Questionnaire based Approach to Measure Security in Requirement Engineering

Souhaib Besrour
Department of Software Engineering
UTM University,Johor,Malaysia

Imran Ghani, PhD.
Department of Software Engineering
UTM University,Johor,Malaysia

ABSTRACT
The aim of this paper is to measure security in requirement engineering using questionnaire based approach. The questionnaire is applied in the four stages of requirement engineering (Elicitation, analyses, validation, management).The questionnaire based approach is composing of three main parts .First the security questions part .Second the evaluation part which should be filled by the stakeholders .Third the assessment part .Finally A case study conducted to apply Questionnaire based approach and to measure security in requirement engineering.

1. INTRODUCTION
Questionnaire based approach is a simple technique to measure security in requirement engineering. The questionnaire is composing of three main parts. First the security questions part which contains a number of listed question ordered in systematic way .Second the evaluation, it contains number of choices, this part should be filled by the stakeholders .Third the assessment part, it contains the summary results and all assessment results this part usually filled by the examiner; the one who want to make a case study measure security in requirement engineering. The questionnaire is applied in the four stages of requirement engineering (Elicitation, analyses, validation, management).

Keywords
Requirements Engineering, Questionnaire based approach, Measuring Security, Requirement Engineering Quality

2. BACKGROUND OF REQUIREMENT ENGINEERING (RE)
A more precise definition of RE is "a systems and software engineering process which covers all of the activities involved in discovering, documenting and maintaining a set of requirements for a computer-based system"[13].There are many other definitions, but a common agreement is that RE is a sub discipline of systems and software engineering and is concerned with establishing the goals, functions and constraints of hardware and software systems[14][15].The term RE first appeared in 1979 in a TRW technical report [16], but it did not come into general use until the 1990s with the publication of an IEEE Computer Society tutorial [17] and the establishment of a conference series on RE. In the traditional waterfall model of the systems or software engineering, [9][10] [11] [12] [6]RE is presented as the first stage of the development process with the

outcome being a requirements document or software requirements specification. In fact, RE is a process that Continues throughout the lifetime of a system as the requirements are subject to change and new requirements must be elicited and documented and existing requirements have to be managed over the entire lifetime of the system. For example, the project [17] maintains an extensive bibliography of RE. The sub-processes that are parts of a general RE process vary widely depending on the type of system being developed and the specific practice of the organization developing the requirements[1]. Activities within the RE process may include: requirements elicitation, requirements analysis, requirements verification, and requirements management. In the next section a brief about Criteria of measurement

3. DESCRIBING QUESTIONNAIRE BASED APPROACH
This section presents the design overview of Questionnaire based approach. It contains a set of security question as shown in Table2.The security questions are chosen and categorized in a systematic way. The questionnaire provides a better security measurement where the list is based on previous RE studies and techniques [1], [2], [5] with more enhancements on security strength. The questionnaire can be used during the four processes of RE as mentioned earlier (elicitation, analyses, validation, management).

Table1. Example of questionnaire based approach during requirements management

Requirements Management		Level of security				
Security Questions		UN	VL	L	A	H
1- Have your RE team clearly understood the security aim of this process.						
2- Have you used secure traceability policies.						
3- Have you use database to manage security requirement.						
4- Have you define the global security requirement.						
5- Have you record rejected security requirement.						
Official use	Overall level of security					
	Number of security questions					
	Average level of security					

UN= unknown=0, VL=very low=1, L=Low=2, A=average=3, H=high=4

As shown in (Table 1), all listed security questions need to answer properly according to its level of security into unknown (UN), level 0; very low (VL), level 1; low (L), level 2; average (A), level 3; and high (H), level 4. To start, all questions must be read and understood before choosing the appropriate required security level. In the column of" Official use", all item numbers have to be counted and inserted into the appropriate column. This technique can be applied during

all RE processes .In the next section a brief about case study of questionnaire based approach.

4. THE CASE STUDY DATA COLLECTION

A case study conducted to apply Questionnaire based approach and to measure security in requirement engineering, at the Centre of Information and Communication Technology (CICT), University Technology Malaysia (UTM).The questionnaire applied in the four processes of RE ((elicitation, analyses, validation, management).All thecollected data in the case study are listed below.

Table 2.Questionnaire based approach during requirement elicitation process.

