Software Security Engineering
Lecture 4

Nancy R. Mead, SEI
nrm@sei.cmu.edu

Outline

I. Background

II. The Need for SQUARE

III. Recap of the SQUARE process

IV. Three Cases for Square for Acquisition (A-SQUARE)

- A. introduction
- B. workflow
- C. important points

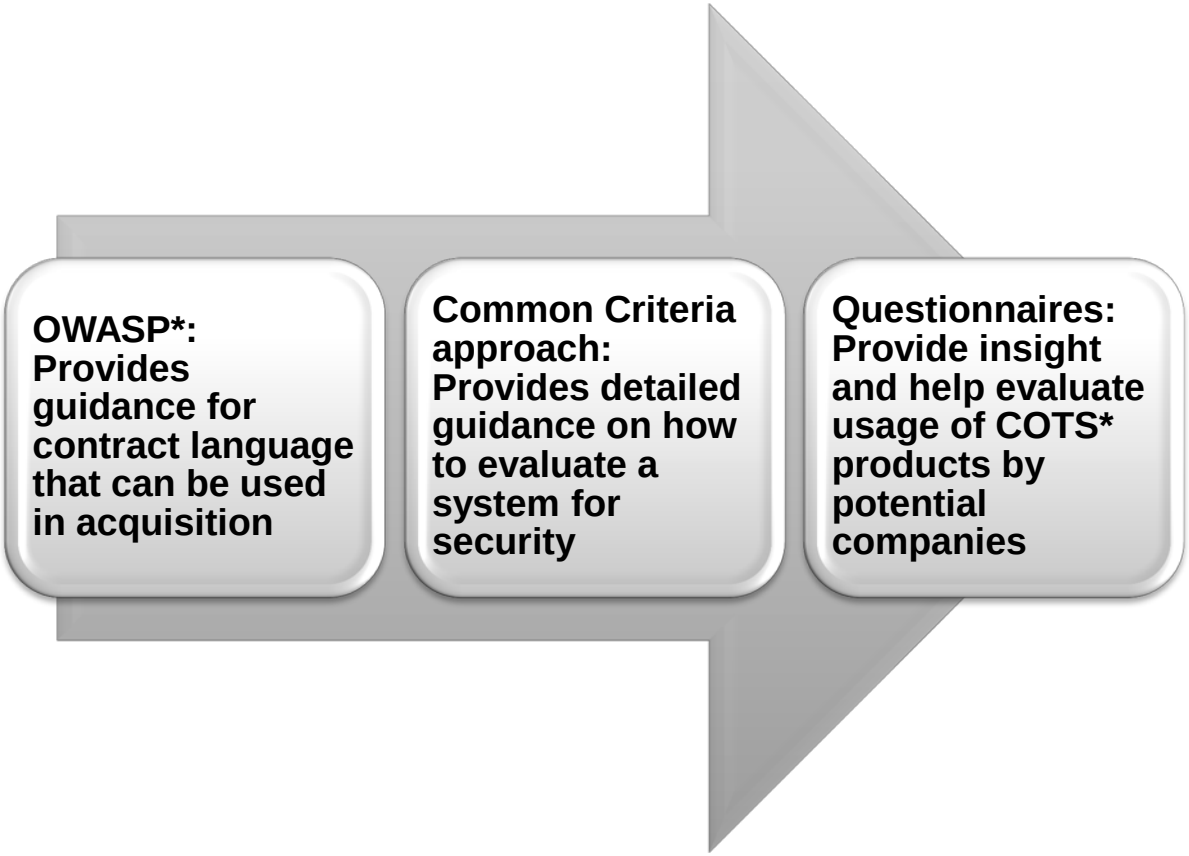
V. Conclusion and further work

VI. Questions

Background

Background

Current efforts in the field of software acquisition



OWASP – open web application security project
COTS – commercial off the shelf

What is Acquisition?

Acquisition: The process of obtaining a system, software product, or software service. Software products may include commercial-off-the-shelf (COTS) products, modified-off-the-shelf (MOTS) products, open source products, or fully developed products.

The above definition was derived from these references:

- Software & Systems Engineering Standards Committee, IEEE Computer Society. *ISO/IEC 12207, IEEE Std. 12207-2008, Systems and Software Engineering - Software Life Cycle Processes, Second Edition*. IEEE Computer Society, 2008.
- Software & Systems Engineering Standards Committee, IEEE Computer Society. *IEEE Std. 1062, IEEE Recommended Practice for Software Acquisition*. IEEE Computer Society, 1998.

