About the Speaker

Nancy Mead is a senior member of the technical staff in the CERT Program at the Software Engineering Institute (SEI). Mead is also a faculty member in the Master of Software Engineering and Master of Information Systems Management programs at Carnegie Mellon University. Her research interests are in the areas of information security, software requirements engineering, and software architectures.

She has more than 100 publications and invited presentations. She is a Fellow of the Institute of Electrical and Electronic Engineers, Inc. (IEEE) and is also a member of the Association for Computing Machinery (ACM). Dr. Mead received her PhD in mathematics from the Polytechnic Institute of New York, and received a BA and an MS in mathematics from New York University.
Contents

• Background (Requirements Engineering)
• SQUARE Methodology
• SQUARE Steps
• SQUARE for Acquisition (A-SQUARE)
• Conclusion (Duration and Outcome)
• Future Work
• Questions

Security QUAlity Requirements Engineering SQUARE
Background

Requirements Engineering issues
Requirements Engineering Issues

RE defects cost up to 200 times more once fielded than if caught in requirements engineering.

Reworking defects consumes >50% of project effort.

>50% of defects are introduced in requirements engineering.

Errors in requirements engineering are costly!
Requirements Problems

Requirements identification may not include relevant stakeholders.

Requirements analysis may or may not be performed.

Requirements specification is typically haphazard.
Effects of Requirements Problems

Bad requirements cause projects to
- exceed schedule
- exceed budget
- have significantly reduced scope
- deliver poor-quality applications
- deliver products that are not significantly used
- be cancelled
Security Requirements

- Address security in a particular application
- Are often ignored in the requirements elicitation process
- Incur high costs when incorporated later
- Must be addressed early - SQUARE
SQUARE Methodology

What is it? Who is involved?
SQUARE

Developed by the Networked Systems Survivability program at the SEI, Carnegie Mellon University

Stepwise methodology for
eliciting, categorizing, and prioritizing
security requirements for
information technology systems and applications

Security requirements are quality attributes.
SQUARE

Who is involved?

- stakeholders of the project
- requirement engineers with security expertise

In the SQUARE approach, security requirements are

- treated as add-ons to the system's functional requirements, *but*
- carried out in the early stages
- specified in similar ways as software requirements engineering and practices
- carried out through a process of nine discrete steps
SQUARE Steps

The Nine Steps
SQUARE Steps

1. Agree on definitions.
2. Identify assets and security goals.
3. Develop artifacts to support security requirements definition.
5. Select elicitation technique(s).
6. Elicit security requirements.
7. Categorize requirements.
8. Prioritize requirements.
9. Inspect requirements.
Step 1

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Def.</td>
<td>Goals</td>
<td>Artifacts</td>
<td>Risk</td>
<td>Technique</td>
<td>Elicit</td>
<td>Categorize</td>
<td>Prioritize</td>
<td>Inspect</td>
</tr>
</tbody>
</table>

Agree on Definitions

- Requirements engineers and stakeholders agree on a set of definitions.
- Process is carried out through interviews.
- Exit criteria: documented set of definitions
- Examples: non-repudiation, DoS, intrusion, malware
Identify Assets and Security Goals

• Identify assets to be protected in the system

• Goals are required to identify the priority and relevance of security requirements.

• Security goals must support the business goal.

• Goals are reviewed, prioritized, and documented.

• Exit criteria: one business goal, several security goals
Step 3

Develop Artifacts

- Collect or create artifacts that will facilitate generation of security requirements.
- Jointly verify their accuracy and completeness.
- Examples: system architecture diagrams, use/misuse case scenarios/diagrams, attack trees, templates and forms
Perform Risk Assessment

- Identify threats to system and its vulnerabilities.
- Calculate likelihood of their occurrence. Classify them. This will also help in prioritizing requirements later.
- Risk expert might be required.
- Exit criteria: documentation of all threats, their likelihood and classifications.
Select Elicitation Technique

- Select appropriate technique for the number and expertise of stakeholders, requirements engineers, and size and scope of the project.

- Techniques: structured/unstructured interviews, accelerated requirements method (ARM), soft systems methodology, issue based information systems (IBIS), Quality Function Deployment
Elicit Security Requirements
*(Heart of SQUARE)*

- Execute the elicitation technique.
- Avoid non-verifiable, vague, ambiguous requirements.
- Concentrate on what, not how. Avoid implementations and architectural constraints.
- Exit criteria: initial document with requirements
Step 7

Categorize Requirements

- Classify requirements into essential, non-essential, system, software, or architectural constraints.

