Which Security Requirements Engineering Methodology Should I Choose?: Towards a Requirements Engineering-based Evaluation Approach

Sravani Teja Bulusu, Romain Laborde, Ahmad Samer Wazan, François Barrère, Abdelmalek Benzekri

Which Security Requirements Engineering Methodology Should I Choose? Towards a Requirements Engineering-based Evaluation Approach

Sravani Teja Bulusu
IRIT/University Paul Sabatier, 118 Route de Narbonne, 31062, Toulouse France
Sravani-Teja.Bulusu@irit.fr

Romain Laborde
IRIT/University Paul Sabatier, 118 Route de Narbonne, 31062, Toulouse France
laborde@irit.fr

Ahmad Samer Wazan
IRIT/University Paul Sabatier, 118 Route de Narbonne, 31062, Toulouse France
ahmad-samer.wazan@irit.fr

Francois Barrère
IRIT/University Paul Sabatier, 118 Route de Narbonne, 31062, Toulouse France
Francois.barrere@irit.fr

Abdelmalek Benzekri
IRIT/University Paul Sabatier, 118 Route de Narbonne, 31062, Toulouse France
Abdelmalek.benzekri@irit.fr

ABSTRACT

Since many decades, requirements engineering domain has seen significant enhancements towards adapting the security and risk analysis concepts. In this regard, there exist numerous security requirements engineering methodologies that support elicitation and evaluation of the security requirements. However, selecting a security requirements engineering methodology (SRE) for a given context of use often depends on a set of ad hoc criteria. In this paper, we propose a methodological evaluation methodology that helps in identifying the characteristics of a good SRE methodology.

CCS CONCEPTS

• **Security and privacy~Security requirements** → Software and its engineering~Requirements analysis

KEYWORDS

Security requirements engineering, evaluation methodology

1 INTRODUCTION

Security requirements engineering (SRE) is continuously evolving as one of the challenging areas of research in the security domain. If the derived security requirements are not good then they could eventually risk inadequate protection of the critical system assets. Consequently, many organizations are compelling keen attention towards the efficient security and risk analysis right from the earlier stages of SRE process. Currently, there exists numerous SRE methodologies that were integrated with the synthesis of security and risk related concepts and enhancements [1]–[5]. However, the question of which SRE methodology to choose for a given context remains an open question till date.

We face this question in the context of the IREHDO2 research project. Our main objective in this project is to derive good security requirements aligned with business strategy as well as the risk control objectives, for aircraft networks. For this, we had to decide which of the existing methodologies is more suitable to derive security requirements for aircraft networks. In this regard, we considered different SRE methodologies focusing on security and risk analysis during early stages of RE process. In practice, majority of the existing SRE methodologies fall into three following categories: goal oriented [2], agent oriented [5] and problem frames oriented approaches [4]. The diversity of SRE methodologies has raised another question: How to evaluate which SRE methodology approach is more suitable to derive good network security requirements for aircraft systems? Accordingly, we started our study with two research questions: *Q1: What are good security requirements?* And *Q2: what is a good security requirements engineering methodology?*

In a previous article [6], we presented an initiative work to address research question Q1. We surveyed the literature on the characteristic of good requirements and proposed a weaving methodology. It provides a consolidated view of the characteristic definitions proposed by 7 different as well as highlights the non-consensus issue. In this article, we aim at addressing research question Q2, for which we propose a generic evaluation

DOI: 10.1145/3098954.3098996

methodology. This methodology follows a requirement engineering-based approach.

The rest of the article is structured as follows. Section 2 provides related works on the comparative studies for evaluating the SRE methodologies. Section 3 describes our proposed methodology. In section 4 we discuss on the highlighting aspects of our methodology. Finally, we conclude our work in Section 4.

2 RELATED WORKS

From a broad perspective, we classify the state-of-the-art of the SRE comparative studies into two categories based on their comparison strategies as: 1) integration of concepts, 2) criteria specific. This categorization seeks facilitating the understanding on the way the comparative studies have performed.

2.1 Integration of concepts

This category of works aims at analysing, to what extend do the methodologies support the integration of the security related concepts.