The Need for SQUARE

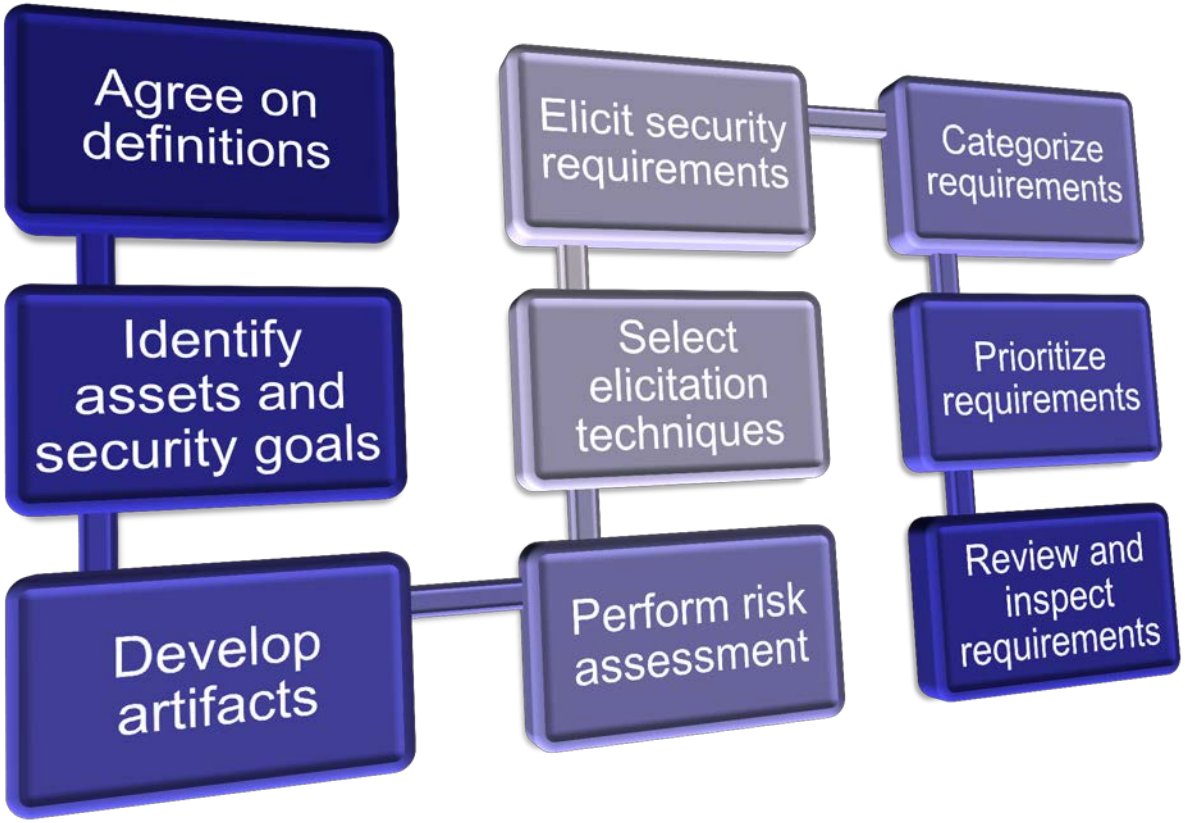
Current problems:

- Lack of control on security requirements of the product by the acquiring company
- Current work lacks level of detail needed, which is specific to security requirements

Benefits of adapting SQUARE for Acquisition:

- Can be easily tailored and modified for various acquisition scenarios
- Well-defined process framework with clear roles and responsibilities defined for each of the stakeholders
- A-SQUARE helps address security requirements early in the project

Recap of the SQUARE Process



SQUARE

	Step	Input	Techniques	Participants	Output
1	**Agree on definitions**	Candidate definitions from IEEE and other standards	Structured interviews, focus group	Stakeholders, requirements team	Agreed-to definitions
2	**Identify assets and security goals**	Definitions, candidate goals, business drivers, policies and procedures, examples	Facilitated work session, surveys, interviews	Stakeholders, requirements engineer	Assets and goals
3	**Develop artifacts to support security requirements definition**	Potential artifacts (e.g., scenarios, misuse cases, templates, forms)	Work session	Requirements engineer	Needed artifacts: scenarios, misuse cases, models, templates, forms

