REQUIREMENTS ELICITATION APPROACH FOR CYBER SECURITY SYSTEMS

By

ISSA ATOUM

Assistant Professor, Information Technology, The World Islamic Sciences and Education University, Amman, Jordan.

ABSTRACT

Requirements elicitation is considered the most important step in software engineering. There are several techniques to elicit requirements, however they are limited. Most approaches are general qualitative approaches. Thus, they do not suite specific software domain, such as cyber security. This article proposes a new technique to elicit requirements from cyber security strategies. The approach is able to formally define requirements' strengths, and link them with respective analyst's expertise. Consequently, management can easily select the appropriate requirements to be implemented. The use of the proposed approach on a selected cyber security domain showed its applicability on cyber security framework implementations.

Keywords: Software Requirement, Requirements Elicitation, Cyber Security Frameworks, Strategic Implementation.

INTRODUCTION

Requirements engineering is concerned with real world goals and functions (Sedelmaier & Landes, 2014; Zave, 1997). It offers suitable techniques for understanding customer needs. According to Lindquist (2005), 71% of project fails are due to poor requirements. Requirements engineering has two major phases; the requirements development and requirements management. The requirements elicitation is considered the most important step in requirement engineering (Kitapci & Boehm, 2007). The basic purpose of eliciting security requirement is to protect the software systems. Many software systems consider security requirements to be non-functional requirements. Nevertheless, it is considered a functional requirement for other large scale security systems (Atoum, Otoom, & Abu Ali, 2012; Otoom & Atoum, 2013).

This article is concerned with requirements elicitation for Cyber Security Strategies (CSSs). The elicitation is important to break the CSS into manageable, understandable requirements and identify strategic moves. They propose to carry out the elicitation using the concept of viewpoints (Nuseibeh, Kramer, & Finkelstein, 2003; Salem, 2010). The software view points capture software from the purposeful aspect of related software. For example, the finance manager is concerned with securing carried out transactions while a marking manager is mostly concerned with increasing the revenue. The viewpoints are particularly useful when a large number of stakeholders are involved in a security system. Therefore, exploiting this approach towards CSS implementation is appealing.

The proposed process for requirements elicitation is outlined in Figure 1. The CSS is taken as an input to the analysis process. The Analysis Team should include members with related expertise in the related domains. The more professional and diverse the team, the more successful the analysis output will be good. The view points of the team are gathered, incorporated, and summarized. The analysis team must resolve conflict, generate a reconciled understanding, and make sure that analysis is complete. With the application of the viewpoints, conflicts can be confronted and the requirements are conciliated.

First, the author has discussed the related work. Next, the paper has illustrated the proposed approach. Then the author evaluates the proposed model, and then concludes the article.

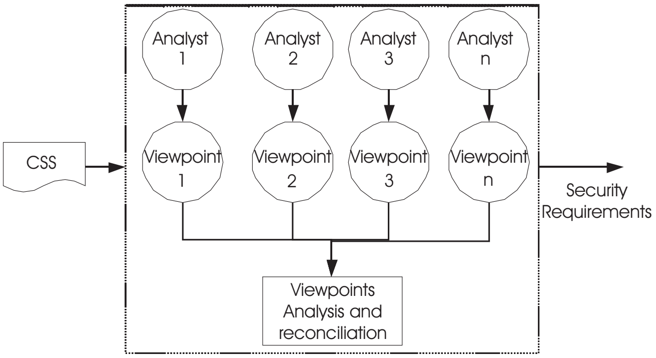

Figure 1. Requirement Elicitation Component

1. Related Work

There are several requirement elicitation methods. Most methods cover requirement elicitation and analysis.

A set of security requirement systems is based on a list of use cases related to the area of study. McDermott & Fox, (1999) proposed methods for collecting and analyzing requirements for object oriented software. Their model is based on communications between the system and other users that may damage the system. Firesmith, (2003) proposed a similar approach that can identify, analyze and specify requirements. Alexander, (2003); Sindre & Opdahl, (2001) proposed another approach dedicated to non-functional requirements. These approaches have no formal analysis.

