Leveraging Systems Modeling to Assess and Mitigate Cyber-Based Mission Risk: A Cybersecurity Architecture Framework

Everett Oliver
Dr. Shahram Sarkani
Dr. Thomas Mazzuchi
October 2018
Modern organizations depend on IT systems that face a steady stream of cyber threats. In response, cybersecurity vendors produce a wide range of cyber defense products and tools. The challenge lies in developing cybersecurity strategies tailored to specific organizations and systems.
Many solutions are available for different parts of the cybersecurity problem.

- NSA IAD’s Top-10 list guides many of the solutions\textsuperscript{13}
- DISA’s Security Technical Implementation Guides (STIGs) provide IT configuration guidance\textsuperscript{26}
- Software patches provide updates for identified vulnerabilities
- A wide range of tools address different threats: access control, whitelisting, IDS/IPS, anti-virus/anti-malware, etc.
Cybersecurity Research Directions

A short list would include these and many more:

- New Vulnerabilities\textsuperscript{15}
- Integrated/Automated tools\textsuperscript{16}
- Risk scoring approaches\textsuperscript{3,5,16}
- Heuristics\textsuperscript{19}
- Modeling and Simulation\textsuperscript{1,7,12,17,18,20,27,29}
- Security extensions to SysML\textsuperscript{2}
What’s Missing?

With all the work that has been done and is being done in cybersecurity, what is missing?

A systems approach that treats cyber threats as mission-impacting problems that need solutions tailored to each organization.\textsuperscript{3,5,22}
Multi-Level Cybersecurity Challenge

- An organization derives its capabilities from different levels in its hierarchy.
- However, cybersecurity challenges also arise at different levels within the organization.

Impact Dependency Graph (Jakobson, 2011)
Leveraging Systems Engineering

What can Systems Engineers bring to the multi-level cybersecurity challenge?

• A systems engineering/architecture perspective – understanding how and why all the pieces fit together (the holistic view). 4,22,23,25

• Tools for connecting systems architecture with analysis techniques such as modeling and simulation. 8
Systems Modeling Overview

The Four Pillars of SysML (OMG website, 2018)
Test System Example
## Missions

<table>
<thead>
<tr>
<th>#</th>
<th>Mission</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Make money by producing and selling products</td>
<td>Company</td>
</tr>
<tr>
<td>1.1</td>
<td>Develop and distribute rules and priorities</td>
<td>Management</td>
</tr>
<tr>
<td>1.2</td>
<td>Sell products</td>
<td>Sales</td>
</tr>
<tr>
<td>1.3</td>
<td>Specify production to satisfy sales</td>
<td>Business Office</td>
</tr>
<tr>
<td>1.3.1</td>
<td>Configure production systems</td>
<td>Engineering</td>
</tr>
<tr>
<td>1.3.1.1</td>
<td>Troubleshoot and repair production systems</td>
<td>Engineering</td>
</tr>
<tr>
<td>1.3.2</td>
<td>Make products</td>
<td>Production</td>
</tr>
<tr>
<td>1.3.3</td>
<td>Report production status</td>
<td>Engineering</td>
</tr>
<tr>
<td>1.3.3.1</td>
<td>Generate production alarms</td>
<td>Production</td>
</tr>
<tr>
<td>1.4</td>
<td>Protect company assets</td>
<td>Company</td>
</tr>
<tr>
<td>1.4.1</td>
<td><strong>Protect business financial records</strong></td>
<td>Business Office</td>
</tr>
<tr>
<td>1.4.2</td>
<td>Protect proprietary product information</td>
<td>Engineering</td>
</tr>
</tbody>
</table>
SysML for Headquarters Interfaces

Diagrams from GENESYS 6.0, Vitech Corporation®
Protecting Business Records

The links through the Internet are encrypted except for the DMZ connection.

The DMZ connection presents a vulnerability unless it is isolated from the remainder of the Headquarters network.

Diagrams from GENESYS 6.0, Vitech Corporation
Are the business records protected?

Protecting the business records

Even through the primary links from each site through the Internet are encrypted, the company’s business records are at risk.

The DMZ presents a potential path through the Headquarters Site to attack the business systems despite the secure tunnels.
Network Change to Mitigate Risk

Diagrams from GENESYS 6.0, Vitech Corporation®
Extending the Use of Systems Modeling

- This example relied on the simple application of systems modeling and analysis displayed through the modeling diagrams.⁸
- For more sophisticated analyses, systems models can provide the framework for automating data analysis and modeling and simulation.
- SysML and model based systems engineering tools on the market provide application programming interfaces (APIs) to support multi-level cybersecurity research and assessments of specific system implementations.⁶,⁸,²¹
A Cybersecurity Architecture Framework for Leveraging Systems Modeling

• To leverage the capabilities of systems modeling and apply a holistic approach to cybersecurity, we propose a cybersecurity architecture framework.

• This architecture framework would combine the structures, behaviors, and parametric capabilities of the system models with analytical tools to support an enhanced systems engineering approach to cybersecurity.
The Cybersecurity Architecture Framework
Cybersecurity Architecture Framework Application to Current Practices

- Reusing Systems Engineering efforts that produce the systems models.\(^8\)
- Capturing known cybersecurity considerations in modeling constructs:
  - Attack trees and attack propagation\(^{13,24}\)
  - Vulnerabilities in homogeneous systems\(^{13}\)
  - Attack surfaces\(^{13}\)
Cybersecurity Architecture Framework
Advancing Systems Engineering Research

• Identifying extensions to SysML and model based systems engineering tools to support cybersecurity

• Applying systems engineering to future cybersecurity research:
  • Speculative execution vulnerabilities
  • Methods to jump air gaps
  • Applications of game theory, stochastic modeling, and other analytical techniques
  • Supply chain impacts
  • Cyber physical systems
Summary

• Cybersecurity Architecture Framework provides a structure for applying systems modeling techniques and analytical tools to cybersecurity
• Leverages capabilities of systems modeling to address the multi-level challenges of cybersecurity in a holistic manner
• Supports system development lifecycle applications and cybersecurity research
Questions?
Contact Information

Everett Oliver, George Washington University (Ph.D. Candidate)
everettoliver@gwu.edu
(814) 414-5210

Dr. Shahram Sarkani, Ph.D., P.E., George Washington University
sarkani@gwu.edu
(888) 694-9627

Dr. Thomas Mazzuchi, D.Sc., George Washington University
mazzu@gwu.edu
(888) 694-9627
References


References (cont.)


References (cont.)