N Mayer [7] provided a comparative study of the SRE methodologies based on a domain model consisting of 14 security concepts, categorized under three groups as asset-related, risk-related and risk treatment related concepts. *Fabian et al.* [8] proposed a conceptual framework to support the comparative study of the existing SRE methodologies. When compared with *Mayer's* modelling framework [7], this work highlights some similar concepts but was extended with granular security analysis concepts. *K Beckers* [9] provided an extension of the conceptual framework proposed by *Fabian et al.* [8], aligned with additional concepts concerning the privacy goals with respect to the confidentiality protection of the personal data while developing secure software. *Munante et al.* [10] provided a comparative study of the SRE methods emphasizing on the aspects related to security risk analysis and model-driven engineering. This work can be viewed as an extension of the previous works [7], [8]. *Amina et al.* [11] proposed a comparison framework to provide a systematic mapping of the reusable concepts and patterns within the existing SRE methodologies.

2.2 Criteria Specific

This category of works aims at analysing, to what extend do the methodologies fulfil a specific list of evaluation criteria. In below, we do not discuss in detail each list of criteria proposed by the respective authors, as our focus is only on analysing how the respective criteria list is claimed to be good enough to do the comparative study.

Uzunov et al. [12] proposed a comparative analysis of security engineering methodologies using a list of 12 criteria. This work provides guidelines on the selection of methodologies upon their comprehensiveness, applicability and uniqueness from the perspective of industrial use. *Jain et al.* [13] proposed a comparison framework to support the comparative analysis of requirement engineering methodologies in deriving quality requirements. In this regard, 14 requirement engineering methods were evaluated against the guidelines and best practices of RE process as discussed in the international standard IEEE 1233[14]. *Nhlabatsi et al.* [15] proposed a comparative study of security requirements engineering approaches in order to evaluate the extent to which they can support the evolution of secure software during the change management process. Accordingly, the criteria addresses different perspectives such as the modularization, component architectures, change propagation and change impact analysis. *Mead et al.* [16], contrary to above works, provided a comparative analysis of the requirement elicitation techniques based on some criteria such as learnability, client acceptance and durability of the requirement elicitation techniques, tools support etc. In addition, this work highlighted the variability of criteria attributes in regards with the requirement engineering methodologies considered in general.

2.3 State-of-the-art analysis

Many interesting aspects were discussed in the related works. However they are not sufficient to evaluate the goodness of the SRE methodologies, due to various reasons such as:

Issue A: None of the related works covered the whole SRE process in their comparative studies. Only limited works [7], [8], [16] have shown significant focus on security requirements analysis during the earlier stages. However, the SRE process subsumes additional activities to elicitation which are evaluation and documentation.

Issue B: Proposed evaluation criteria were either subjective or ad hoc and lack affirmation on why the criteria were good enough to be considered for the evaluation [12], [15], [16]. In addition, ad hoc selection of criteria for comparing and evaluating the SRE methodologies constrains the reusability and adaptability of the comparison strategies.

***Issue C*:** Finally, none of these comparative studies consider the perspectives of the security requirement engineers who will use the SRE methodology for deriving security requirements.

3 OUR PROPOSED METHODOLOGY

We want to identify an ideal requirement engineering methodology for aircraft network security. In our discussion on the related works in section 2, the comparative studies were made specific to a context or based on some criteria. But how good are those criteria? Are they complete and correct? It is not only sufficient to acknowledge the significance of having some evaluation criteria, but also it is necessary to provide arguments on why and how the proposed criteria were good enough to consider. Therefore, existing comparative studies lack focus on asserting the correctness and reliable aspects of the proposed evaluation criteria (section 2.3).

From a requirement engineering (RE) perspective, these evaluation criteria implicitly correspond to the high-level requirements of the SRE methodology. Thus, we headed to tackle the evaluation of SRE methodologies from the point of view of requirement engineering. Furthermore, instead of providing yet another comparative study specific to our SRE context (similar to the works in section 2), we are interested in developing a generic evaluation methodology independent from SRE context of use.

3.1 The global picture of our SRE evaluation methodology

In the philosophy of requirements engineering, the derived requirements target a future system which is called the system-to-be [3]. Similarly, in our evaluation methodology, the target system is indeed the SRE methodology itself, which we want to choose (see Figure **1**). To our convenience, henceforth we refer this target methodology as the *SRE-Methodology-to-be*. In order to choose a requirement engineering methodology, firstly one has to acquire knowledge on the target context in which requirement engineering is planned to perform[17]. Here the context we are referring concerns the actual RE context of the system-to-be in which the requirement engineers intend to use the SRE-Methodology-to-be. This activity is called "understanding the problem context" in the jargon of RE domain[3]. Then, it is important to identify the stakeholders who are part of the security requirement engineering process in the target context (security requirement engineers, security analysts, etc). Taking into account the people who will use the SRE-Methodology-to-be is mandatory. Likely, this activity is called "identifying stakeholders" in the jargon of RE domain[3].