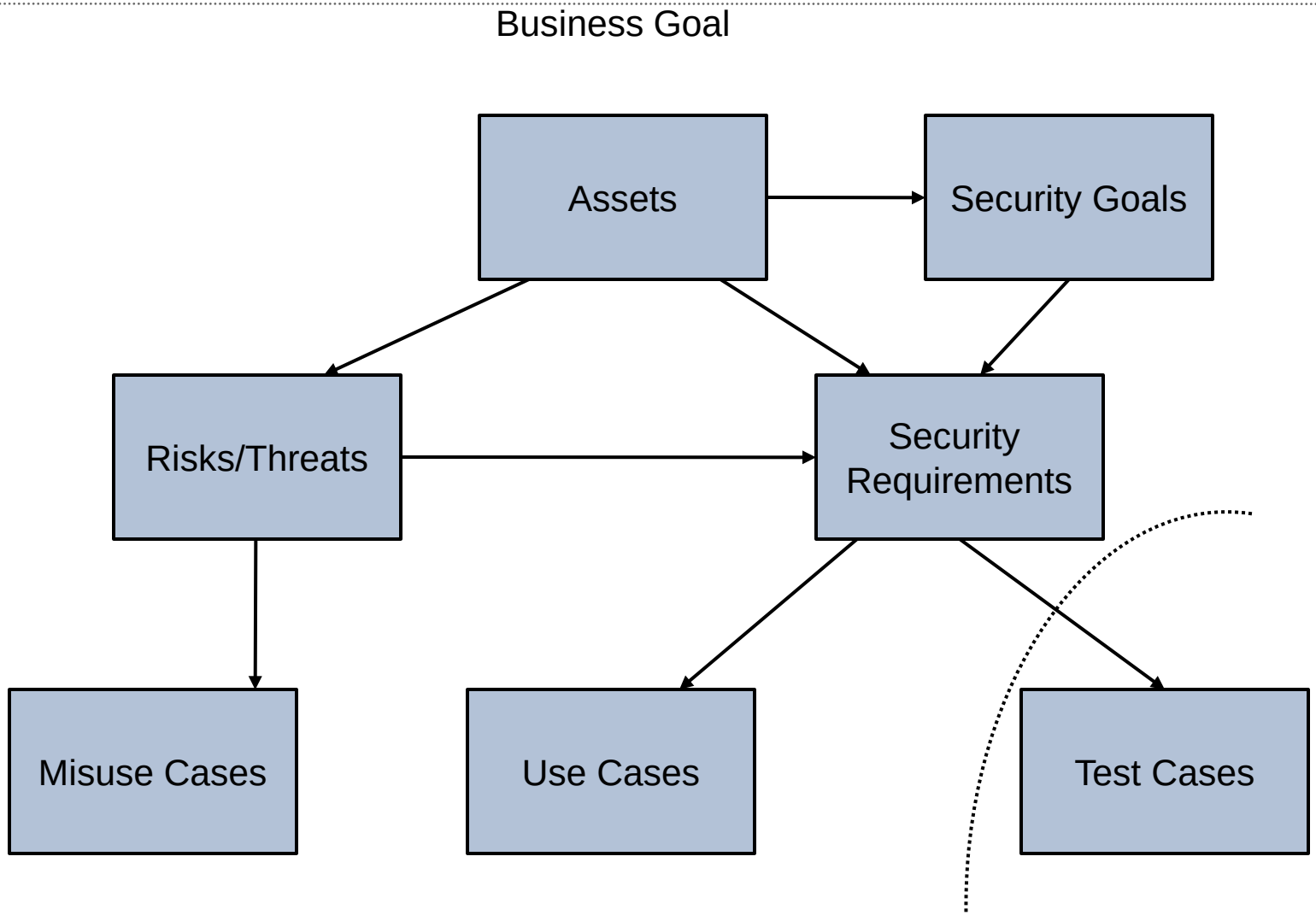
SQUARE

	Step	Input	Techniques	Participants	Output
4	**Perform risk assessment**	Misuse cases, scenarios, security goals	Risk assessment method, analysis of anticipated risk against organizational risk tolerance, including threat analysis	Requirements engineer, risk expert, stakeholders	Risk assessment results
5	**Select elicitation techniques**	Goals, definitions, candidate techniques, expertise of stakeholders, organizational style, culture, level of security needed, cost benefit analysis, etc.	Work session	Requirements engineer	Selected elicitation techniques
6	**Elicit security requirements**	Artifacts, risk assessment results, selected techniques	Joint Application Development (JAD), interviews, surveys, model-based analysis, checklists, lists of reusable requirements types, document reviews	Stakeholders facilitated by requirements engineer	Initial cut at security requirements

SQUARE

	Step	Input	Techniques	Participants	Output
7	**Categorize requirements as to level (system, software, etc.) and whether they are requirements or other kinds of constraints**	Initial requirements, architecture	Work session using a standard set of categories	Requirements engineer, other specialists as needed	Categorized requirements
8	**Prioritize requirements**	Categorized requirements and risk assessment results	Prioritization methods such as Triage, Win-Win	Stakeholders facilitated by requirements engineer	Prioritized requirements
9	**Inspect requirements**	Prioritized requirements, candidate formal inspection technique	Inspection method such as Fagan, peer reviews	Inspection team	Initial selected requirements, documentation of decision making process and rationale

