SYSTEMS ENGINEERING RESEARCH CENTER
8TH ANNUAL SERC DOCTORAL STUDENTS FORUM
12TH ANNUAL SERC SPONSOR RESEARCH REVIEW
HOSTED VIRTUALLY ON : NOVEMBER 17-18, 2020
STEVENS INSTITUTE OF TECHNOLOGY THE INNOVATION UNIVERSITY
Raytheon Technologies

Identifying Security Patterns for Modular Open Systems

Giselle Bonilla-Ortiz

RESEARCH TASK / OVERVIEW

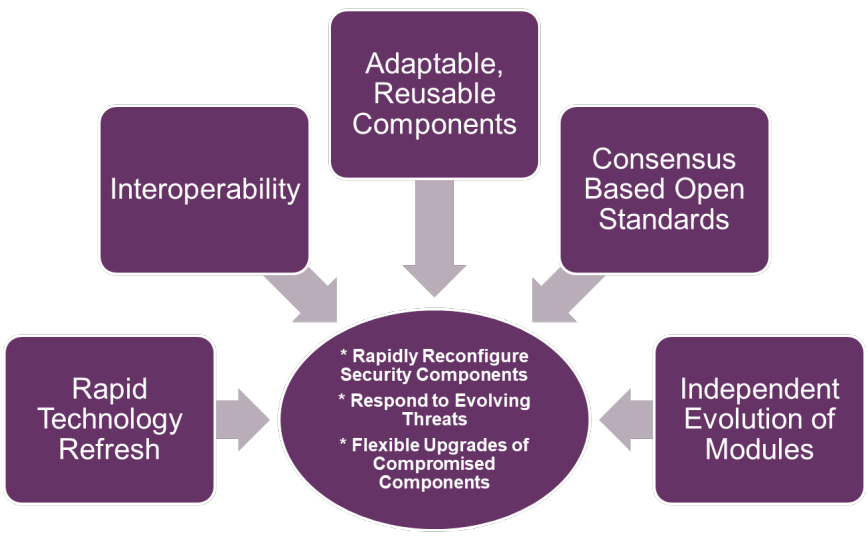
- Modular Open Systems Approach (MOSA) is the Department of Defense (DoD) method to designing composable systems that follow open standards and can be acquired from independent vendors
- Equally as important is the DoD's desire to mitigate the risks of losing critical program information and to maintain operability of their systems during potential cybersecurity attacks
- This research aims to determine attack vectors to modular open systems and to explore security patterns to mitigate these threats