The next phase in a RE process is the requirements elicitation. In our context, the elicited requirement goals are the high-level characteristics of the SRE-methodology-to-be, which in turn become the evaluation criteria for the comparative study. Our evaluation methodology is built mainly upon the refinement of two research questions: *Q1: what are good security requirements? And Q2: what is a good security requirement engineering methodology?*

The refinement of the research question Q1, addresses the quality aspects of derived requirements which in turn helps in reducing requirement errors [6]. When speaking of the quality of requirements, this aspect is independent to the SRE context. Likewise, the refinement of the research question Q2 addresses the applicable quality aspects of the requirement engineering methodologies which in turn helps in reducing performance errors of the methodology. Unlike Q1, research question Q2 is hooked up with the SRE context. In other terms, it enforces the requirement engineers to think what sort of features in an SRE methodology would be best suitable to their SRE context. Altogether, these questions form the **core building blocks** for eliciting requirements of the SRE-methodology-to-be.

Accordingly, we elicit requirements of the SRE-methodology-to-be based on the anticipated quality aspects of the security requirements as well the anticipated methodology features from the stakeholders (i.e., requirement engineers) objectives. We label the requirements of the SRE-methodology-to-be as $\boldsymbol{R^M}$. Figure 1 projects the RE process of our evaluation methodology. Our methodology subsumes three steps: 1) Identifying problem context and eliciting initial characteristic goals, 2) Refining the characteristics goals into Requirements (R^M), 3) Finally, evaluating the selected methodologies using the elicited requirements (R^M). Accordingly, in the following we discuss the process steps of our methodology.

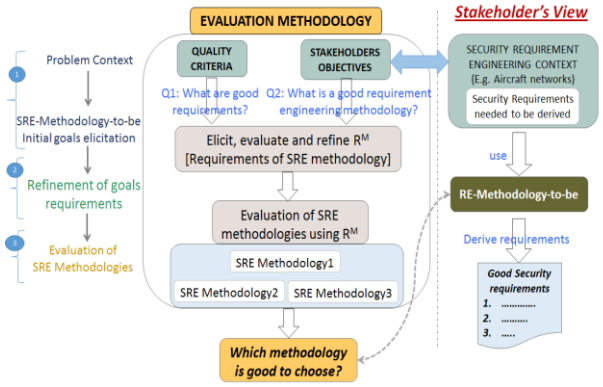

Figure 1: Our Evaluation methodology

3.2 Step1: Problem context and initial goals elicitation

We explain the employment of our evaluation methodology approach by instantiating it to the context of our research project IREHDO2. Accordingly, the problem context of the SRE-methodology-to-be is aircraft network security. Also, we interviewed different people from an aircraft manufacturer company who participate at different levels of the aircraft network security process from the definition of security requirements and risk analysis to the evaluation of the security requirements enforcement on aircraft networks.

Eliciting requirements is a hard task. Especially, meetings/brainstorming with stakeholders must be controlled in order to be effective. In this regard, we propose to employ the elicitation technique introduced by SABSA[18], a business risk driven enterprise security architecture development methodology framework. The SABSA framework handles this elicitation issue by proposing a list of generic high-level business security concerns, called business attributes. These business attributes might lead to several interpretations. Interpretation of business attributes is refined for a specific problem context by a security architect who interacts with the business stakeholders. These business attributes guide the interaction during the elicitation phase.

The list of 20 quality criteria characterizing good security requirements that we proposed in [6] is similar to business attributes in SABSA. Accordingly they constitute the generic high-level goals of the SRE-Methodology-to-be. As consequence, we have organized the 20 quality criteria in order to facilitate the elicitation of requirements R^M. Due to the space limit, we only provide a sample of it in Figure 2. The first three columns contain a unique identifier, a quick definition and the synonyms found in the literature. The last column describes the quality criteria via a set of questions, each reflecting different perspectives of the respective criterion definitions. Suitably, we added this last column to make such different perspectives easily conveyable to all our stakeholders, in order to facilitate their understanding and capture multiple interpretations. Altogether, the 20 characteristic definitions subsume all the aspects of RE process such as

elicitation (e.g., feasible) and evaluation (e.g., consistency), documentation (e.g., traceable) as well the stakeholder's perspectives (e.g., comprehensibility).