Traceability in the SQUARE Tool



Introduction to A-SQUARE

A-SQUARE: Three Cases

Case 1 – acquisition organization has typical client role for new software



Acquisition Org. Contractor Requirements

Case 2 – acquisition organization does requirements specification



Acquisition Org. Requirements Contractor

Case 3 – acquisition organization is purchasing COTS software



Acquisition Org. COTS

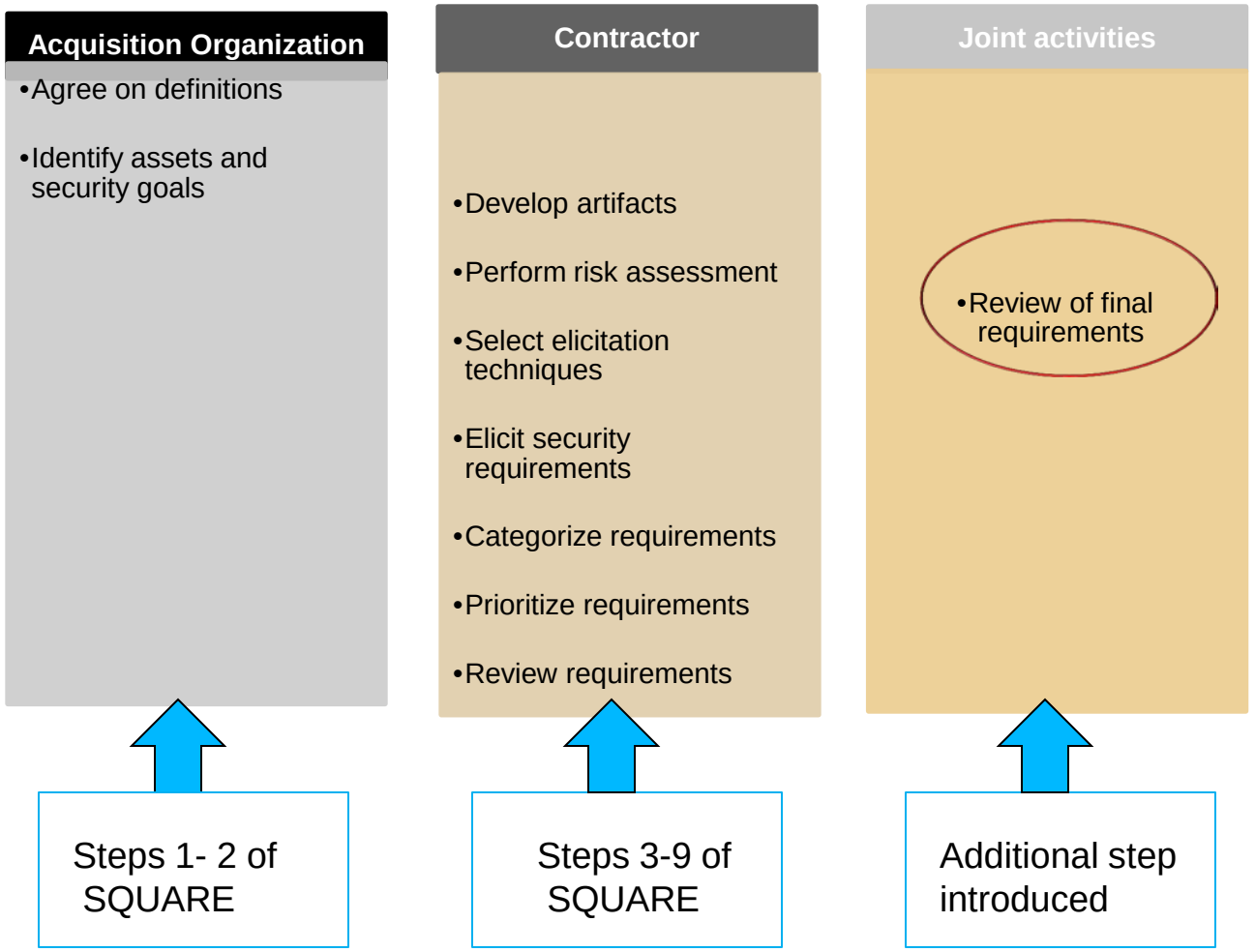
Case 1

A-SQUARE: Case 1 Introduction

Nature of software acquisition:

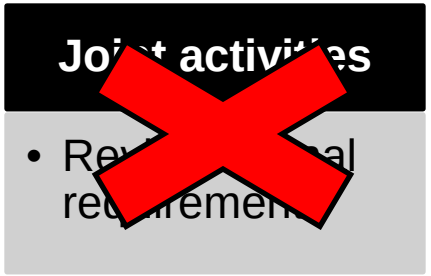
- contractor is responsible for the requirements definition
- contractor should be on board and the contract is awarded
- acquisition organization plays a typical client role

