JOURNAL OF SOFTWARE ENGINEERING & INTELLIGENT SYSTEMS
ISSN 2518-8739
31st December 2017, Volume 2, Issue 3, JSEIS, CADMEI Copyright © 2016-2017
www.jseis.org

Interaction between team of requirement engineers and the stakeholders to obtain security requirements of an IT project

[1] Muhammad Sadiq, [2] Rana Muhammad Ashfaq
[1]Department of Software Engineering, Bahria University, Islamabad, Pakistan
[2]Department of CS & SE, International Islamic University, Islamabad, Pakistan
Email: sadiq1pk@gmail.com, ashfaqasp@gmail.com

ABSTRACT

Security Requirements are most important part of overall requirements but they are often not given due importance. Different guidelines are proposed by research for elicitation of security requirements. Security Requirements are often considered as non-functional only but studies reveal that most of the security requirements belong to functional part. Different methods are proposed to streamline the processes of security requirement elicitation, SQUARE proposed by SEI is most popular of those. SQUARE methodology consists of nine steps which uses different traditional techniques and define framework for security requirement engineering (RE). SQUARE method is difficult to integrate with current RE practices and in small organizations, thus a scaled down version was proposed named SQUARE Lite which has only four steps. A survey conducted by paper shows that SQUARE Lite is quite feasible for integration in current environment as many of its proposed guidelines already being practiced indirectly.

Keywords: security requirements; non-functional; stakeholders; requirements engineering; SQUARE; prioritization;

1. INTRODUCTION

Requirement engineering (RE) is the root process of an IT project and if there are some defects in this process they do reflect in other phases later as well and fixing these defects at that time can be a costly job. Security requirements are mainly considered as non-functional but studies show that security requirements are mostly functional [1]. Security requirement are an important part of overall RE process but requirement engineers usually lack specific knowledge, they have either no or very little training in design and architecture of security aspects like encryption, intrusion detection, password protection [2]. Requirements elicitation involves use of various techniques which can be broadly grouped into *traditional, group elicitation, prototyping, model driven, cognitive and contextual techniques* [3], many of these techniques involve stakeholder's interaction at various levels. Apart from these general techniques several different methods have been developed for elicitation of security requirements specifically e.g. SQUARE (Security Quality Requirement Engineering) and CLASP (Comprehensive Lightweight Application Security Process). SQUARE developed by Software Engineering Institute (SEI) has been proved to be the most comprehensive model for security requirement elicitation.

The purpose of this research is to study how effectively security requirements can be communicated; moreover, some general guidelines will be discussed. A scaled down version of SQUARE will be applied upon different projects to check at what extent security requirements are defined in conformance with SQUARE Lite.

2. GUIDELINES

In order to produce an effective interaction between stakeholders and RE teams for elicitation of security requirements certain guidelines need to be followed.

A) Criteria for security requirement

a) RE must show that what security requirements are
b) Incorporating behavior assumption
c) Elicited requirement should satisfy security goals[4].

B) Requirement categorization

Requirement categorization is very important in a sense that it helps to find out right stakeholders for a specific category for interaction. For all requirements there are broadly two types of requirements functional and non-

functional. Apart from this broad categorization a pattern is presented about some common specific security related categories which are given as under[5]:

a) Functional

i. Access management/control
ii. Intrusion detection
iii. Digital signatures
iv. Data encryption and security
v. Log of activities
vi. Privacy policy (In some cases many organizations have their own privacy policy)
vii. Login control

b) Non-functional

i. Authentication
ii. Availability
iii. Physical security
iv. Risk analysis/assessment
v. Security management
vi. Security testing

C) Security policy

Different organizations develop their dedicated security policy, it is necessary for requirement engineers to communicate with stakeholders on the basis of this policy if it exists. Resolve any conflicts if posed by this document and clear ambiguities in it.

D) What vs how

We know that RE phase is concerned what part of software development; it is not the job of requirement engineers to specify the design of software so they should avoid drawing design or architecture when they are eliciting requirements from stakeholders[2].