No	Abstract criterion abstract definition	Criterion Names in use	QUESTIONAIRES To what extent does the SRE methodology facilitate?
C2	Compatible, non-contradictory requirements	Consistent	1) Does it allow to verify the conflicts between the requirements, goals, assumptions and the domain properties?
C3	Accomplishable within the given financial, time, legal, technical constraints	Feasible/affordable legal Achievable	1) Does it allow to capture all the constraints pertinent to a security requirement? such as technical? Legal? Time? Financial? And time and costs of the implementation? 3) How long does it take to learn the methodology? Is it within the time constraints? 4) what are the training costs? do they exceed the financial constraints?
C5	Requirement should be able to refer back to its objective. Dependency or reference links between requirements should be explicitly defined.	Traceable, Cohesiveness Allocated, satisfied/qualified	1) Does it facilitate to trace the requirements to their source (e.g., goals, mission profile, operational scenarios, context of use, performance, effectiveness, person etc.)? 2) Does it allow to group the requirements under similar abstraction?
C10	Stakeholders needs are sufficiently expressed	Adequacy, Validatability	1) Does it allow to validate the sufficiency of the elicited requirements? 2) Does it facilitate the explicit association of security and risk analysis information with respective requirements? 3) Does it verify if each requirement is self contained with no all the necessary assertions? such as preconditions/post conditions/invariants?
C11	Requirements defined are simple using common terminology and non-technical jargon.	Clear, Concise, Comprehensibility, Customer, User Orientation	1) Do the derived requirements are easily understandable to the intended users? 2) Does the methodology support to facilitate the comprehensibility of the formal languages employed?

Figure 2: Sample of our SRE Requirements Elicitation Tool

We used this quality criteria list (Figure 2) for initiating our discussion in meetings/interviews during the elicitation phase. Subsequently, we gathered requirements goals from security requirements experts, risk analysis and security assessors. These persons are the stakeholders who intend to use the SRE-methodology-to-be in their context which is deriving aircraft network security requirements. This step solely focuses on conveying the true meaning of the characteristic definitions and collecting various perspectives from the stakeholders to find any missing aspects. This activity is known as "agree upon the anticipated features" in the conventional RE process. It also corresponds to the first procedural step "agree on definitions" of the SQUARE SRE methodology[1].

For example, let consider the *adequacy* criterion that could implicitly mean many things. According to NIST[19], adequate security results from "the reasoned sum of all system protections (both active and passive protections) for all system execution modes (e.g., initialization, operation, maintenance, training, shutdown); for all system states (e.g., secure, insecure, normal, degraded, recovery); and for all transitions that occur between system states and between system execution modes". That means the SRE-methodology-to-be methodology should facilitate the security risk analyst to be able to capture all the dimensions of the protection states and modes efficiently[19].

Another example is the priority criterion. Priority of security requirements may vary based on the criticality of the operational contexts. While risk analysis is all about identifying security risks based on potential impacts of the security threats, prioritization of security goals is a fundamental prerequisite. Firesmith [20] has highlighted 13 diversified dimensions that could influence the prioritization aspects of the goals. That means, the SRE methodology should facilitate the security risk analysts to be able to explicitly identify the influencing factors from all such dimensions in order to accurately reason the prioritization. Likewise we have constructed the questionnaires to consolidate the perspectives and viewpoints from the various related works and international standards as we highlighted in our previous article [6].

Furthermore, similar to the business attributes proposed by SABSA, our quality criteria list is not fixed. It can be extended with new criteria with the help of the weaving methodology that we proposed in our previous article [6]. Our weaving approach facilitates the categorization and consolidation of different quality criteria proposed by various authors into one place under a single umbrella. The strategy we employed in our weaving methodology is flexible enough to integrate new criteria or new sources easily to our survey results. Correspondingly, the set of questionnaires provided for each of the criteria in our elicitation tool (see Figure 2) is also flexible to amend the advent of new perspectives.