- Sample table:

<table>
<thead>
<tr>
<th></th>
<th>System level</th>
<th>Software level</th>
<th>Architectural constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reqt. 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reqt. 2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step 8

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Def.</td>
<td>Goals</td>
<td>Artifacts</td>
<td>Risk</td>
<td>Technique</td>
<td>Elicit</td>
<td>Categorize</td>
<td>Prioritize</td>
<td>Inspect</td>
</tr>
</tbody>
</table>

Prioritize Requirements

- Use risk assessment and categorization results to prioritize requirements.

- Prioritization techniques: Triage, Win-Win, Analytical Hierarchy Process

- Requirements engineering team should produce a cost-benefit analysis to aid stakeholders.
## Step 9

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Def.</td>
<td>Goals</td>
<td>Artifacts</td>
<td>Risk</td>
<td>Technique</td>
<td>Elicit</td>
<td>Categorize</td>
<td>Prioritize</td>
<td>Inspect</td>
</tr>
</tbody>
</table>

### Requirements Inspection

- Inspection aids in creating accurate and verifiable security requirements.

- Look for ambiguities, inconsistencies, mistaken assumptions.

- Fagan inspections / peer reviews

- Exit criteria: all requirements verified and documented
SQUARE for Acquisition (A-SQUARE)
SQUARE for Acquisition (A-SQUARE)

- Modify SQUARE method for use in acquisition
- Resulting method should be consistent with CMMI for acquisition
A-SQUARE: Three Cases

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

Case 2 – Acquisition organization does requirements specification

Case 3 – Acquisition organization is purchasing COTS software
A-SQUARE: Case 1

A client–contractor relationship

It is important to have client involvement in

• agreeing on definitions
• identifying security goals
• final review of requirements (new step)
# A-SQUARE: Case 1

<table>
<thead>
<tr>
<th>Acquisition Org. &amp; Contractor</th>
<th>Contractor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Agree on definitions.</td>
<td>3. Develop artifacts to support security requirements definition.</td>
</tr>
<tr>
<td>2. Identify assets and security goals.</td>
<td>4. Assess risks.</td>
</tr>
<tr>
<td></td>
<td>5. Select elicitation technique(s).</td>
</tr>
<tr>
<td></td>
<td>6. Elicit security requirements.</td>
</tr>
<tr>
<td></td>
<td>7. Categorize requirements.</td>
</tr>
<tr>
<td>8. Prioritize requirements.</td>
<td></td>
</tr>
<tr>
<td>9. Inspect requirements.</td>
<td></td>
</tr>
<tr>
<td>10. Review of requirements by acquisition organization</td>
<td></td>
</tr>
</tbody>
</table>
A-SQUARE: Case 2

- Acquisition organization specifies requirements as part of RFP
- The original SQUARE should be used by the acquirer
- The requirements specified will have relatively high-level security requirements
- Acquisition organization will want to avoid identifying requirements at a granularity that will overly constrain the contractor
A-SQUARE: Case 3

- Security requirements need to be prioritized together with other requirements when acquiring COTS software
- Do COTS trade-off analysis with security requirements concern
- Need to consider “must have” vs. “nice to have” security requirements
- Reviewing the requirements may help the acquiring organization to identify important security requirements
A-SQUARE: Case 3

1. Agree on definitions.
2. Identify security goals.
3. Identify preliminary security requirements.
4. Review COTS specifications.
5. Finalize security requirements.
6. Perform tradeoff analysis.
7. Write final product specification.
Conclusion
Conclusion

- The SQUARE process
  - takes about three months calendar time to complete
  - has been implemented in several case studies
- SQUARE-Lite
  - Agree on definitions.
  - Identify assets and security goals.
  - Perform risk assessment
  - Elicit security requirements.
  - Prioritize requirements.
SQUARE-Lite has been implemented in one case study
Transition and Future Work

- Education
- Tool development
- Broaden experience base
Education

- Tutorial (overview and details) complete
- Half-day case study complete
- Academic course materials complete and delivered in the classroom – lectures and instructor notes
- Materials available for download from CERT website

Consider web-based training and/or transition to a training vendor
SQUARE Tool Development

- SQUARE prototype tool completed and distributed
- Robust SQUARE tool under development
Broaden Experience Base

- SQUARE experience includes case studies with industry and government users. Current users include several medium to large companies. There is international interest as well.

- Objective is to broaden industry and government usage.
Additional Resources


BSI content on requirements engineering
https://buildsecurityin.us-cert.gov/

SQUARE Technical Report – SEI web site
www.sei.cmu.edu/pub/documents/05.reports/pdf/05tr009.pdf

SQUARE Case Study Reports – SEI web site

“Integrating Security and Software Engineering”
Questions