E) Goals and threats

Unlike other requirements which are driven by organizational goals security requirement depends on threats. Security requirements define what should not happen instead of what must happen. Thus, threats must be calculated based on some risk assessment.

F) Misuse cases

Use cases are usually used to document functional requirements; they are success scenario of a function along with possible alternatives. But there are users who usually disrupt the normal flow of a function and try to violate security of software. Such behavior and systems security oriented response is documented with the help of misuse cases.

3. SQUARE AND SQUARE LITE

Software Quality Requirement Engineering (SQUARE) developed by SEI at Carnegie Mellon University is a method for elicitation, prioritization and categorization of security related requirements[6]. As we have already discussed that requirement engineers involved in security requirement elicitation must have good knowledge of security issue, this methodology emphasize the same[6]. SQUARE methodology is composed of nine basic steps which define certain input and exit criteria, methodologies and participants i.e. stakeholders. It is to be noted that SQUARE is not another elicitation technique like the traditional RE elicitation method but a model that uses a combination of these techniques to achieve quality goals towards requirements. Nine constituent steps of SQUARE are:

Step1- Agreeing on definitions: A Set of different terms should be defined in the form of glossary. Requirement engineers can use existing set of terms defined by different standardization languages like IEEE, SEBOK but it is necessary these initial set of terms/definition should be communicated and approved by the stakeholder. Stakeholders

should also prepare list of terms/definitions and present them to requirement engineers. Exit criterion is a document having agreed set of definitions which is single point of contact (POC) between stakeholder and requirement teams.

Step2-Secuity goal identification: The step requires stakeholder to set and prioritize security goals for the project. Requirement engineers should help stakeholder to define overall security goal with the help of brainstorming sessions, review meetings. A document containing overall security goal and prioritized list of sub goals should be prepared by requirement engineers. During the goal defining processes requirement engineer should help stakeholder and act as an expert for example for availability requirement, requirement engineer can suggest stakeholder to invest in backup software and hardware.

Step3-Artificat development: Before specification of security requirements, requirement engineers should gather different artifacts of project e.g. system architecture diagrams, use cases, misuse cases, standard templates. In some cases, these documents may not be present, in that case it is responsibility of requirement engineers to motivate stakeholder for producing such documents and give them confidence that investing in these documents will add value to their system and business. Both stakeholder and requirement engineers should work together to verify different artifacts. An exit criterion for this phase is a set of artifacts identified and produced by engineers and shared by stakeholders.

Step4-Risk assessment: This step focuses on discovery of threats and vulnerabilities, and their likelihood of becoming real attacks. Risk assessment helps to counter these attacks and shape security requirements according to this assessment. It is responsibility of requirement engineers to facilitate risk assessment, review that assessment and share it with stakeholders. Exit criterion is that all possible threats and vulnerabilities are assessed and classified according to their possibilities of occurrence.

Step5-Secltion of elicitation technique: Requirement engineers are required to select an appropriate technique e.g. interviews, survey, soft system analysis, use cases/ misuse cases, attack trees. Technique or techniques should be according to needs of stakeholders, project scope and RE team's expertise. Exit criterion for this phase is that RE team selects a technique and document it's rational.

Step6-security requirement elicitation: It is the most important step in SQUARE methodology. Requirement engineers should take that they document requirements in such way that they can be verified. Moreover, during elicitation process engineers should not try to add design aspect, requirement should only concern with *what* part not *how*. The elicitation techniques involve face to face collaboration thus, requirement engineers should make necessary arrangements for logistics involved. Stakeholders should cooperate with requirement engineers and follow their instructions in the process. Exit criterion for this phase is the initial draft '*t*' of security requirements.

Step7-Requirement categorization: Purpose of this step is to classify requirement such as essential, non-essential, architectural constraints or software level. Requirement engineers provide a formatted document to stakeholders in which they can place different requirements. It is responsibilities of requirement engineers to facilitate the stakeholders in the process and also provide them initial set of classification. A consensus needs to be developed between stakeholders and requirement engineers on categorization of requirements. Exit criterion is the initial set of categorized requirements.