3.3 Step2: Refinement of Goals to Requirements (R^M)

In our requirement engineering context, the stakeholders are the requirement engineers working in various contexts such as security and risk analysis. Although, the quality attributes are the high level goals of the *SRE methodology-to-be*, their refinement is specific to the context of use as well as the stakeholders. Accordingly, we need to refine the quality criteria goals into requirements R^M in order to characterize the *SRE-methodology-to-be*. Due to the limitation of the space, we provide only two short examples of elicited R^M.

One of the elicited concerns of the stakeholder is regarding the completeness of the security to risk analysis. Therefore, the anticipated feature on the *SRE-methodology-to-be* was: "*The methodology should facilitate in performing sufficient security and risk analysis with respect to the threats concerning confidentiality, integrity and availability"* This statement was devised upon our discussions with the requirement engineers working in security and risk analysis context. This high level quality goal pertains to the *adequacy* quality criterion (C10 in Figure 2), which we refined as "The *SRE-Methodology-to-be* should facilitate in eliciting and capturing security and risk assessment information related to fetching the information from the on-board aircraft network" (R^M1.1 in Figure 3).

We have used the KAOS goal modelling notation [3] to represent the goals refinement hierarchy, for the obvious reasons that our evaluation methodology follows a pure goal-based approach for eliciting requirements (R^M) of the SRE-Methodology-to-be. In addition, KAOS facilitates in tracing the refined goals. The first stage of the refinement regards customizing the anticipated characteristic definitions to the target context (R^M1.1 in Figure 3). This initial refinement activity is similar to the "attributes profiling" of the SABSA framework. The following refinements are driven based on the stakeholder's expectations on the SRE-methodology-to-be. Accordingly, the R^M1.1.1 R^M1.1.2 and R^M1.1.3 (in Figure 3).

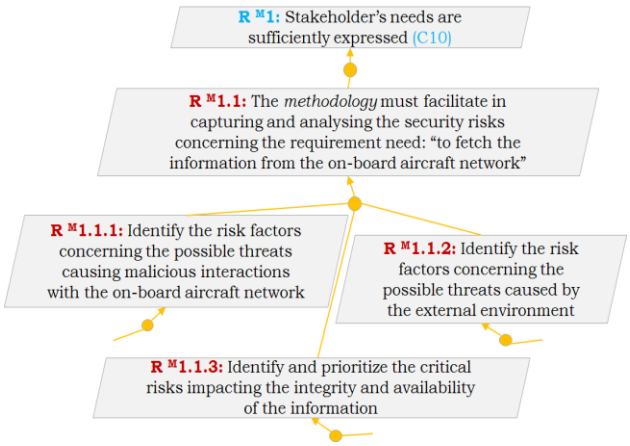

Figure 3: Sample of stakeholders' objectives based on Adequacy Criterion

Another elicited concern of the stakeholders corresponds to the understandable aspects of the security requirements. Respectively, this concern relates to the quality criterion *comprehensibility*, which roughly means that respective users should be able to easily understand the security requirements that are derived by the SRE-methodology-to-be. Therefore, the anticipated feature on the *SRE-methodology-to-be* was: "*Does the derived requirements by the methodology can be easily understood by all users who use them?*" Figure 4 reflects the refined requirements (***R^M***) related to the *comprehensibility* criterion.

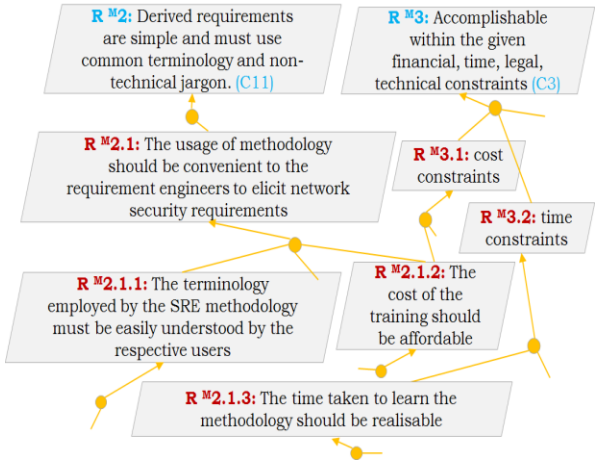

Figure 4: Sample of stakeholders' objectives based on Comprehensibility Criterion