GOALS & OBJECTIVES

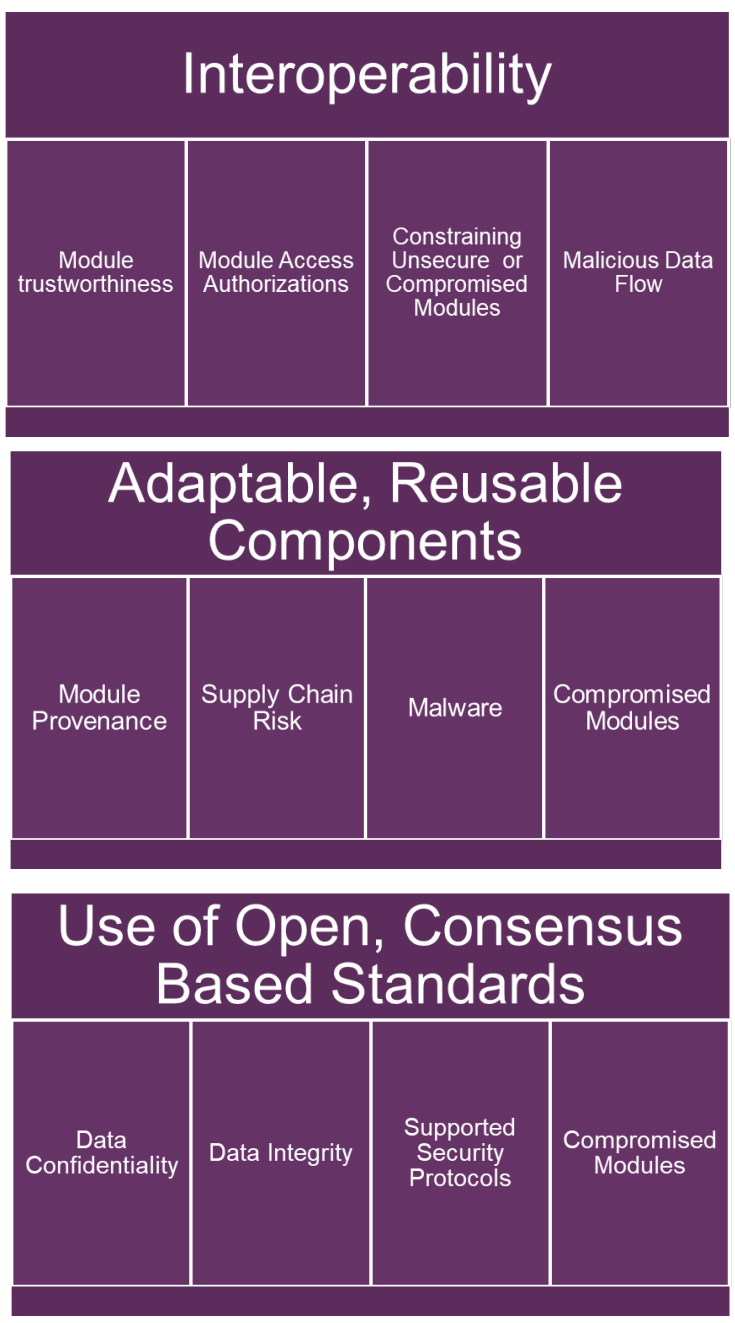
- The topics presented are part of an in-progress systematic literature review by the author with the purpose of establishing the knowledge base available to execute Systems Security Engineering for Modular Open Systems

DATA & ANALYSIS

Enhancing Security with MOSA principles



Security challenges of modular open systems



METHODOLOGY

In progress Systematic Literature Mapping (SMS) based on the following research questions:

- Initial Research Question:
  - How do we build a modular open system without compromising its security posture?
- Research Sub-questions:
  - What properties of modular open systems can potentially enhance security?
  - What properties of modular open systems can potentially compromise security?
  - What are the attack vectors that threaten modular open systems?
  - What security patterns can be applied to modular open systems to mitigate these threats?
  - Can applying security patterns from other similar concepts, such as Cyber Physical Systems (CPS) and System of Systems (SoS) reduce the threats and vulnerabilities of MOSA systems?

FUTURE RESEARCH

- Complete Systematic Mapping Review
- Baseline publicly available literature on the intersection between MOSA and Security
- Research Design

CONTACTS / REFERENCES

Giselle Bonilla-Ortiz gbonilla@stevens.edu
Advisor: Dinesh Verma, Ph.D dinesh.verma@stevens.edu

- B. Shirley, Q. Young, P. Wegner, J. Christensen, and J. Janicik, "Multi-layered Security Approaches for a Modular Open Network Architecture-based Satellite," presented at the 28th Annual AIAA/USU Conference on Small Satellites, 2014.
- A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security—A Survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017, doi: 10.1109/JIOT.2017.2703172.
- 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, doi: 10.1177/1548512917751281.
- G. Bonilla-Ortiz and D. Verma, "The Need for a Secure Modular Open Systems Approach (MOSA): Building the Case Using Systems Thinking Methodologies," in 2020 IEEE Systems Security Symposium (SSS), Jul. 2020, pp. 1–4, doi: 10.1109/SSS47320.2020.9197726.
- C. P. Collier, I. Lipkin, S. A. Davidson, R. Baldwin, M. C. Orlovskye, and T. Ibrahim, "Sensor Open System Architecture (SOSA) evolution for collaborative standards development," Anaheim, California, United States, Apr. 2017, p. 1020502, doi: 10.1117/12.2265841.