Step8-Priortize requirements: In many cases it is not possible to implement all security requirements, prioritization helps to identify critical requirements which need to be developed at first and which can be dismissed. There are various structured methods available for this purpose like Triage [7], Win-win [8], AHP [9], PHandler [10] and some other techniques like [11-13]. Requirement engineers should help stakeholder in understanding these methods and prioritization of requirements. Stakeholder's responsibility is to prioritize requirements with the help of risk assessment and categorization. Security requirement prioritization is exit criterion for this phase.

Step9-Requirment inspection: Inspection of requirements is last step in SQUARE methodology. The purpose of inspection is to identify defects in requirements, inspection method can be formal or informal like peer reviews. Requirement engineers should guide users in case of formal inspections and provide checklist in case of informal inspections. Stakeholders should verify a requirement and check its feasibility. Both RE teams and stakeholders should make sure that every requirement is applicable and in accordance with security goals. Verified requirements by stakeholders and RE team is an exit criterion for this step.

Different case studies conducted by SEI depicted that all steps of SQUARE are not feasible in many situations as they require high cost and efforts. Based on study conducted by the SEI a scaled down version of SQUARE was produced which contain only four steps which can be adopted along with existing RE processes in many organizations. This scaled down version of SQUARE is called SQUARE LITE.

4. CASE STUDIES

SEI developed some case studies to check applicability of SQUARE method. These case studies depict that SQUARE is costly and lengthy method and difficult to implement in current conditions thus, they introduced its scaled down version [14]. Peer review is a useful technique for requirement inspects and risk assessment of security requirements lack in many organizations [15]. Overall feedback of client organizations was positive.

5. SURVEY RESULTS

Based on SQUARE LITE guidelines we surveyed two systems, one from public sector organization and other from private sector. The purpose of survey is to find out the small to medium scale organization are doing security requirement elicitation and feasibility of incorporation of SQUARE LITE in Pakistan's environment. Table 1 provides summarized comparison of those systems against SQUARE LITE.

Table. 1 Summarized comparison

	Steps	Inputs	Methods/Techniques	Participants	Exit Criteria
	Definition agreement	Set of Definitions from candidate or standard IEEE	Interviews, surveys	Stakeholders and requirement engineers	Agreed set of definitions
Org1		There is no defined document available; however, some indirect rules are available like PEDA rules which address some data security issues etc. Clients also agree on usage of IEEE or other standards which are not in conflict with their organizational policies.	Both methods are used effectively.	Difficult to find right stakeholders. As the one who have technical knowledge usually don't have decision powers.	Available in form of glossary but can be separated from other terms/ definitions and an exclusive list can be prepared.
Org2		There are no direct documents available. But as these kinds of organizations are more independent thus, adapting international standards such as IEEE or ISO is easier.	Same as above	Stakeholders (available and communication is relatively easier with RE teams)	Same as above
	Security goals identification	Business goals, policy documents.	Surveys, interviews, facilitated work sessions	Stakeholders and RE Teams	Security Goals
Org1	Stakeholders often mix the threats and goals.	Many complex documents available difficult to extract information from that, often conflicting information.	Facilitated work session tends to be more useful	Both stakeholders and RE teams available but selection of correct stakeholders is difficult	Security Goals are not available in current software but addition of such goals is possible without much effort.
Org2		Business goals and policy documents are available and not much ambiguous as they are already following ISO standards.	Interview sessions works fine	Same as above	Security goals are not available but can be added easily
	Security requirement elicitation	Risk assessment, selected techniques, different artifacts.	JAD, interviews, surveys, reviews, reusable requirements, checklists	Stakeholders (supported by RE teams)	Initial draft of security requirements
Org1		Risk assessment is not being practiced and it is difficult to perform a quantifiable risk	Interviews backed by prototypes checklists, surveys/	Requirement engineers need to guide stakeholder on different requirement	Security requirements are not available at the moment but can be