Requirements Elicitation		Level of security				
Security Questions		UN	VL	L	A	H
1. Have you using any feasibility study before the beginning of new project.						✓
2. Have you use secure prototype for non-understood requirement.						✓
3. Have you use secure scenario before the beginning of elicit requirement.						✓
4. Have you have any ready security plan, for UN-expected situation.					✓	
5. Have you been reuse security requirement techniques from another system.					✓	
Official use	Overall level of security	18				
	Number of security questions	5				
	Average level of security	3.6				

UN= unknown=0 , VL=very low=1, L=Low=2, A=average=3, H=high=4

The table2 presents Questionnaire based approach and to measure security in requirement engineering during "requirement elicitation". The question number one, two and three get "H" (high) which is equal to the number 4 as shown below the table. The rest of question answered by "A" (average) which is equal to 3.In the last row "Official Use", to calculate "total level of security" we combines Q1 value which is (4) + Q2 value (4) +Q3 value (4) +Q4 value (3) + Q5 value (3). To get the total value a simple addition operation have to be done (Q1+Q2+Q3+Q4+Q5) like this (4+4+4+3+3) =18. In the last row of the table "Average levels of security "to calculate that simple division operations have to be done. Divide the overall level of security "(18) / by the number of questions (5) = the result is (3.6). The number (3.6) represent the average level of security is elicitation stage.

Table 3 Questionnaire based approach during requirement analyses process.

Requirements Analyses.		Level of security				
Security Questions		UN	VL	L	A	H
1-Have you been designed system security boundary.					✓	
2- Have you use any security checklist during RE.						✓
3- Have you prioritize security requirement.						✓
4- Have you use interaction matrix to measure security practices during analyses.						✓
5- Have you use any risk assessment during analyses.						✓
Official use	Overall level of security	19				
	Number of security questions	5				
	Average level of security	3.8				

UN= unknown=0 , VL=very low=1, L=Low=2, A=average=3, H=high=4

Questionnaire based approach and to measure security in requirement engineering during "requirement analyses" .As show in (The table3) the question number one get "A" (average) which is equal to the number 3 as shown below the table. The rest of question answered by "H" (high) which is equal to 4.In the last row "Official Use", to calculate "total level of security" we combines Q1 value which is (3) + Q2 value (4) + Q3 value (4) +Q4 value (4) +Q5 value (4). To get the total value a simple addition operation have to be done (Q1+Q2+Q3+Q4+Q5) like this (3+4+4+4+4) =19.In the last row of the table "Average levels of security "to calculate that simple division operations have to be done. Divide the overall level of security "(19) / by the number of questions (5) =the result is(3.8). The number (3.8) represent the average level of security is analyses stage.

Table 4 Questionnaire based approach during requirement management process.

Requirements Management		Level of security				
Security Questions		UN	VL	L	A	H
1- Have your RE team clearly understood the security aim of this process.						✓
2- Have you used secure traceability policies.					✓	
3- Have you use database to manage security requirement.						✓
4- Have you define the global security requirement.						✓
5- Have you record rejected security requirement.						✓
Official use	Overall level of security	19				
	Number of security questions	5				
	Average level of security	3.8				

UN= unknown=0 , VL=very low=1, L=Low=2, A=average=3, H=high=4

As show in (The table4) it presents Questionnaire based approach and to measure security in requirement engineering during "requirement management". The question number two get "A" (average) which is equal to the number 3 as shown below the table. The rest of question answered by "H" (high) which is equal to 4.In the last row "Official Use", to calculate "total level of security" we combines Q1 value which is (4) + Q2 value (3) + Q3 value (4) +Q4 value (4) + Q5 value (4). To get the total value a simple addition operation have to be done (Q1+Q2+Q3+Q4+Q5) like this (4+3+4+4+4) =19. In the last row of the table "Average levels of security "to calculate that simple division operations have to be done. Divide the overall level of security "(19) / by the number of questions (5) = the result is (3.8). The number (3.8) represent the average level of security is management stage.

Table 5 Questionnaire based approach during requirement validation process.

Requirements validation		Level of security				
Security Questions		UN	VL	L	A	H
1. Have you check the security of requirement during validation.						✓
2. Have you defined a security validation checklist.						✓
3. Have you allow same stakeholder to participate during requirement validation.					✓	
4. Have you use any security template during requirement validation.					✓	
5. Have you use TM. To measure security during validation.					✓	
Official use	Overall level of security	17				
	Number of security questions	5				
	Average level of security	3.4				

UN= unknown=0 , VL=very low=1, L=Low=2, A=average=3, H=high=4

The table5presents Questionnaire based approach and to measure security in requirement engineering during "requirement validation". The question number one and two get "H" (high) which is equal to the number 4 as shown below the table. The rest of question answered by "A" (average) which is equal to 3.In the last row "Official Use", to calculate "total level of security" we combines Q1 value which is (4) + Q2 value (4) + Q3 value (3) +Q4 value (3) + Q5 value (3). To get the total value a simple addition operation have to be done (Q1+Q2+Q3+Q4+Q5) like this (4+4+3+3+3) =17. In the last row of the table "Average levels of security "to calculate that simple division operations have to be done. Divide the overall level of security "(17) / by the number of questions (5) = the result is (3.4). The number (3.4) represent the average level of security is validation stage.