This concern drives the main motivation for all the model based RE approaches. The reason is straight forward, a security requirement not understood cannot be analysed or implemented properly. In this regard, one of the factors influencing the comprehensibility is the language of the RE methodology itself. That means, which language is understandable to the users? A formal language? UML? Or a natural language? This aspect completely depends on the language familiarity of the stakeholders who are going to use the methodology. If they are familiar with formal notations then using formal languages is better. If they are familiar with UML, then it is better to choose the requirement engineering methodology accordingly. Furthermore, learning and mastering a new language has a cost in terms of both money and time as highlighted in the related works[12], [16]. This aspect is close to *feasibility* criterion. As consequence, one can also observe in Figure 4, that there is a dependency link with the between the refined characteristic goals of the quality criteria *comprehensibility* and *feasibility*.

3.4 Step3: Evaluation of the SRE methodologies

This step concerns the evaluation of the SRE methodologies. The resulting requirements R^M elicited at Step2 will eventually become the evaluation criteria. In our research project context, evaluated three distinct SRE methodologies: Secure KAOS (a goal-oriented methodology – noted KAOS) [3], Secure Socio-Technical System (an agent-oriented methodology – noted STS) [5] and Security Engineering Process using Patterns (a problem-oriented methodology – noted SEPP) [4]. Due to space limitations, we restrict our explanation with first the two steps of our methodology and therefore we do not provide details of the evaluation results.

4 Discussion

Our evaluation methodology implements a RE process to elicit characteristics of *SRE-methodology-to-be*. Unlike the other comparative study strategies, it allows the elicitation of SRE evaluation criteria according to the context of use. This flexibility was made possible with the help of the two pluggable building blocks: 1) our quality criteria list[6] and 2) the stakeholder's objectives which allows dynamic customization of the context.

Firstly, ***tight coupling of the quality criteria with consensus*** strictly forces to elicit requirements (R^M) respecting the quality characteristics of good requirements. Since the 20 quality criteria cover all the aspects of SRE process, the resulting requirements (R^M) are not limited to elicitation only (***issue A*** in section 1). Moreover, these 20 criteria result from the consensus of the works varying from research contributions to international standards such as ISO29148[17]. Therefore, they are not subjective (***issue B*** in section 2.3).

Secondly, ***tight coupling of the stakeholder views*** strictly forces to elicit context specific requirements (R^M) complying with the requirement engineers' objectives (***issue C*** in section 2.3) confined to a business operational context. Accordingly, the elicited criteria are considered as high-level goals which are then refined with help of our elicitation tool (Figure 2). Therefore our approach provides an explicit explanation and affirmation of final R^M (***issue B***. section 2). Altogether, these two building blocks of our RE based evaluation methodology contributes towards the ***adaptability*** as well as the ***reusability*** of our evaluation strategy irrespective of the security requirement engineering context. Likewise, the characterization of *SRE methodology-to-be* based on

the quality criteria coupled with stakeholder's objectives, contribute towards asserting the ***correctness*** and ***reliability*** of the derived evaluation criteria.

To conclude, our requirement engineering based evaluation approach allows its users to think like a requirements architect who plans, designs and reviews the derivation of security requirements well before selecting an SRE methodology. As a result, it implies a significant focus on security requirements analysis right from the earlier stages of SRE process.

5 CONCLUSION AND PERSPECTIVES

It is admitted that requirement engineering is an important activity, especially in the security process. However, choosing the good SRE method is still a complex task. Different comparative studies exist in the literature, however, they are all confined to a specific requirements engineering context. Furthermore, no comparative study so far has introduced the significant consideration of the security requirements engineers as the stakeholders who will use the SRE methodology.

In this article, we proposed an evaluation methodology that facilitates the evaluation of SRE methodologies. Our principal motive in this article is to convey the fact that the evaluation criteria are context dependent and cannot be considered as generic. We dealt with this issue in a similar manner as a requirements engineering problem. We elicited requirements from requirement engineers. This task was assisted by our unified list of 20 quality attributes. As consequence, we can derive evaluation criteria specific to a requirements engineering context. It is to note that this article mainly focuses on the derivation of evaluation criteria and not to perform a comparative study. However the resulting criteria can also be used to do a comparative study, if needed.