Case 1: Process Workflow



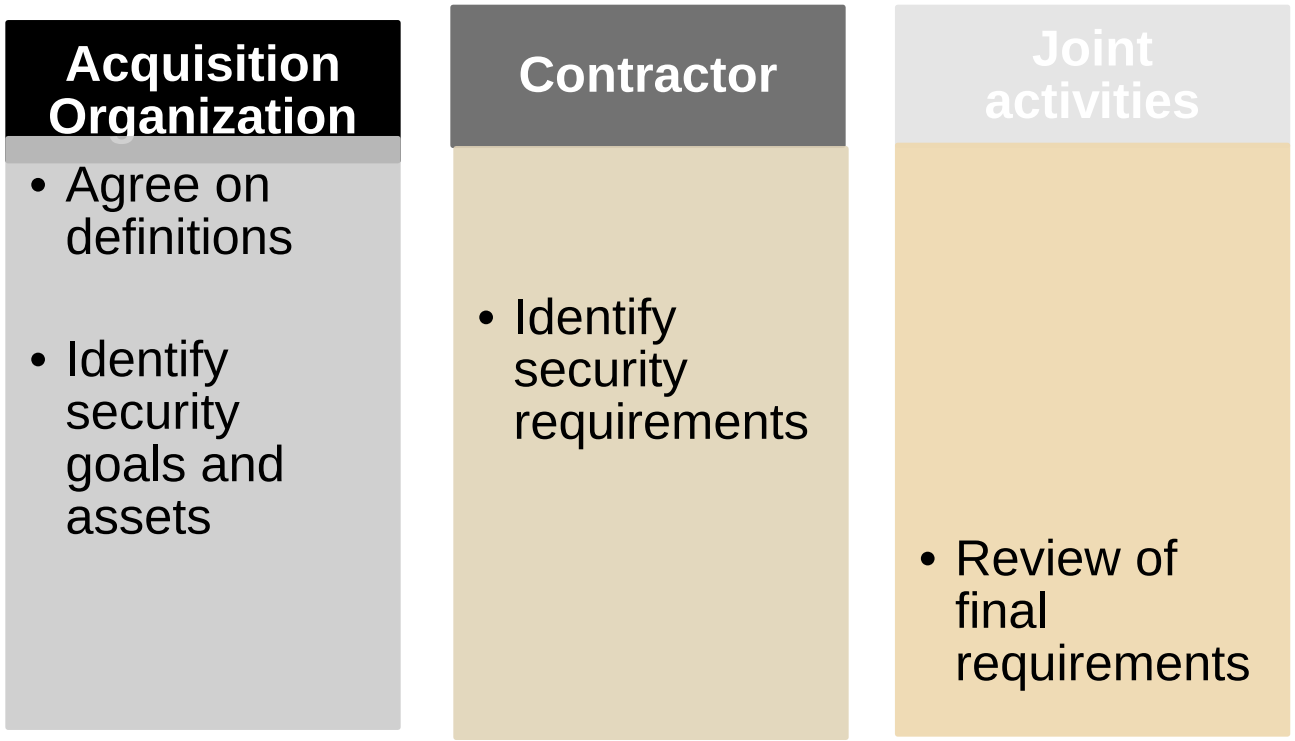
Case 1: Important Points

- The client has no formal role in requirements elicitation for the project.
- The contractor uses SQUARE as the driving process framework for identifying security requirements.
- The additional step (as shown in workflow) may not be needed if both the parties work together.



Case 1: Compressed Workflow

In the event that the client is unaware of the requirements engineering process, the resultant workflow is compressed as shown below



Case 2

A-SQUARE: Case 2 Introduction

Nature of software acquisition:

- acquisition organization specifies requirements as part of request for proposal (RFP)
- original SQUARE should be used by the contractor
- requirements specified will have relatively high-level security requirements

Case 2: Important Points

- The process workflow is similar to the nine-step SQUARE process.
- Level of detail in the requirements definition is crucial.
  - Too much detail can constrain the contractor.
  - The contractor needs some flexibility in defining the requirements.
  - The exit criteria for this process is the final review and approval of the requirements by both parties.