5. COLLECTING RESULTS FROM ALL TABLES

The aim of collecting results from all tables is to have a general assessment about the overall level of security in RE.The questionnaire is applied in the four stages of requirement engineering (Elicitation, analyses, validation, management).The Average security level of each stage have to be listed and be combined together to get the "overall level of security ". The average level of elicitation stage (3.6) +the average level of analyses stage (3.8) +the average level of validation stage (3.4) +the average level of management stage (3.8) = The total results is (3.65). As shown below the (table5) there is the level of security classification .If we want to convert the "overall level of security"(3.65) this number is located between Average level and the high level as shown below (table5).All in all the "overall level of security "(3.65) this number reflect a good security level in CICT institution ,however this number can be increased by applying better security techniques and following security best practices to enhance the overall organization security level.

The aim of this paper is to measure security in requirement engineering using questionnaire based approach. The questionnaire based approach is composing of three main parts .First the security questions part .Second the evaluation part which should be filled by the stakeholders .Third the assessment part .Finally A case study conducted to apply Questionnaire based approach and to measure security in requirement engineering.

5. FUTURE WORK

In future works, RE techniques and technical questionnaires has to be more specific and efficient using new mathematical algorithm and better methods enhanced from new researches[8][3][4]. Exponential advancement in the IT industry has made security threat an increasingly challenging problem. Thus, RE tools have to be more efficient to preserve the confidentiality, integrity, availability, complexity and full fill the exact customer need.

6. CONCLUSION

This paper presents Questionnaire based approach to measure security in requirement engineering. The questionnaire based approach is composing of three main parts .First the security questions part .Second the evaluation part which should be filled by the stakeholder's .Third the assessment part. The questionnaire is applied in the four stages of requirement engineering (Elicitation, analyses, validation, management).Finally A case study conducted to apply Questionnaire based approach and to measure security in requirement engineering.

7. REFERENCES:

[1] Ian Sommerville .software engineering 9th Edition , ISBN-10: 0137035152 | ISBN-13: 978-0137035151 | Publication Date: March 13, 2010

[2] Lusiamich, Roberto GariglianoAmbiguity measures in requirement engineering.2000

[3] Daniel Rodriguez, Israel HerraizandRachelHarrison,On Software Engineering Repositories and Their Open Problems,May 2012.

[4] Leif Singer and Kurt Schneider, Influencing the Adoption of Software Engineering Methods Using Social Software, Hannover, Germany 2012.

[5] Stuart Anderson and Massimo Felici Laboratory .Requirements Engineering questionair,University of Edinburgh James, 3JZ Scotland, UK.January 2001.

[6] Royce, W.W. 'Managing the Development of Large Software Systems: Concepts and Techniques', IEEE Westcon, international conference on Software Engineering. 1970.

[7] Thayer, R.H., and M. Dorfman (eds.), System and Software Requirements Engineering, IEEE Computer Society Press, Los Alamitos, CA, 1990.

[8] ChristofEbert ,Practice: Requirements Engineering in Global Teams.2011

[9] ACM (2006)."Computing Degrees & Careers".ACM.Retrieved 2010-11-23.

[10] Laplante, Phillip (2007). What Every Engineer Should Know about Software Engineering. Boca Raton: CRC. ISBN 9780849372285.Retrieved 2011-01-21.

[11] Peter, Naur; Brian Randell (7–11 October 1968). "Software Engineering: Report of a conference sponsored by the NATO Science Committee" (PDF). Garmisch, Germany: Scientific Affairs Division, NATO. Retrieved 2008-12-26.

[12] Randell, Brian ."The 1968/69 NATO Software Engineering Reports".NewcastleUniversity.Retrieved 2008.

[13] Kotonya G. and Sommerville, I. Requirements Engineering: Processes and Techniques. Chichester, UK: John Wiley & Sons. 1998 .

[14] Phillip A. Laplante What Every Engineer Should Know about Software Engineering.Page 44.(2007).

[15] Zave, P. 'Classification of Research Efforts in Requirements Engineering'. ACM Computing Surveys, 29(4): 315-321, 1997.

[16] Software Requirements Engineering Methodology (Development) Alfor,M. W. and Lawson,J. T. TRW Defense and Space Systems Group. 1979.

[17] Requirements bibliography Reviewed November 10th 2011

AUTHORS PROFILE

SouhaibBesrour is a master student at Faculty of Computer Science and Information Systems, University Technology Malaysia (UTM), Johor Campus. He received his Master of Computer Science from UTM (Malaysia). His research focus includes studying security in software engineering and measuring security in requirement engineering.

Dr. Imran Ghani is a Senior Lecturer at Faculty of Computer Science and Information Systems, University Technology Malaysia (UTM), Johor Campus. He received his Master of Information Technology Degree from UAAR (Pakistan), M.Sc Computer Science from UTM (Malaysia) and Ph.D. from Kookmin University (South Korea. His research focus includes studying semantics techniques, content-based, collaborative filtering techniques, semantic web services, semantics-based software testing, and security in agile software development practices, enterprise architecture and software architecture.