Identifying Security Patterns for Modular Open Systems

Ms. Giselle Bonilla-Ortiz

8th Annual SERC Doctoral Students Forum
HOSTED VIRTUALLY ON: November 17, 2020
www.sercuarc.org
Agenda

- Introduction
- Research Questions
- Benefits and Properties of Modular Open Systems Approach (MOSA)
- Enhancing Security with MOSA Principles
- Benefits to Securing Modular Open Systems
- Security Challenges of Modular Open Systems
- Leveraging Security Challenges of Cyber Physical Systems (CPS)
- Existing Modular Open Systems Standards: Security Lessons Learned
- Conclusion
- 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 research aims to determine attack vectors to modular open systems and to explore security patterns to mitigate these threats.

- 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.
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?
Benefits and Properties of MOSA

<table>
<thead>
<tr>
<th>Improve Agility</th>
<th>Cost Avoidance and Savings</th>
<th>Interoperability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rapid Technology Refresh</td>
<td>Efficient Logistics and Maintenance Strategies</td>
<td>Adaptable, Reusable Components</td>
</tr>
<tr>
<td>Open Consensus-Based Standards</td>
<td>Independent Evolution of Modules</td>
<td>Sharing of Modular Components Across Weapon Systems</td>
</tr>
</tbody>
</table>

(Zimmerman et al. 2018)

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.
Enhancing Security with MOSA Principles

* Rapidly Reconfigure Security Components
* Respond to Evolving Threats
* Flexible Upgrades of Compromised Components

Interoperability

Adaptable, Reusable Components

Consensus Based Open Standards

Rapid Technology Refresh

Independent Evolution of Modules

(Zimmerman et al. 2018)
Benefits to Securing Modular Open Systems

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

(Bonilla-Ortiz, Verma 2020)
Security Challenges of Modular Open Systems

### Interoperability

<table>
<thead>
<tr>
<th>Module trustworthiness</th>
<th>Module Access Authorizations</th>
<th>Constraining Unsecure or Compromised Modules</th>
<th>Malicious Data Flow</th>
</tr>
</thead>
</table>

- Module 1A
- Module 2
- Module 3

(Zimmerman et al. 2018, Shirley et al. 2014)

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.
Security Challenges of Modular Open Systems

Adaptable, Reusable Components

<table>
<thead>
<tr>
<th>Module 1A</th>
<th>Module 2</th>
<th>Module 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Compromised Modules</td>
<td>Supply Chain Risk</td>
</tr>
<tr>
<td>Module Provenance</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.
Security Challenges of Modular Open Systems

### Use of Open, Consensus Based Standards

<table>
<thead>
<tr>
<th>Data Confidentiality</th>
<th>Data Integrity</th>
<th>Supported Security Protocols</th>
<th>Compromised Modules</th>
</tr>
</thead>
</table>

- What security protocols does the selected open standard support?
- Do the protocols meet program needs?

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.
Leveraging Security Challenges of CPS

- Can CPS properties and security patterns be leveraged in understanding security for modular open systems?
  - Heterogeneity of building blocks
    - Commercial of the Shelf (COTS) Devices
    - Proprietary Components
    - Every component, as well as their integration, could contribute to an attack vector
  - Potentially large number of stakeholders
    - Can lead to uncoordinated changes of modules
    - How could change management aid in maintaining the security posture of the whole system?
  - Standard interfaces enable use of legacy components and COTS
    - Vulnerabilities at the boundaries of integration
    - Integration must be done with security in mind to minimize risks (Humayed et al. 2017)
Existing and Emerging MOSA Standards: Security Lessons Learned

- It is critical to perform security use cases and needs analyses

- Understand common threat vectors

- Develop and use common security reference architectures
  - Leverage existing modular open standards (e.g. Sensor Open System Architecture - SOSA)

- Modularize security patterns when possible
  - Standardized security components and algorithms
  - Usable security components

- Plan for a scalable configuration and phased deployment of security

- Enable for upgradeable and extensible security components for evolving requirements

(Collier et al. 2017)
Conclusion

• Understanding threat vectors for Modular Open Systems and leveraging Cyber Physical Systems security concerns may help provide inputs for reference security architectures and composable security patterns

• Research in progress to baseline publicly available literature on the intersection between MOSA and Security
References


Giselle Bonilla-Ortiz is a Systems Security Engineer (SSE) at Raytheon Missiles and Defense in Tucson, AZ. She has over 13 years of experience in software and systems engineering, cryptographic key management and application and secure processing solutions architecture. Giselle has a BS in Computer Engineering from the University of Puerto Rico at Mayagüez and a MS in Systems Engineering from the Johns Hopkins University. In 2018, Giselle began her doctoral studies in Systems Engineering at Stevens Institute of Technology and is a Systems Engineering Research Center (SERC) Doctoral Fellow.

In addition to her career and educational pursuits, Giselle is a triathlete and trail runner who has completed five half-Ironman races and a 50km trail running event.