Literature also discussed graph based security requirement models. Some of these models are based on building trees of potential security aspects (e.g., faults and attacks) in order to find a formal way to protect a system (Martins & de Oliveira, 2014). Brooke & Paige, (2003) broke down the system into subcomponents and then link to potential faults in fault tree based on defined unwanted events. Some works are based on security goals (Li, Horkoff, Beckers, Paja, & Mylopoulos, 2015a) while others are based on anti-goals (Li, Horkoff, Paja, Beckers, & Mylopoulos, 2015b) by negating security properties. Based on the list of defined security patterns, Hatebur, Heisel, & Schmidt, (2006); Yoshioka, Washizaki, & Maruyama, (2008) proposed a model to link security problems together. They applied the patterns to identify several requirements. Using semi-strutted interviews, Alsaleh & Haron, (2016) proposed an approach to extract functional and non-functional requirements for knowledge sharing systems.

Most of the methods discussed in literature are generic, informal and incomplete. To our knowledge, none of the studied methods were used in order to convert a strategic goal to a real requirement.

2. Proposed Approach

The author formally define Requirement Elicitation for CSS process as follows: given a set of analysts, $A = \{a_1,a_2,a_3,...,a_{|A|}\}$ and the set of all domains of all analysts $D=\{d_1,d_2,d_3,...,d_{|D|}\}$ and W is the set of the corresponding weights of domains $W=\{w_1,w_2,w_3,...,w_{|W|}\}$. Each analyst has an experience in years/months x_i in any domain d_i. In practice, selecting analysts is subjective however, the team should be diverse enough with the proper expertise. The Expertise of an analyst has been defined as in formula:

$$E(A_k) = \sum_{i=1}^{|d|} x_i w_i \qquad (1)$$

where:

A_k is any analyst $\in$ A.

x_i is experience of analyst A_k measured in years or months in domain d_i.

w_i is the weight of domain d_i.

This formula will help us in forming the analysis team to select those having maximum expertise. Each analyst will ultimately have an effect on the holistic security implementation, specifically on each requirement identified directly or indirectly by his/her viewpoint.

Let R be the set of all possible requirements in the CSS document, $R = \{r_1, r_2,..., r_{|R|}\}$. Let an effective factor F be defined as the ability to identify a requirement in R. This function shows whether an analyst can identify a requirement or not. The effective factor F can be defined as a function of analysts and requirements as in formula:

$$F(A_k, R_s) = f, \quad f \in \{0,1\} \qquad (2)$$

where:

A_k is any analyst $\in$ A.

R_s is any requirement $\in$ R.

f is any value in the set {0,1} (i.e., the range of the effect factor).

In the set {0,1}, zero means the analyst has failed to identify the requirement and one means the analyst has fully identified the requirement. In theory, an analyst may partially identify a requirement which means the effect factor will take a value between 0 and 1. However, for simplicity, this case is neglected and a partially identified requirement is considered as if it is identified. For example, $F(a_1,r_1) = 1$ and $F(a_1,r_5) = 0$ means analyst (a_1) has identified the requirement (r_1), yet failed to identify the requirement (r_5). The Strength of any requirement, R_s is defined in the formula:

$$S(R_s) = \frac{\sum_{i=1}^{|A|} F(A_i,R_s) \,.\, E(A_i)}{\sum_{j=1}^{|r|} \sum_{i=1}^{|A|} F(A_i,R_j) \,.E(A_i)} \qquad (3)$$

where:

R_s is any requirement $\in$ R

$F(A_i,R_j)$ is as defined by formula (1)

The stronger the requirement, the more consensus the team has made on. Requirements with lower strength values mean that these requirements were identified by few or less expertize team members. These requirements should go through a reconciliation process to decide if these requirements are valid, or they were identified by mistake and should be removed. Formula (4) illustrates the Requirements Acceptance Criterion.

$$Acceptance(R_s) = \begin{cases} valid & S(R_s) \geq \ \theta \\ invalid & otherwise \end{cases} \qquad (4)$$

$S(R_s)$ is as defined in formula (3).

θ is the requirement acceptance threshold value.

valid, means the requirements above threshold are accepted by the team.

Invalid, means the requirements are below the threshold and need to go through the reconciliation process.

Analyst Effectiveness has been defined as shown in formula (5). This function rates the effectiveness of an analyst who is participating in the requirement elicitation.

$$\textbf{Effectivness } (\mathbf{A_k}) = \frac{E(A_k).\sum_{i=1}^{|R|} \mathrm{F}(\mathrm{A_k},\mathrm{R_i})}{\sum_{j=1}^{|R|} \sum_{i=1}^{|A|} F(A_i,R_j) \ .E(A_i)} \qquad (5)$$

where:

A_k is an analyst $\in$ A

$F(A_k,R_1)$ is as in formula (2).

