MOSA



- Inputs to Secure MOSA impact decisions throughout the system's lifecycle
- Known or suspected exploiter attacks will influence security capabilities design
- Funding received impacts scope a program can undertake
- NIST and Consortiums provide guidance and best practices
- Requirements are driven by warfighter needs

Identifying the Benefits of Secure MOSA

- MOSA and SSE have well understood benefits
- Benefits of MOSA: enhanced competition, innovation, cost savings/avoidance, improved interoperability
- Benefits of SSE: threat mitigation, address system loss scenarios, protection of capabilities that enhance warfighter advantage

Rapid upgrades of compromised modules

Securing IP / CPI while still improving interoperability

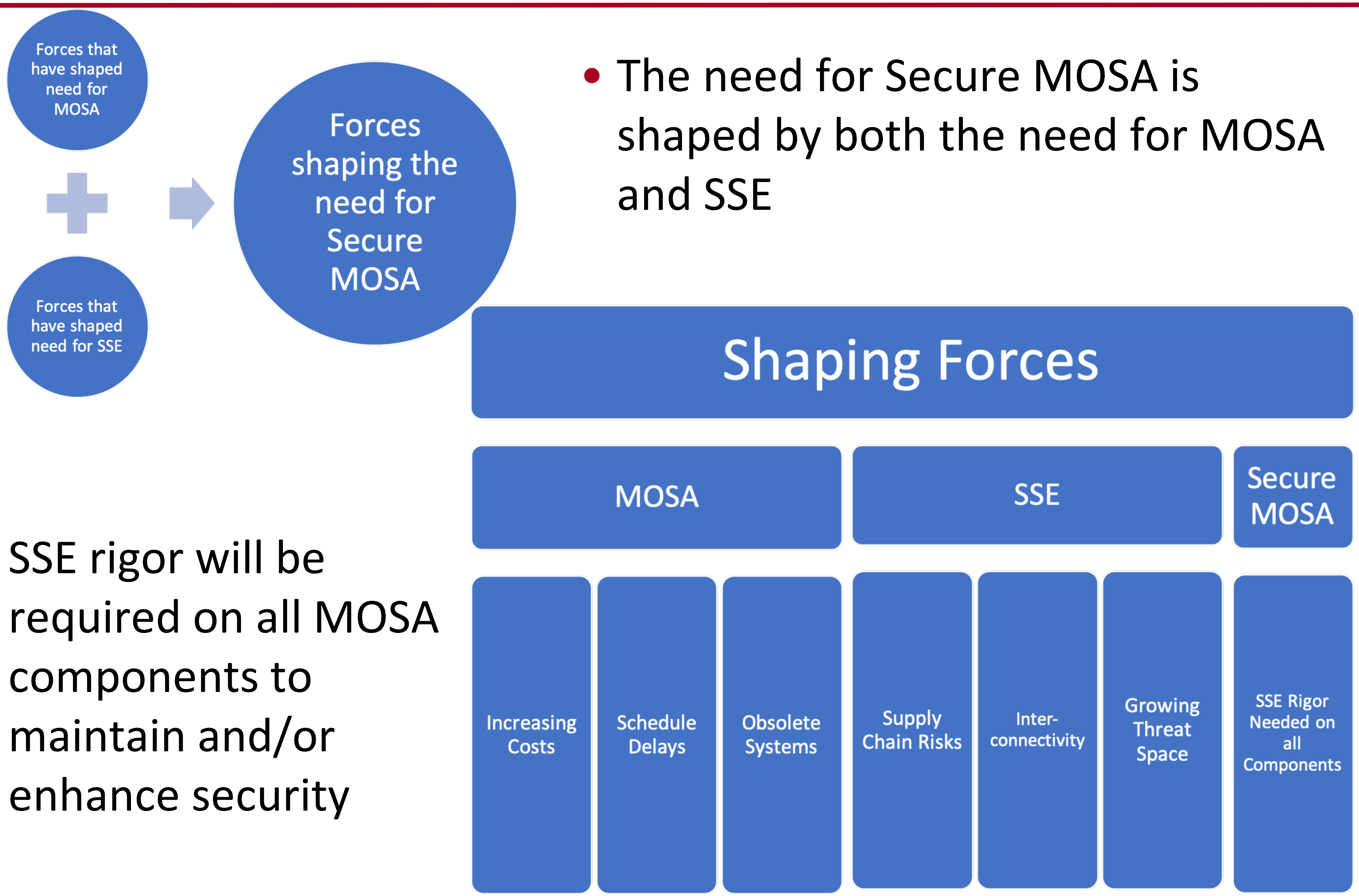
Design for Authenticity

Rapid upgrades of modular security components

- Establishing the value of SSE incorporated into MOSA to determine benefits

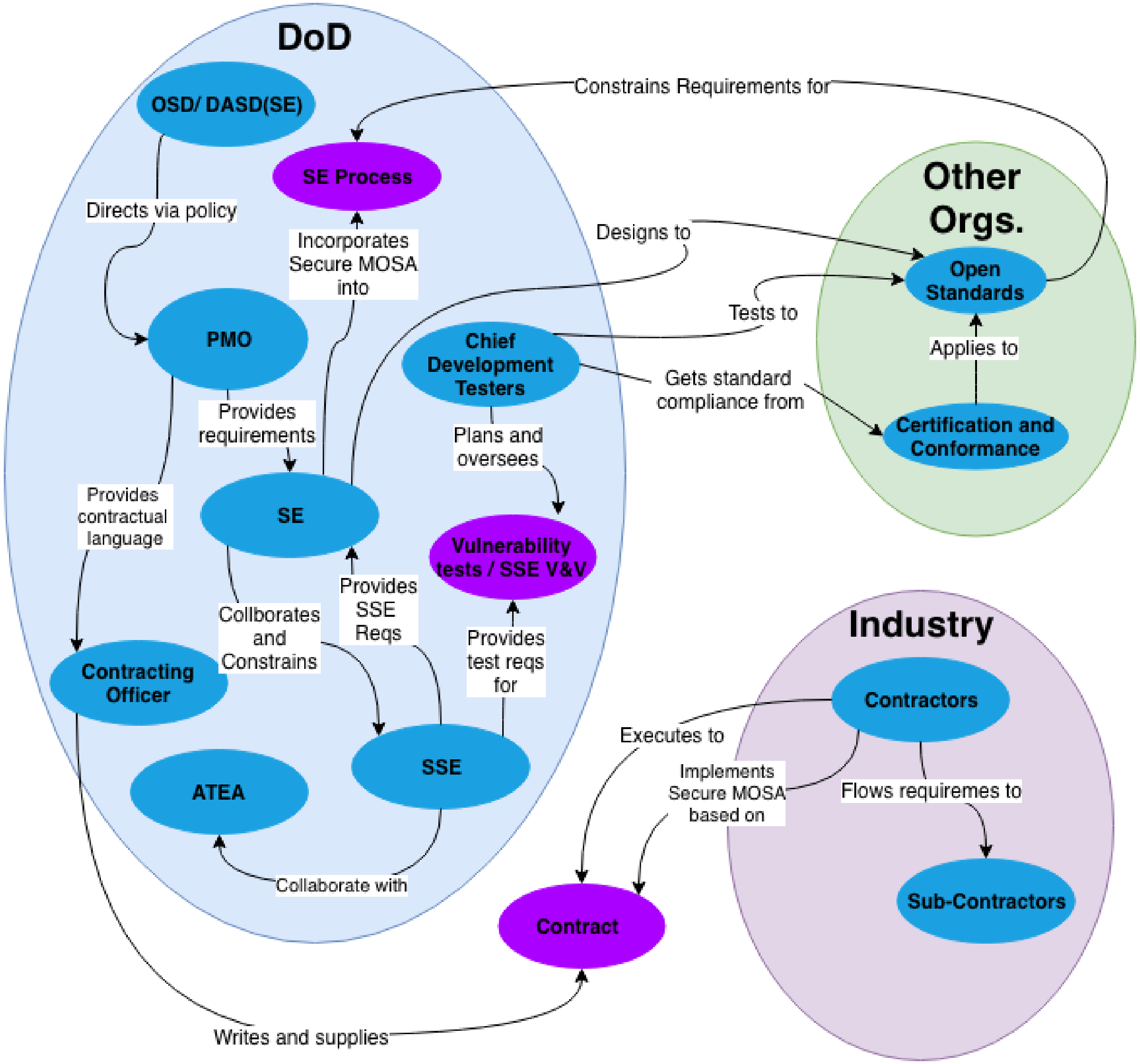
Secure MOSA Shaping Forces

- The need for Secure MOSA is shaped by both the need for MOSA and SSE


Forces that have shaped need for MOSA
Forces that have shaped need for SSE
Forces shaping the need for Secure MOSA
Shaping Forces
MOSA
SSE
Secure MOSA
Increasing Costs
Schedule Delays
Obsolete Systems
Supply Chain Risks
Inter-connectivity
Growing Threat Space
SSE Rigor Needed on all Components

- SSE rigor will be required on all MOSA components to maintain and/or enhance security

Telling the Story: Secure MOSA Relationships



- Used Systemigram to analyze and visualize relationships between stakeholders and components within the Secure MOSA system