Case 3

A-SQUARE: Case 3 Introduction

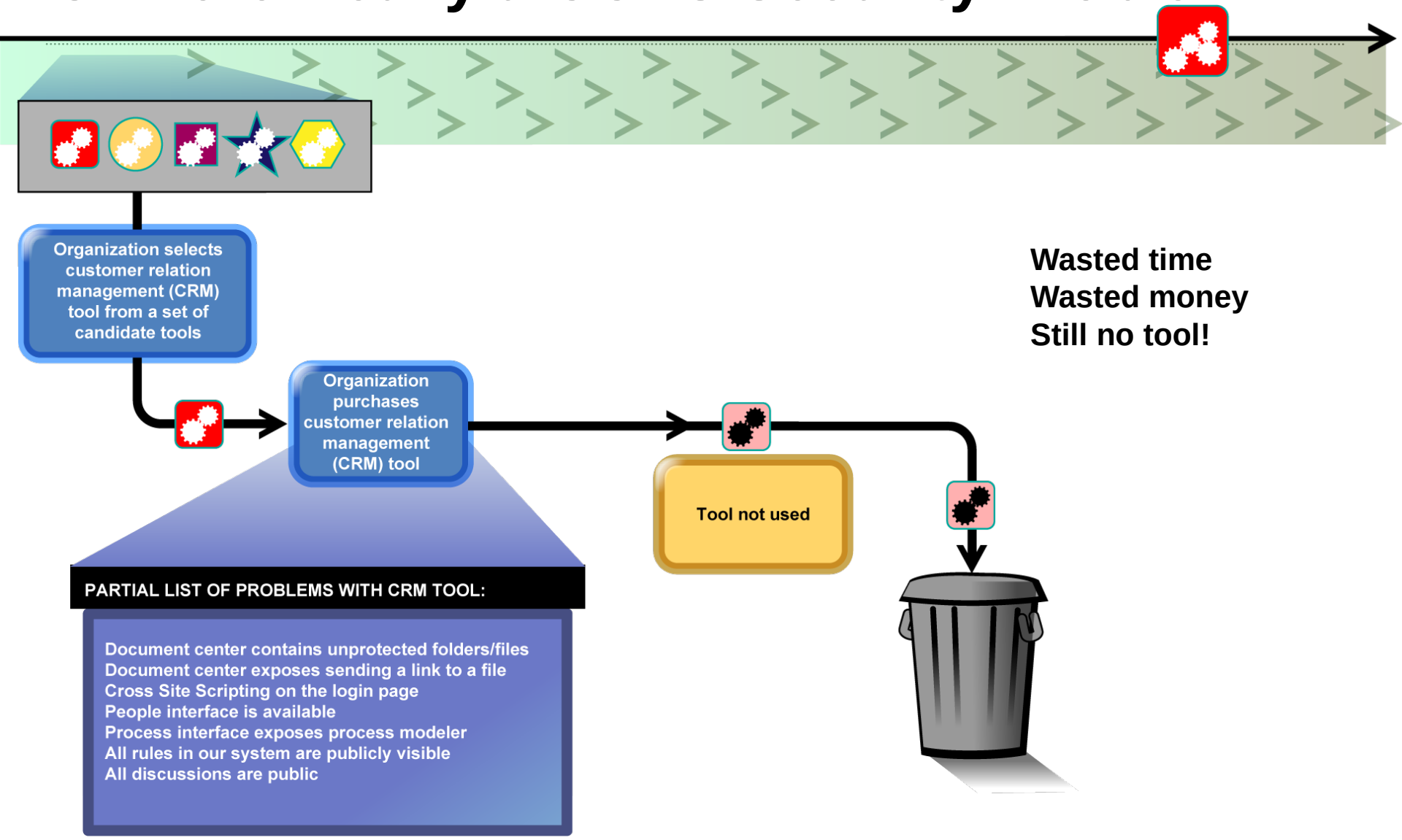
- Nature of software acquisition
  - acquisition of COTS products
- What is COTS ?
  - computer software products that are ready-made and available for use
  - serve as good alternatives for in-house developments
- Benefits of using COTS
  - applications can be built “out-of-the-box”
  - improves overall productivity and reduces company costs

A-SQUARE: Case 3 Introduction

Examples of well-known COTS applications acquired by organizations

- Spreadsheets
- Databases
- Document management Systems
- Emails

Is There Really a COTS Security Problem?



Wasted time
Wasted money
Still no tool!

A-SQUARE Case 3

Process for acquiring COTS software

	Step	Input	Techniques	Participants	Output
1	**Agree on definitions**	Candidate definitions from IEEE and other standards	Structured interviews, focus group	Acquisition organization – stakeholders, security specialists	Agreed-to definitions
2	**Identify assets and security goals**	Definitions, candidate goals, business drivers, policies and procedures, examples	Facilitated work session, surveys, interviews	Acquisition organization – stakeholders, security specialists	Assets and goals
3	**Identify preliminary security requirements**	Assets and goals	Work session	Acquisition organization – security specialists	Preliminary security requirements
4	**Review COTS software package information and specifications**	Assets, goals, preliminary security requirements	Study security features of various packages and documents them, in a spreadsheet, for example	Acquisition organization – security specialists, COTS vendors	Spreadsheet of security features of various packages