		assessment, SRS is available which can be an input source.	questionnaires are effective tools, Use cases though indirectly provide good information e.g. different access level to managers depicts issue of data security.	and a checklist can be given to stakeholder that lists possible security requirement that RE team summarized through introspection. Stakeholder is usually one department or member but will be backed by other departments. (As they like to take more responsibilities)	categorized separately from other requirements.
Org2		Business process document is available which contains risk assessment from different business processes though it is not being practiced currently but can be included with little effort as organization is willing to do so to achieve different standards like ISO, UKAS.	Interviews, checklists, studying documents like BPP, use cases indirectly provide information e.g. Approval process and 24/7 availability of reports depicts data security and Performance related requirement.	RE teams need to guide stakeholders may need to interact with variety of stakeholders for different requirements. People don't like to take responsibility of other requirement for example data access may be dealt by one department and data backup by other i.e. IT support	Security Requirements are not available but can be added easily
	Requirement prioritization	Categorized requirements, risk assessment	AHP. Win-win, Traditional methods, PHandler	Stakeholders (facilitated by RE Teams)	Priority-wise requirements
Org1	Requirement are available priority wise e.g. medium, high and low.	Requirements are being categorized but security requirement as category is missing from current implementation but it can be added.	There is no practice of requirement analysis in current systems. A quantifiable approach such as AHP's implementation cannot be implemented easily as it requires budget and time justification difficult do so in current environment.	Analysis and prioritization can be done by collaboration with stakeholders. (Prioritization is relatively difficult to do due to different point of views of stakeholders e.g. vice-chancellor and IT services head.)	Can be prepared by prioritization need to be focused as all requirements are deemed as important by stakeholder.
Org2	Requirements are available priority wise e.g. medium, high and low.	Requirement categorization is missing. Requirements can be categorized.	Requirement analysis is not being done. Traditional techniques can be applied but some standard methods such as win-win, AHP which requires expertise and resources are not being welcomed.	Stakeholders including the decision makers, RE teams. RE teams should make sure that stakeholder who has decision power and technical/domain expertise should be available if they are not following agile way of assigning some person with domain knowledge decision powers as well.	Priority-wise requirements are already available so prioritizations of security can be achieved.

6. SQUARE LITE INTEGRATION STRATEGY

a) Define a document with definitions related to security terms.
b) Document and define security goals:
   i. Approval of purchase order according to ISO documents (org2).
   ii. Secure and defined access to employee's data only (org1).
   iii. No alteration to data once a transaction is processed except with due permissions (org1).
   iv. Mechanism for employee's database backup along with manual file backup (org1).
c) Define a risk assessment document for example (for org1, org2 respectively) as shown in Table 2 and 3:

Table. 2 Risk assessment grid (org1)

Category	Id	Risk	Possibility of occurrence
High	R1	SQL Injection	High
High	R2	Alteration into employee data	Medium
Low	R3	Data Loss	Low
Low	R4	Server equipment failure	Low

Table. 3 Risk assessment grid (org2)

Category	Id	Risk	Possibility of occurrence
High	R1	SQL Injection	High
High	R2	Order Approval Rights	Low
Low	R3	Data Loss	Low
Low	R4	Server equipment failure	Low
High	R1	SQL Injection	High

d) Elicit security requirements by using different elicitation techniques e.g.
   i. Different access roles for employees
   ii. After editing employees record it should be approved before saving
   iii. Report generation log
   iv. Access log
   v. Daily backup of database

e) Traceability matrix for prioritization of requirements is shown in Table 4 for org1:

Table. 4 Traceability matrix (org1)

Test case	Security Req.	Risk Id	Business goals
Access rights	Dif. Access rights for employees	R1	Defined access to employee's data

Org1=Organization 1: Public Sector Organization (University of Gujrat), *HR Management System*
Org2=Organization 2: Private Sector Organization (Kamal Labs Pvt. Ltd.) *Purchase Process Automation* System according to ISO standards.

