Adapting the SQUARE Method for Security Requirements Engineering to Acquisition

Nancy R. Mead
Software Engineering Institute
nrm@sei.cmu.edu

Abstract

Organizations that are acquiring software have the same security concerns as organizations that are developing software, but they usually have less control over the actual development process. Depending on the exact situation, the acquisition stakeholders may be heavily involved in security requirements engineering, or they may have a role that is largely limited to reviewing requirements developed by the supplier. In this paper the SQUARE process for security requirements engineering is adapted for different acquisition situations. In the future, it is hoped that other security requirements engineering methods will be adapted to acquisition. The next steps for SQUARE for Acquisition are to use it on actual projects.

1. Background

Although much work in security requirements engineering research has been aimed at in-house development, there are many organizations that acquire software from other sources, rather than developing it in house. These organizations are faced with the same security concerns as organizations doing in-house development, but they usually have less control over the actual development process. As a consequence, acquirers need a way to assure themselves that security requirements are being addressed, regardless of the development process.

There have been some efforts related to acquisition of secure software. The Open Web Application Security Project (OWASP) group [1] has provided guidance for contract language that can be used in acquisition. This includes a brief discussion of requirements. More recently, a document produced by the Software Assurance Acquisition Working Group [2] discusses acquisition at length, including requirements. Questionnaires are available for gaining information about proprietary COTS software, open source software, custom software, GOTS software, and hosted applications. Another approach that is discussed in the Software Assurance Acquisition document is that of developing a software assurance case to provide evidence of due diligence on the part of the supplier. The Common Criteria approach [3] provides detailed guidance on how to evaluate a system for security. While these efforts can be very helpful to acquisition organizations, they lack the level of detail that we see in research projects that are specific to security requirements engineering, such as SQUARE [4], SREP [5], and Secure Tropos [6].

In this paper various acquisition cases for security requirements engineering are examined using the SQUARE process model as a baseline. The SQUARE process for security requirements engineering is intended for new in-house software development, but as we will see, it can readily be modified for acquisition. Of course, there are many approaches to security requirements engineering that could also be adapted to acquisition, and it is hoped that the developers of other methods would also consider such adaptation. If this were done, it would be possible to compare and contrast the alternative methods, and to validate or improve on what has been done here.

2. SQUARE for new development

The SQUARE process for new development is shown in Table 1. This process has been documented [4], described in various papers and websites [7], and used on a number of projects [8]. This is the process that was used as the basis for SQUARE for Acquisition.

Table 1. SQUARE steps

	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
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
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

	Step	Input	Techniques	Participants	Output

3. SQUARE for acquisition (A-SQUARE)

Various acquisition cases and the associated SQUARE adaptations are presented here. This represents a first cut at adaptation. It is hoped that discussion, suggestions for improvement, and application on real projects will lead to validated and improved versions of A-SQUARE.

3.1. Case 1: The acquisition organization has the typical client role for newly developed software

In this example, the contractor is responsible for requirements identification. We have used SQUARE as the underlying method, but depending on how the contract is written, presumably the contractor could use another method to identify the security requirements. If SQUARE is used throughout, Steps 3-9 (highlighted in italics) are performed by the contractor. Otherwise the contractor may use some other method for identifying security requirements (see below). This presumes that the contract award has been made and the contractor is on board. The acquisition organization has the typical client role in this example and reviews the resultant requirements, but does not necessarily specify which method to use in developing the requirements. It's important to note the client involvement in Steps 1, 2, and 10. Note that if the acquisition organization works side by side with the contractor, the separate review in Step 10 could be eliminated, as the client inputs would already be taken into account in the earlier steps.

Table 2. Process when acquisition organization has typical client role for new software

	Step	Input	Techniques	Organizational Responsibility	Output
1	**Agree on definitions**	Candidate definitions from IEEE and other standards	Structured interviews, focus group	Acquisition organization, contractor	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, contractor	Assets and goals
3	***Develop artifacts to support security requirements definition***	*Potential artifacts (e.g., scenarios, misuse cases, templates, forms)*	*Work session*	*Contractor*	*Needed artifacts: scenarios, misuse cases, models, templates, forms*
4	***Perform risk assessment***	*Misuse cases, scenarios, security goals*	*Risk assessment method, analysis of anticipated risk against organizational risk tolerance, including threat analysis*	*Contractor*	*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*	*Contractor*	*Selected elicitation techniques*

	Step	Input	Techniques	Organizational Responsibility	Output
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*	*Contractor*	*Initial cut at security requirements*
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*	*Contractor*	*Categorized requirements*
8	***Prioritize requirements***	*Categorized requirements and risk assessment results*	*Prioritization methods such as Triage, Win-Win*	*Contractor*	*Prioritized requirements*
9	***Review and inspect requirements***	*Prioritized requirements, candidate formal inspection technique*	*Inspection method such as Fagan, peer reviews*	*Contractor*	*Initial selected requirements, documentation of decision making process and rationale*
10	**Review of requirements by acquisition organization**	Initial selected requirements	Traditional review	Acquisition organization, contractor	Final requirements