This formula will be useful to rate the effectiveness of the analysis team. Such rating will serve as a feedback to select team members to engage in possible future cyber security requirement analysis.

3. Evaluation

Given a CSS document, the major requirements should be identified first. These requirements could be elicited from the CSS document using the proposed technique. The objective of the proposed approach is to show the technique; a complete case study is out of scope (Atoum & Otoom, 2016). For example, the CSS of Jordan (Otoom & Atoum, 2013) has several requirements: risk management, awareness, encryption and the JO-CERT requirements.

The applicability of the proposed approach has been shown by an example. Refer to Table 1 for an example to illustrate formulas (1) to (5). Each cell in the table represents the effect factor, filled using the formula (2). The higher the summation value across columns, the more consensus on the identified requirement, whereas the higher the summation values across rows reflects the experience and the effectiveness of an analyst in identifying requirements.

Figure 2 illustrates an example on applying formula (4) by showing a list of requirements ordered by strength given a threshold value of 0.5. The requirements (r_5, r_1, r_4, r_7, r_2, r_3,) are considered valid whereas, the requirements (r_6, r_8) should be considered further by the analysis team who will either accept or reject them depending on the reconciliation process.

The proposed approach can be applied at high level cyber security requirements. It can be applied on the identified requirements based on the management

Requirement Analyst	R_1	R_2	…	$R_{\|R\|}$	Effectiveness (A_k)
A_1	1	1	⋯	1	3
A_2	0	1	⋯	1	2
⋯	⋯	⋯	$F(A_k,R_s)$	⋯	⋯
$A_{\|A\|}$	1	1	⋯	⋯	2
$S(R_s)$	2	3	⋯	2	⋯

Table 1. Requirement Elicitation Matrix

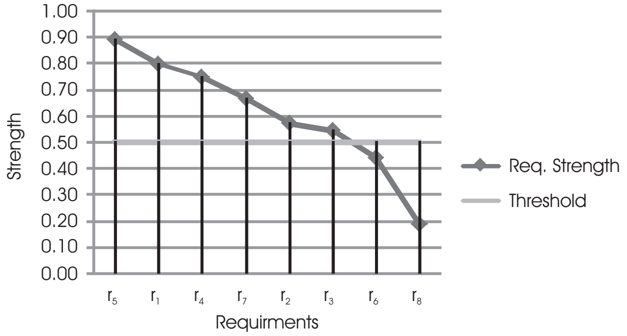

Figure 2. Requirements Acceptance

needs. In other words, the same identified requirement (by this approach) could be further detailed using the same approach.

Conclusion

The author proposed a new approach which is able to elicit requirement from cyber security strategies. The proposed approach is based on viewpoints concept. The cyber security goals are converted to one or more requirements by considering diverse expertise in security and management. The final decision on initial requirements are deemed to the cyber security authority. The approach is considered applicable to the cyber security strategies that are generally very abstract documents.

References

[1]. Alexander, I. (2003). "Misuse cases: use cases with hostile intent". *IEEE Software*, Vol.20, No.1, pp.58-66. doi:10.1109/MS.2003.1159030

[2]. Alsaleh, S., & Haron, H. (2016). "The Most Important Functional and Non-Functional Requirements of Knowledge Sharing System at Public Academic Institutions: A Case Study". *Lecture Notes on Software Engineering*, Vol.4, No.2, pp.157.

[3]. Atoum, I., & Otoom, A. (2016). *Holistic Cyber Security Implementation Frameworks: A Case Study of Jordan*.

[4]. Atoum, I., Otoom, A. A., & Abu Ali, A. (2012). "A Holistic Cyber Security Implementation Framework". *International Journal of Information Security*, Vol.22, No.3, pp.251-264, doi:10.1108/IMCS-02-2013-0014

[5]. Brooke, P. J., & Paige, R. F. (2003). "Fault trees for security system design and analysis". *Computers & Security*, Vol.22, No.3, pp.256-264. doi:http://dx.doi.org/10.1016/S0167-4048(03)00313-4

[6]. Firesmith, D. G. (2003). "Security Use Cases". *Journal of Object Technology*, Vol.2, No.3.