A-SQUARE Case 3

Process for acquiring COTS software

	Step	Input	Techniques	Participants	Output
5	**Finalize security requirements**	Preliminary security requirements, features of various packages	Work session – use the spreadsheet to refine and modify the preliminary security requirements to arrive at a final set	Acquisition organization – security specialists	Final security requirements
6	**Perform tradeoff analysis**	Final security requirements, spreadsheet of security features	Tradeoff analysis of COTS products relative to final security requirements	Acquisition organization – stakeholders, security specialists	Prioritized list of COTS products relative to security requirements
7	**Final product selection**	Prioritized list of COTS products relative to security, other important COTS product features	Tradeoff analysis	Acquisition organization – stakeholders	Final COTS product selection

Case 3: Important Points

Prioritization

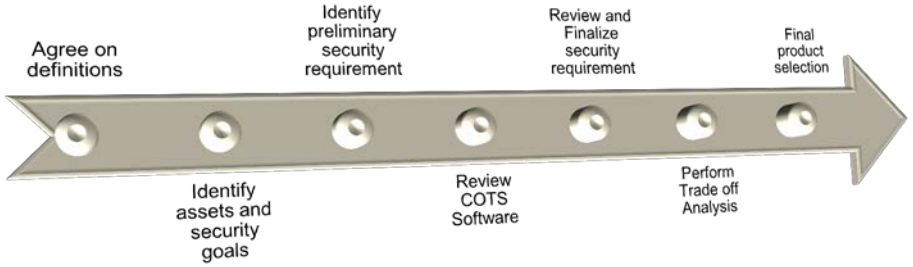
- Security requirements need to be prioritized together with other requirements when acquiring COTS software.

Tradeoff

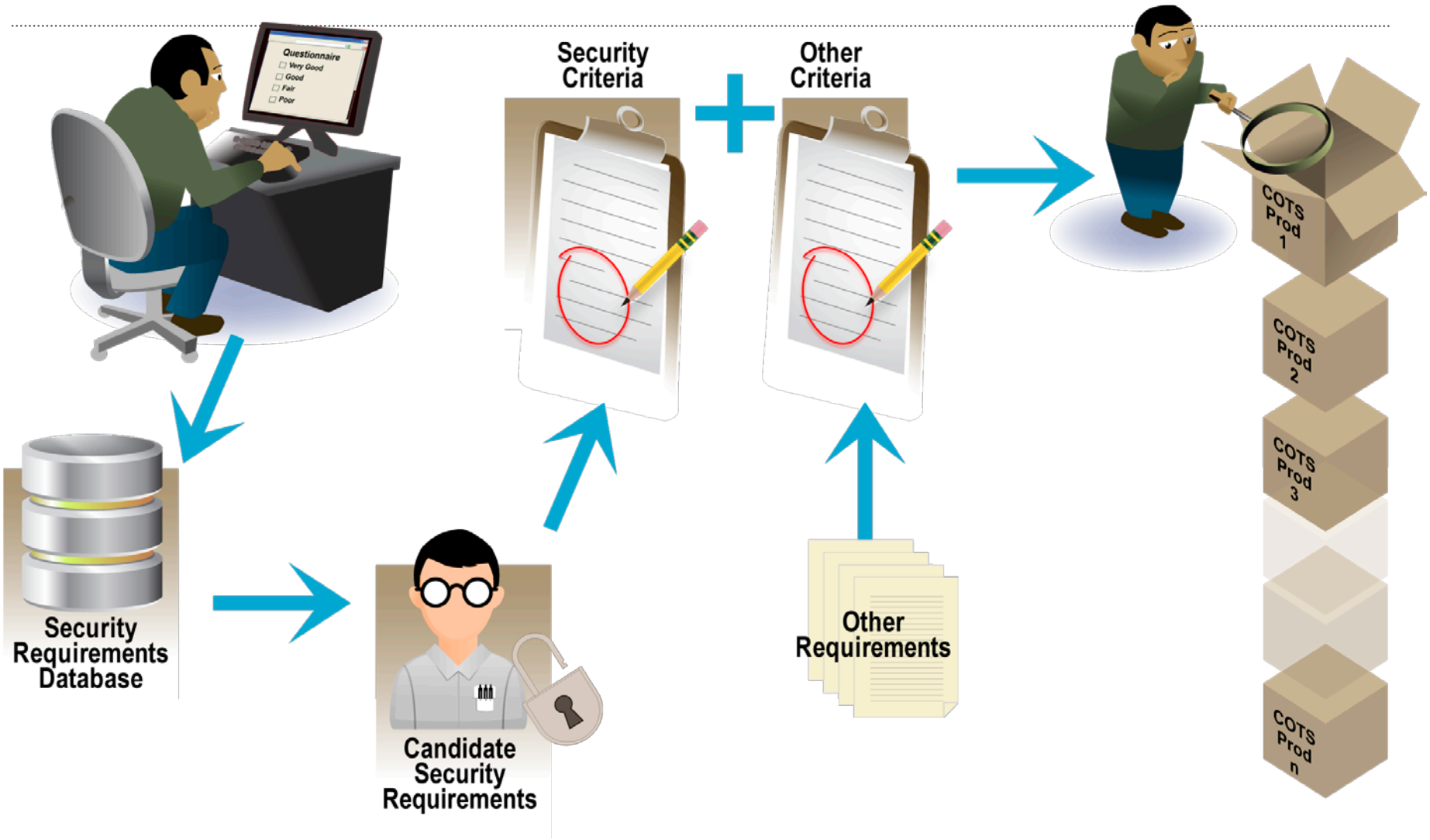
- Tradeoffs and compromises might have to be made since the software might not meet all the security goals of the organization.