Conclusion

- MOSA, if adopted effectively by the DoD and its contractors, will result in significant cost savings, rapid upgrades and greater advantage for the warfighter
- Ensuring that Program Protection and Systems Security Engineering are incorporated into the MOSA lifecycle will be paramount in the approach's success and maintaining technological advantage over adversaries
- Systems Thinking provides excellent tools that can help gain a deeper understanding of the problem scope that is incorporating SSE practices into MOSA

Ongoing Research

- Leveraging Cyber-Physical Systems (CPS) to Identify Security Patterns for Secure Modular Open Systems Approach (MOSA) Designs
- Using this research to expand on the value adding processes identified:
  - Rapid upgrades of compromised modules
  - Securing Intellectual Property (IP)/CPI while still improving interoperability
  - Design for Authenticity
  - Rapid upgrades of modular security components
- Identifying parallels and commonality, security patterns, protection approaches

References

- Openness in military systems part 1: Analysis & applications. MILCOM 2012 - 2012 IEEE Military Communications Conference, MILITARY COMMUNICATIONS CONFERENCE, 2012 - MILCOM 2012. 1, 2012. ISSN: 978-1-4673-1729-0.
- Defense Acquisition Guidebook, Chapter 9: Program Protection, Version 5
- N. Davendralingam, C. Guariniello, S. Tamaskar, D. DeLaurentis, and M. Kerman, “Modularity research to guide MOSA implementation,” The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, Jan. 2018.)
