Towards Analysis of Templates for Security Requirements

Vanessa Wan Sze Tsang

Department of Computer Science

University of Auckland

vtsa001@ec.auckland.ac.nz

Abstract

Researches have shown that security requirements can be highly reusable and it has been only recently the development of templates for reusable security requirements have gone underway. This paper gives an analysis to the templates proposed for security requirements and thereby presents a new approach to templates for security requirements to become more reusable.

1. Introduction

Nowadays, there is an increasing trend in software systems development. In order to cope with such a high demand and increase in productivity, a number of studies have been conducted to investigate whether there are ways to ease the development process and thus reduce the effort of development. The results have found out that at some stages of the development process, there are some similarities even for different systems. Thus, having to go through similar processes for the development of each software system can become repetitive and time consuming. This will also lead to job dissatisfaction and not being able to accomplish the project efficiently and thus decrease productivity. Therefore, a number of approaches have been introduced for software reuse by categorizing similarities from code reuse, design reuse and recently to requirements reuse.

As studies have proven that security requirements are at best done during the requirement phase to become more maintainable and achieve integrity, a number of templates for security requirements have been proposed in order to take security into considerations and ease the development for secure software systems.

The rest of the paper is structured as follows: Section 2 summaries different methodologies existed and introduced for templates for security requirements and the interaction of one another; Section 3 includes a brief overview of the SIREN (SImple REuse of software requiremeNts) approach; Section 4 gives a discussion the existed approaches for templates for security requirements, the advantages for each of the approaches and the further development for templates for security requirements as a proposed approach. Finally, Section 5 concludes this paper with a suggestion for further research.

2. Templates for Security Requirements

2.1 Misuse Case Description Templates

The idea of misuse case descriptions is to provide text-based representation for misuse cases. This is used to describe misuse cases in a more complete and detailed respect which addresses extra information for the analysis of security threats cannot be shown diagrammatically.

As Sindre and Opdahl suggested in [4], the approach adapted from the templates for use case descriptions, the common fields such as

Name, Summary Author, Date and Basic Path, as well as a modification in favour to state the misuses to include Alternative Paths, Capture Points and Extension Points to provide an overview analysis of possible security threats. Also, there are optional fields can be added along to help further analysis at different stages during development. The suggested template would be helpful when determining security issues in a clear and constructive manner.

2.2 Security Use Case Description Templates

Security use cases elaborate further on misuse cases as misuse cases provide an analysis of security threats in a negative sense whereas security use cases describe in an opposite way from the prospective to protect security threats which uses misuse cases as trigger to specify security requirements [1].

According to the above categorization, the template proposed includes both the user and misuser interactions to the system and postconditions to clearly distinguish what is required for security requirements and what is not. Firesmith suggested specifying the use of words in security use cases at a high level of abstraction to achieve

reusability. Therefore, words can be replaced to a more specific level at the phase of reuse.

2.3 Security Requirements Templates

The template proposed is a parameterized template for specifying security requirements [2]. Firesmith believed all security requirements can be categorized into a set of security subfactors and can be further categorized to quality criteria with associated quality measures to describe and measure each subfactor. Thus, it provides a focus on reusability due to the limited variation in security requirements and has improved the security requirements to be measurable and testable.

3. Repository for Reusable Requirements

The idea of reusability presented in [5] is based on the approach of reusable requirement templates being stored into a repository. The paper proposed an approach called SIREN (SImple REuse of software requiremeNts) which is an example for requirements reuse.

SIREN contains a repository for documenting requirement templates where the templates are for specifying requirements and are structured

hierarchically for each specification level, such as Software Requirements Specification, Software Test Specification, Interface Requirements Specification, etc. The documentation is evolved iteratively during the requirements phase to maintain reusability.

SIREN also recommended the spiral life cycle model for the iterative process for requirements reuse as composed by four phases: Requirements Elicitation; Requirements Analysis and Negotiation; Requirements Documentation and Requirements Validation. This model proposed can maintain the quality of security requirement templates in the repository through an iterative process, to be applicable across different domains and to be still well suitable for the evolution of software systems.

4. Discussion

For the misuse case and security use case description templates, the approaches as suggested in [1] and [4], the templates are derived from the fields of normal use case descriptions and tailor-made to be made applicable and useful to the fields for describing security threats and security requirements in a constructive and procedural way. As such, templates can be reused similar to the idea of filling in a form.

Therefore, guidelines of appropriate information that should be included are provided in order to avoid any useful information that might be excluded. However, once the fields of the templates are set, reuse is to this level of abstraction. The actual security requirements specified in the templates may have similarities between systems and reuse at this level may also be possible to increase efficiency and reusability.

Security requirements templates extend misuse case and security use case description templates to provide a parameterized template for specifying security requirements. Thus, gain an advantage over reusing the fields of the templates to maintain completeness and consistency by categorizing security requirements into security subfactors as to constrain the amount of variations involved and investigate the amount of commonalities at certain generic level of abstraction with parameters. Although this is an improvement over misuse case and security use case description templates, the reusability is still only at a textual reuse level. By all means, the parameters in the templates are proposed based on the previous knowledge development for reuse and came out with the conclusion of the analysis. However, no matter how thoroughly the analysis was done based on the knowledge and

similarities of the security requirements of the previous systems to come up with the parameters, since the level of security requirements across different systems may vary from time to time, it can be foreseen there is a need to have a repository of security requirements to update and analyse the parameters for the templates automatically [2], [5], [6].

Therefore, based on the advantages of the approaches in Section 2 and 3 on templates for security requirements and repository for reusable requirements, it brings this further by combining both approaches to a new approach on repository for reusable security requirement templates. This means that a repository is built containing different security requirement templates across different domains by categorization based on iterative knowledge. In this case, security requirement templates are not considered as finale as each security requirement template is evolved during the iterative process, this would therefore give a better quality to the security requirement templates to be more applicable for different domains and become further and highly reusable.

5. Conclusion and Future Work

This paper presents a detailed analysis of different approaches of templates for security requirements as proposed by different researches interested in this field and suggested a new approach to combine the idea of templates for security requirements together with a repository for reusable requirements to create a repository of templates for security requirements to further enhance reusability.

Future work suggests here can include the integration of the repository not only for security requirements, but also include non-functional requirements and further to include functional requirements to serve the whole process of requirements engineering. Also, the development of the repository of templates for security requirements is to be considered, the evolution of how the iterative process should be automated is also needed to be further extended.

6. References

1. Firesmith, D.G. “Security Use Cases”, Journal of Object Technology, 3.2 (May-June 2005): 53-64.

2. Firesmith, D. “Specifying Reusable Security Requirements”, Journal of Object Technology, 3.1 (January-February 2004): 61-75.
3. Sindre, G., Firesmith, D. and Opdahl, A.L. “A Reuse-Based Approach to Determining Security Requirements”, Proceedings of the Ninth International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ’03), (16-17 June 2003).
4. Sindre, G. and Opdahl, A.L. “Templates for Misuse Case Description”, Proceedings of the Seventh International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ’01), (4-5 June 2001).
5. Toval, A., Nicolás, J., Moros, B. and García, F. “Requirements Reuse for Improving Information Systems Security: A Practitioner’s Approach”, Requirements Engineering, 6.4 (2002): 205-219.
6. Toval, A., Olmos, A. and Piattini, M. “Legal Requirements Reuse: A Critical Success Factor for Requirements Quality and Personal Data Protection”, Proceedings. IEEE Joint International

Conference on Requirements Engineering (RE’02), (2002): 95-103.