7. CONCLUSION

Security requirements are an important part of overall requirements and is often ignore. Security requirements lay both under functional and non-functional part. A comprehensive collaboration strategy is required in order to interact with stakeholders to elicit security requirements. Different methods are proposed in this regard, the most widely accepted method for security elicitation is SQURE proposed by SEI at Carnegie Mellon University. SQUARE is though quite comprehensive but also very costly and time consuming hence, a scaled down version of SQUARE was later introduced which can easily integrated into current RE processes. RE teams eliciting security requirements must have some technical knowledge in this area as they have to facilitate the stakeholders in the process and guide them on different issues they have to make them realize the importance of different security related issues and value of investment in such requirements implementation.

ACKNOWLEDGEMENT

This research was supported by Department of Software Engineering, Bahria University Islamabad, Pakistan and Department of Computer Science & Software Engineering, International Islamic University Islamabad, Pakistan. Special thanks to colleagues from NRSP who provided guidelines and expertise that greatly improved the quality of research.

REFERENCES

1. Wilander, J. and J. Gustavsson. *Security requirements–A field study of current practice*. in *E-proceedings of the symposium on requirements engineering for information security*. 2005.
2. Donald G. Firesmith, F.C., U.S.A., *Engineering Security Requirements.* JOURNAL OF OBJECT TECHNOLOGY, 2003. 1.

3. Nuseibeh, B. and S. Easterbrook. *Requirements engineering: a roadmap*. in *ICSE '00 Proceedings of the Conference on The Future of Software Engineering*. june, 2000. NewYork.
4. Charles B. Haley, R.L., Jonathan D. Moffett, Member, IEEE, and Bashar Nuseibeh, Member, IEEE Computer Society, *Security Requirements Engineering:A Framework for Representation and Analysis.* IEEE Transactions on Software Engineering,, 2008. 34: p. 2,3.
5. John Wilander, J.G. *A Field Study of Current Practice*. in *Symposium on Requirements Engineering for Information Security (SREIS 2005)*. august 2005. Paris, France.
6. Nancy R. Mead, E.D.H., Theodore R. Stehney II, *Software Quality Requirements Engineering Methodology*. 2005.
7. Davis, A.M., *The Art of Requirements Triage.* Computer, 2003. 36(3).
8. Barry Boehm, P.G., Robert O. Briggs, *Developing Groupware for Requirements Negotiation: Lessons Learned.* IEEE Software, 2001. 18: p. 2.
9. Joachim Karlsson, K.R., *A Cost-Value Approach for Prioritizing.* IEEE Software, 1997. 14(5): p. 67-74.
10. Babar, M.I., et al., *PHandler: an expert system for a scalable software requirements prioritization process.* Knowledge-Based Systems, 2015. 84: p. 179-202.
11. Sher, F., et al. *Multi-aspects based requirements priortization technique for value-based software developments*. in *Emerging Technologies (ICET), 2014 International Conference on*. 2014: IEEE.
12. Sher, F., et al. *Requirements prioritization techniques and different aspects for prioritization a systematic literature review protocol*. in *Software Engineering Conference (MySEC), 2014 8th Malaysian*. 2014: IEEE.
13. Babar, M.I., et al., *Stakemeter: Value-based stakeholder identification and quantification framework for value-based software systems.* PloS one, 2015. 10(3): p. e0121344.
14. *SQUARE-Lite: Case Study on VADSoft*. 2008: Pittsburg.
15. Dan Gordon, T.S., Eugene Yu, *System Quality Requirements Engineering (SQUARE):Case Study on Asset Management System,*. 2005.

AUTHORS PROFILE

Muhammad Sadiq completed his MS in Software Engineering from Department of Software Engineering Bahria University, Islamabad, Pakistan. Currently, he is working as Software Engineer in a public-sector organization in Islamabad, Pakistan. His research interests are in software design & architecture, design patterns, requirements engineering and component base software development, software evolution and data mining.

Rana Muhammad Ashfaq completed his MS in Software Engineering from Department of Computer Science and Software Engineering at International Islamic University, Islamabad, Pakistan. Currently, he is pursuing his PhD in Software Engineering from Department of Computer Science and Software Engineering at International Islamic University, Islamabad, Pakistan. He has more the 9 years working experience as Senior Software Engineer in Public and Private Organizations in Pakistan. His research interests are in software engineering, GIS bases Software Development, software testing, requirements engineering and model driven development.