Review

- Reviewing the requirements may help the acquiring organization to identify important security requirements.



Future Vision – a New Scenario



Conclusion

Conclusion and Further Work

- A-SQUARE helps identify security requirements early into the project.
- It can reduce the risk associated with software acquisition.
- A-SQUARE tool developed by MSIT Team
- Application of A-SQUARE on projects would help:
  - support acquisition organizations
  - validate the practices of A-SQUARE
  - understand the tailoring needed

Additional Resources

- Allen, Julia H., Barnum, Sean, Ellison, Robert J., McGraw, Gary, & Mead, Nancy R. *Software Security Engineering: A Guide for Project Managers*. Addison Wesley Professional, 2008. (Available from Amazon.com.)

- U.S. Department of Homeland Security. *Build Security In: Requirements Engineering.* <https://buildsecurityin.us-cert.gov/daisy/adm-bsi/articles/best-practices/requirements.html>

- IDEA Group Publishing. <http://www.idea-group.com>

- Mead, Nancy R., Hough, Eric, & Stehney II, Ed. *Security Quality Requirements Engineering (*CMU/SEI-2005-TR-009). Software Engineering Institute, Carnegie Mellon University, 2005. <http://www.sei.cmu.edu/library/abstracts/reports/05tr009.cfm>

- Mead, Nancy R. “Identifying Security Requirements Using the Security Quality Requirements Engineering (SQUARE) Method” *Integrating Security and Software Engineering: Advances and Future Visions*. Edited by H. Mouratidis and P. Giorgini. Idea Group, pp. 44-69, 2006 (ISBN: 1-59904-147-2).

Additional Resources

SQUARE case study reports:

- Gayash, Ashwin, Viswanathan, Venkatesh, & Padmanabhan Deepa. Advisor: Nancy R. Mead. *SQUARE-Lite: Case Study on VADSoft Project* (CMU/SEI-2008-SR-017). Software Engineering Institute, Carnegie Mellon University, 2008. <http://www.sei.cmu.edu/library/abstracts/reports/08sr017.cfm>

- Hough, Eric, Ojoko-Adams, Don, Chung, Lydia, & Hung, Frank. *Security Quality Requirements Engineering (SQUARE): Case Study Phase III* (CMU/SEI-2006-SR-003). Software Engineering Institute, Carnegie Mellon University, 2006. <http://www.sei.cmu.edu/library/abstracts/reports/06sr003.cfm>

- Panusuwan, Varokas & Batlagundu Prashanth. Faculty Advisor: Nancy Mead. *Privacy Risk Assessment Case Studies in Support of SQUARE* (CMU/SEI-2009-SR-017). Software Engineering Institute, Carnegie Mellon University, 2009. <http://www.sei.cmu.edu/library/abstracts/reports/09sr017.cfm>

Questions?

Looking Ahead: Lecture #5

Guest Lecture by Carol Woody on Mission Thread Analysis

Reading Assignment

- SQUARE White Paper on Acquisition
  http://www.cert.org/sse/square/a-square.html

Case Study Assignment 2

- Using the SQUARE Technical Report as a guide, apply SQUARE steps 1, 2, 3, 4 (you just need to identify risks by brainstorming, you don't have to do a formal risk analysis), 5, 6, 7, and 8 to your Case Study project. You do not need to interview your actual stakeholders for purposes of this exercise. Develop attack trees and selected corresponding misuse cases as part of this exercise. Document the methods used for each step. The intent of the exercise is for you to experience most of the aspects of security requirements engineering.
- Turn this in on Blackboard BEFORE 10:30 AM on July 17.

Case Study Assignment 3

- Using the SQUARE for Acquisition white paper and lecture materials as a guide, apply SQUARE for Acquisition Case 3 (acquisition of COTS software) to your project. You may reuse material from Case Study Assignment 2, such as steps 1 and 2. The intent of the exercise is for you to experience security requirements engineering as part of the acquisition process.
- Turn this in on Blackboard BEFORE the class on July 24.

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.