For future works, we plan to propose refinement patterns to enhance the refinement process in step 1. For instance, when we refined the 20 quality attributes, we referred to some original definitions like [17], [21] for risk. In this regard, it would also be interesting to integrate refinement patterns referring to works like mayor's work [7] that assists in refining risk related requirements with its 7 risk related concepts (*risk*, *impact*, *event*, *threat*, *vulnerability*, *threat agent* and *attack method*). Facilitating the access to such information will make the refinement of requirements R^M easier.

6 Acknowledgement

This work is part of project IREHDO2 funded by DGA/DGAC. The authors thank all the security experts at Airbus who helped us with their useful comments.

7 REFERENCES

[1] N. R. Mead and T. Stehney, *Security quality requirements engineering (SQUARE) methodology*, vol. 30. ACM, 2005.

[2] A. van Lamsweerde, 'Elaborating security requirements by construction of intentional anti-models', in *26th International Conference on Software Engineering, 2004. ICSE 2004. Proceedings*, 2004, pp. 148–157.

[3] A. Van Lamsweerde, *Requirements engineering: from system goals to UML models to software specifications*, Wiley. 2009.

[4] D. Hatebur, M. Heisel, and H. Schmidt, 'A pattern system for security requirements engineering', in *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, 2007, pp. 356–365.

[5] M. Salnitri, E. Paja, and P. Giorgini, 'From socio-technical requirements to technical security design: an sts-based framework', Technical report, DISI-University of Trento, 2015.

[6] S. T. Bulusu, R. Laborde, F. Barrère, A. Benzekri, and A. samer Wazan, 'Towards the weaving of the characteristics of good security requirements', in *International Conference on Risks and Security of Internet and Systems - CRISIS 2016*, Roscoff, France, 2017.

[7] N. Mayer, 'Model-based management of information system security risk', University of Namur, 2009.

[8] B. Fabian, S. Gürses, M. Heisel, T. Santen, and H. Schmidt, 'A comparison of security requirements engineering methods', *Requir. Eng.*, vol. 15, no. 1, pp. 7–40, 2010.

[9] K. Beckers, 'Comparing privacy requirements engineering approaches', in *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*, 2012, pp. 574–581.

[10] D. Muñante, V. Chiprianov, L. Gallon, and P. Aniorté, 'A review of security requirements engineering methods with respect to risk analysis and model-driven engineering', in *International Conference on Availability, Reliability, and Security*, 2014, pp. 79–93.

[11] A. Souag, R. Mazo, C. Salinesi, and I. Comyn-Wattiau, 'Reusable knowledge in security requirements engineering: a systematic mapping study', *Requir. Eng.*, pp. 1–33, 2015.

[12] A. V. Uzunov, E. B. Fernandez, and K. Falkner, 'Engineering Security into Distributed Systems: A Survey of Methodologies.', *J UCS*, vol. 18, no. 20, pp. 2920–3006, 2012.

[13] R. Jain, M. VanLeer, and A. Chandrasekaran, 'A framework for requirements engineering method selection', *Int. J. Ind. Syst. Eng.*, vol. 8, no. 2, pp. 198–214, 2011.

[14] 'IEEE Guide for Developing System Requirements Specifications', *1998 Ed. IEEE Std 1233*, Dec. 1998.

[15] A. Nhlabatsi, B. Nuseibeh, and Y. Yu, 'Security requirements engineering for evolving software systems: A survey', 2009.

[16] N. R. Mead, 'How to compare the Security Quality Requirements Engineering (SQUARE) method with other methods', DTIC Document, 2007.

[17] I. ISO, IEC, and IEEE, 'ISO/IEC/IEEE 29148:2011 Systems and software engineering – Life cycle processes – Requirements engineering', *Int. Organ. Stand.*, 2011.

[18] N. A. Sherwood, *Enterprise security architecture: a business-driven approach*. CRC Press, 2005.

[19] 'NIST Computer Security Publications - NIST Special Publications (SPs)', 17-Jan-2016. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html#800-53. [Accessed: 17-Jan-2016].

[20] D. Firesmith, 'Prioritizing Requirements.', *J. Object Technol.*, vol. 3, no. 8, pp. 35–48, 2004.

[21] I. ISO, 'ISO/IEC 31010:2009 - Risk management – Risk assessment techniques', *Int. Organ. Stand.*, 2009.