In the event that the contractor's security requirements engineering process is unknown, the resultant compressed process looks like this:

Table 3. Compressed process if security requirements engineering process is unknown

	Step	Input	Techniques	Organizational Responsibility	Output
1	**Agree on definitions**	Candidate definitions from IEEE and other standards	Structured interviews, focus group	Acquisition organization, contractor	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, contractor	Assets and goals
3	***Contractor identifies security requirements***	*Assets and goals*	*Requirements engineering approach selected by contractor*	*Contractor*	*Initial selected requirements, documentation of decision making process and rationale*

	Step	Input	Techniques	Organizational Responsibility	Output
4	**Review of requirements by acquisition organization**	Initial selected requirements	Traditional review	Acquisition organization, contractor	Final requirements

3.2. Case 2: The acquisition organization specifies the requirements as part of the RFP for newly developed software

If the acquisition organization specifies the requirements as part of the request for proposal (RFP), then the original SQUARE for development should be used (**Table 1**). Note that these may be relatively high-level security requirements that result from this exercise, since the acquisition organization may be developing the requirements in the absence of a broader system context. Also, the acquisition organization will want to avoid identifying requirements at an implementation level of granularity as that will overly constrain the contractor.

3.3. Case 3: Acquisition of COTS software

In acquisition of COTS software, the organization will have to develop a list of requirements for the software and compare those requirements with the software packages under consideration. Security requirements may need to be prioritized together with other requirements. Compromises and tradeoffs may need to be made, and the organization may have to figure out how to satisfy some security requirements outside the software itself—for example with system-level requirements, security policy, or physical security. The requirements themselves are likely to be high-level requirements that map to security goals rather than detailed requirements used in software development.

Note that in acquiring COTS software, organizations often do minimal tradeoff analysis and may not consider security requirements at all, even when they do such tradeoff analysis. The acquiring organization will need to consider "must have" versus "nice to have" security requirements. It is also the case that reviewing the security features of specific offerings may help the acquiring organization to identify the security requirements that are important to them.

Table 5. 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

	Step	Input	Techniques	Participants	Output
5	**Review and finalize security requirements**	Preliminary security requirements, features of various packages	Work session – use the spreadsheet to refine, review, 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

4. Conclusions and future plans

This paper has presented alternative versions of SQUARE for use in acquisition. A-SQUARE needs to be applied on real projects so that it can be validated and modified based on actual practice. In addition, it could be tailored to various acquisition environments. For example, acquisition processes in government organizations may differ from acquisition processes in commercial and academic organizations. In addition, differences may exist from one country to another.

As noted earlier, there are many other approaches to security requirements engineering, and these could be adapted to acquisition. It would be beneficial if the developers of those processes would go through a similar adaptation exercise so that we could compare and contrast results.

5. References

[1] "OWASP Secure Software Development Contract Annex," Aspect Security, Inc. and the Open Web Application Security Project Foundation, 2008. http://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

[2] Software Assurance Acquisition Working Group, "Software Assurance (SwA) in Acquisition: Mitigating Risks to the Enterprise," 2008. https://buildsecurityin.us-cert.gov/daisy/bsi/dhs/908-BSI.html

[3] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 1 (CCMB-2006-09-001), Sept. 2006. http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf

[4] N. R. Mead, E. Hough, and T. Stehney, "Security Quality Requirements Engineering (SQUARE) Methodology" (CMU/SEI-2005-TR-009), Software Engineering Institute, Carnegie Mellon University, 2005. http://www.sei.cmu.edu/publications/documents/05.reports/05tr009.html

[5] D. Mellado, E. Fernández-Medina, and M. Piattini, "Applying a Security Requirements Engineering Process," in *11th European Symposium on Research in Computer Security*, Hamburg, Germany, 2006, pp. 192-206. http://www.springerlink.com/content/91l8q364jk2p5421/

[6] P. Giorgini, H. Mouratidis, and N. Zannone, "Modelling Security and Trust with Secure Tropos," 2006. http://www.cs.toronto.edu/~zannone/publication/gior-mour-zann-06-IDEA.pdf

[7] N. R. Mead, "SQUARE: Requirements Engineering for Improved System Security," 2008. http://www.cert.org/sse/square.html

[8] L. Chung, F. Hung, E. Hough, and D. Ojoko-Adams, "Security Quality Requirements Engineering (SQUARE): Case Study Phase III," Software Engineering Institute, Carnegie Mellon University (CMU/SEI-2006-SR-003), 2006. http://www.sei.cmu.edu/pub/documents/06.reports/06sr003.pdf