Secure Sourcing of COTS Products:
A Critical Missing Element in Software Engineering Education

Nancy R. Mead, Carnegie Mellon University
Anne Kohnke, University of Detroit Mercy
Dan Shoemaker, University of Detroit Mercy
Introduction

• Software engineering education is justifiably focused on the development of software artifacts.

• According to the SWEBOK, software engineering is: “The application of a systematic, disciplined, quantifiable approach to the development, operation, and maintenance of software.”

• However, the vast majority of software used in organizations is COTS.

• Often, the provenance is unknown due to the supply chain.
Introduction

• The acquirer rarely knows which supplier did what work.

• The possibility of the insertion of malicious code or counterfeit parts is real.

• The emphasis in software engineering education is on good design, secure coding and effective testing.

• However, many business applications are no longer developed as stand-alone but require interoperability with a variety of other applications.
Introduction

• Curricula do not fully address the product and programmatic interdependencies when multiple applications are used.

• There is little systematic knowledge to guide practitioners in the formal assurance that COTS products meet specifications and do NOT contain unwanted functionality.

• Specifically, the educational focus should be on how to ensure the code in COTS products hasn’t been compromised through the sourcing process.
A Process for Secure Acquisition

- Acquisition is a strategic process.
- Involves three distinct communities of practice: customer, supplier, and integrator.
- All three require a defined process to properly execute their tasks.
Ten Principles to Regulate Performance

1. Identify Supply Chain Elements
2. Limit Access and Exposure
3. Create and Maintain Provenance
4. Share Information
5. Perform SCRM Awareness and Training
6. Employ Defensive Design
7. Perform Integrator Review
8. Strengthen Delivery Mechanisms
9. Assure Sustainment Activities
10. Manage Disposal Activities
Redesigning the Typical Software SCRM Course

Critical tasks to be included in a proposed software SCRM course

<table>
<thead>
<tr>
<th></th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Establish acquisition strategy and policy</td>
</tr>
<tr>
<td>2</td>
<td>Establish a formal acquisition process</td>
</tr>
<tr>
<td>3</td>
<td>Specify the software requirements</td>
</tr>
<tr>
<td>4</td>
<td>Identify potential suppliers</td>
</tr>
<tr>
<td>5</td>
<td>Establish contractual terms and conditions</td>
</tr>
<tr>
<td>6</td>
<td>Evaluate supplier proposals and contract</td>
</tr>
<tr>
<td>7</td>
<td>Monitor supplier progress</td>
</tr>
<tr>
<td>8</td>
<td>Certify that acceptance criteria have been satisfied</td>
</tr>
<tr>
<td>9</td>
<td>Conduct analysis of software acquisition contract, retain performance data</td>
</tr>
</tbody>
</table>
Course Modules Mapped to Performance and Critical Tasks

Module 1
Program Initiation and Planning
- Define project scope and boundaries
- Identify supply chain elements
- Specify cost, schedule, and quality criteria
- Specify the required functional capabilities
- Specify the required level of software assurance
- Develop comprehensive strategy and criteria for software integration/reintegration
- Software assurance risk mitigation strategies
- Risk management and monitoring practices

Module 2
Specification, RFPs, Contract Terms
- Specify supply chain assurance requirements
- Specify software assurance terms and conditions
- Specify software assurance metrics and measures
- Specify the required level of software assurance
- Specify overall bid evaluation criteria
- Develop detailed statement of work (SOW)
- Specify contractual terms, conditions, security features, updates, vulnerability test reporting, limit access and exposure within supply chain
- Establish policies to assure provenance, sharing

Module 3
Evaluation, Responses to RFP
- Ensure supplier satisfies bid evaluation factors
- Ensure supplier addresses security capabilities, statement of work, and contains assurance case
- Evaluate proposed software product, architecture, defensive design for systems, elements, processes
- Evaluate software security risks and mitigations
- Ensure evaluation criteria is in the RFP, used to determine supplier selection
- Perform contract negotiations
- Perform continuous integrator review

Module 4
Project / Contract Management
- Develop plan for overseeing reviews and audits
- Specify how performance will be evaluated
- Specify how architectural integration will be managed, risks evaluated, issues resolved
- Specify how key personnel will be identified, trained, managed, and evaluated
- Assure sustainment activities and processes
- Deliver product, execute acceptance process
- Manage disposal activities throughout life cycle
- Implement test cases, data, testing of deliverable
Recommendations and Conclusion

• Given the significance, we suggest that the subject matter be encapsulated in a capstone-type course or single process-oriented course.

• For undergrad, the focus should be on fundamentals of accomplishing the topics.

• For graduate-level, emphasis should be on how to implement a unified SCRM approach as a single, coherent strategic process across all three communities of practice.

• Recommend that educators make their course materials available.
References and Resources

Contact Information

Nancy R. Mead  
SEI Fellow & IEEE Life Fellow  
Carnegie Mellon University  
nrmcmu@gmail.com

Anne Kohnke  
Associate Professor  
University of Detroit Mercy  
kohnkean@udmercy.edu

Dan Shoemaker  
Senior Research Scientist & Professor  
University of Detroit Mercy  
shoemadp@udmercy.edu