- K. R. Hibbert, “A need for systems architecture approach for next generation mine warfare capability,” Naval Postgraduate School, Monterrey, California, 2006.
- P. Zimmerman, M. Ofori, D. Barrett, J. Soler, and A. Harriman, “Considerations and examples of a modular open systems approach in defense systems,” Journal of Defense Modeling & Simulation, Apr. 2018.
- http://acqnotes.com/acqnote/careerfields/system-security-engineering
- K. Baldwin, J. Dahmann, and J. Goodnight, “Systems of Systems and Security: A Defense Perspective,” INSIGHT, vol. 14, no. 2, pp. 11–14, Jul. 2011.
- United States Government Accountability Office (GAO), “DOD Efforts to Adopt Open Systems for Its Unmanned Aircraft Systems Have Progressed Slowly”, July 2013.
- R. Harrison, “Future-Proof Today’s Test Systems to Handle Tomorrow’s Devices,” EE: Evaluation Engineering, vol. 51, no. 9, pp. 54–54, Sep. 2012.
- https://www.afmc.af.mil/News/Article-Display/Article/1752516/services-improve-interoperability-through-common-data-standards/
- K. Baldwin, P. R. Popick, J. F. Miller, and J. Goodnight, “The United States Department of Defense revitalization of system security engineering through program protection,” in 2012 IEEE International Systems Conference SysCon 2012, 2012, pp. 1–7.
- J. Dahmann, G. Rebovich, M. McEvilley, and G. Turner, “Security engineering in a system of systems environment,” in 2013 IEEE International Systems Conference (SysCon), 2013, pp. 364–369.
- Boardman, J. and B. Sauser, Systems Thinking: Coping with 21st Century Problems. 2008, Boca Raton, FL: Taylor & Francis / CRC Press.