[7]. Hatebur, D., Heisel, M., & Schmidt, H. (2006). "Security Engineering using Problem Frames". *Emerging Trends in Information and Communication Security, International Conference, ETRICS 2006*, Freiburg, Germany, June 6-9, 2006. *Proceedings*. In G. Müller (Ed.), pp.238-253. Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/11766155_17

[8]. Kitapci, H., & Boehm, B. W. (2007). "Formalizing Informal Stakeholder Decisions-A Hybrid Method Approach". In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference,* pp.283c-283c. doi:10.1109/HICSS.2007.233

[9]. Li, T., Horkoff, J., Beckers, K., Paja, E., & Mylopoulos, J. (2015a). "A holistic approach to security attack modeling and analysis". In *Proceedings of the Eighth International i* Workshop* (2015, to be published).

[10]. Li, T., Horkoff, J., Paja, E., Beckers, K., & Mylopoulos, J. (2015b). "The Practice of Enterprise Modeling". *8th IFIP WG 8.1. Working Conference Proceedings, PoEM 2015*, Valencia, Spain, November 10-12, 2015. In J. Ralyté, S. España, & Ó. Pastor (Eds.), (pp. 75-90). Cham: Springer International Publishing. doi:10.1007/978-3-319-25897-3_6

[11]. Lindquist, C. (2005). "Required: Fixing the requirements mess". *CIO*, Vol.19, No.4, pp.1.

[12]. Martins, L. E. G., & de Oliveira, T. (2014). "A case study using a protocol to derive safety functional requirements from Fault Tree Analysis". In *Requirements Engineering Conference (RE), 2014 IEEE 22nd International*, pp.412–419. doi:10.1109/RE.2014.6912292

[13]. McDermott, J., & Fox, C. (1999). "Using abuse case models for security requirements analysis". In *Computer Security Applications Conference, 1999, (ACSAC '99) Proceedings. 15th Annual,* pp. 55-64. doi:10.1109/CSAC.1999.816013

[14]. Nuseibeh, B., Kramer, J., & Finkelstein, A. (2003).

"View Points: meaningful relationships are difficult". *Proceedings of 25th International Conference on Software Engineering, IEEE*. pp.676-681. doi:10.1109/ICSE.2003. 1201254

[15]. Otoom, A., & Atoum, I. (2013). "An Implementation Framework (IF) for the National Information Assurance and Cyber Security Strategy (NIACSS) of Jordan". The *International Arab Journal of Information Technology*, Vol.10, No.4.

[16]. Salem, A. M. (2010). "Requirements Analysis through Viewpoints Oriented Requirements Model (VORD)". *International Journal of Advanced Computer Science and Applications*, Vol.1, No.5, pp.6-13. Retrieved from http://www.thesai.info/Downloads/Volume1No5/Paper 2-Requirements Analysis through Viewpoints Oriented Requirements Model (VORD).pdf

[17]. Sedelmaier, Y., & Landes, D. (2014). "Using business process models to foster competencies in requirements engineering". In *Software Engineering Education and Training (CSEE T), 2014 IEEE 27th Conference*, pp.13-22. doi:10.1109/CSEET.2014.6816776

[18]. Sindre, G., & Opdahl, A. L. (2001). *Capturing security requirements through misuse cases*. NIK 2001, Norsk Informatik konferanse 2001, Http://www. Nik. no/2001.

[19]. Yoshioka, N., Washizaki, H., & Maruyama, K. (2008). "A survey on security patterns". *Progress in Informatics*, Vol.5, No.5, pp.35-47.

[20]. Zave, P. (1997). "Classification of Research Efforts in Requirements Engineering". *ACM Comput. Surv.*, Vol.29, No.4, pp.315-321. doi:10.1145/267580.267581

ABOUT THE AUTHOR

Issa Atoum is currently working as an Assistant Professor in the Department of Information Technology at The World Islamic Sciences and Education University in Jordan. He is also a Lecturer of various subjects in Computer Science and Software Engineering. He holds a PhD. Degree in Software Engineering from University Malaysia Sarawak and M.Sc. Degree in Computer Science from Philadelphia University in Jordan. Furthermore, he has diverse non-academic experience. He is a Project Manager Professional (PMP®), ITIL® V3 and ISO/IEC 20000 Certified Professional.