Persona Security: A Technique for Supporting the Elicitation of Security Requirements

Marco Santos, Jacilane Rabelo, Raimundo Barreto, Tayana Conte
Universidade Federal do Amazonas (UFAM)
Manaus, Amazonas – Brasil
{marco.santos, jaci.rabelo, rbarreto, tayana}@icomp.ufam.edu.br

Abstract—Safety-critical embedded systems have assisted people in the execution of daily tasks, causing a search for security approaches in the initial phases of the development. The elicitation of security requirements in such systems is a key element for the definition of secure software. Nonetheless, security requirements are mostly ambiguous, incomplete or even not considered, which may be the reason of accidents. In this sense, it is essential to provide a good comprehension of peoples’ roles within the development process, and the interactions with the safety-critical embedded systems. This paper presents the Persona Security technique which aims at aiding software engineers in the elicitation of security requirements. We have performed a pilot study to verify the perception and relationship between the easiness of eliciting security requirements, and find out improvement points. The initial results indicate that dividing the requirements into both system and users allow the software engineer to have a clearer and more general view of the system. However, we also identified improvement opportunities such as: (a) the need for identifying requirements related to users and generating their traceability with the software requirements; and (b) the need for the identification of the security requirements that are most relevant for the problem domain, showing their dependencies and their selection impact.

Keywords: Security Requirements; Safety-critical Embedded Systems; Software Requirements; Requirements Elicitation, Personas.

I. INTRODUCTION

Safety-critical embedded systems (SCESs) are systems in which there is a possibility to cause accidents [1]. Increasingly, SCESs are assisting people in the execution of everyday tasks in areas such as [2]: aircraft flight control, medical devices, weapons, and nuclear systems. Safety-critical software is commonly embedded into some greater technical system [3]. Thus, they represent systems or applications in which failures and errors can lead to severe consequences, harm to properties or the environment, or even death [2].

The major cause for accidents pertinent to SCESs is associated to the poorly performed requirements elicitation or inconsistencies in what the software should do [4]. In this sense, the requirements elicitation is one of the knowledge areas in software requirements [5]. According to Lahoz et al. [6], the elicitation should be capable of producing requirements that preserve the security system’s behavior at any stage, condition or circumstance. The application of good practices for elicitation can avoid errors in the identification and comprehension of requirements [6].

Functional requirements specify what the system should do or should make happen. On the other hand, security requirements specify what the system should not do or what must be kept from happening [7]. In this sense, security requirements are considered the main non-functional requirements that must be provided in a project on SCESs [8]. According to Firesmith [9], security requirements are frequently ambiguous, incomplete or even not treated, which may be the cause of accidents. Consequently, such requirements are considered an essential element to prevent errors and security attacks [10].

In order to assist software engineers in the elicitation of security requirements for SCESs, we have proposed the Persona Security technique. This paper presents how we developed the Persona Security technique and how to apply it through an example. The initial results show that the fact of dividing the requirements into system and requirements related to users provides a general and clearer view of the software to be developed. The functional requirements and the requirements related to users were listed and also traced. Moreover, in the security requirements lists, we noted a difficulty in verifying which requirements were more important, since all requirements were considered representative due to the criticality of the software. We also verified the need for improving the security requirements list, by identifying the security requirements that are more relevant to the problem domain and providing their dependencies. Such improvements will aid software engineers in the selection of security requirements prioritized according to the analyzed critical system.

The remainder of this paper is organized as follows. Section II presents the theoretical background and related work, our findings suggest a deficiency to approaches elicitation of security requirements. In Section III we describe the proposed Persona Security technique. Then, in Section IV we present the results from a pilot study in order to identify improvement opportunities in our proposal. Finally, Section VI presents the final remarks for this paper.

II. BACKGROUND

Safety-critical embedded systems are present in software for cars, trains, airplanes, and possibly within hundreds of
critical security components [10]. Due to the increasing demand on security software, eliciting security requirements has turned into an important task. In most cases, such requirements are included in a system in order to verify [11]:

- Authority problems: in which access to the system must only be granted to authorized users;
- Integrity problems: in which the integrity of the system must be maintained in order to avoid accidental or malicious attacks.

Generic requirements are one of the categories of security requirements [12]. In this sense, generic security requirements are a collection of characteristics and design restrictions to solve security problems in common software. Such requirements are used in different programs and environments, and can be extracted based on good practices and previous experience in well succeeded projects [13]. In this sense, Yang [14] classified generic security requirements into eight categories according to their content: dangerous command-related, initialization-related, data processing-related, detection of failure-related, control of safety critical functions-related, assurance of safety state-related, human-computer interaction-related, and other generic safety requirements.

According to Barry [15], “Requirements Engineering approaches assume that a system is designed for users”. Human Computer Interaction (HCI) covers getting acquainted with people as members of groups or organizations, the conditions under which subjects are likely to want to use their device, as well as the characteristics involved in this interaction [16]. In this sense, Personas is a technique proposed in HCI that offers an understanding of the users of the system regarding their characteristics, needs and goals [17]. Therefore, it defines a persona, which is a profile of a user that is described through data elicitation with users by applying techniques such as interviews or observations [15].

The Personas technique can improve the requirements engineering activities, by identifying the users' needs [16]. In this context, Castro et al. [18] developed Persona*, which consists of a set of inter-related activities that lead to the creation of personas. In this sense, Persona* can allow the elicitation of generic requirements. However, it does not focus on the elicitation of security requirements.

Aiming at developing secure and useful systems, we identified two main challenges in the literature: (a) how can we understand the involved roles in the development process, and their interaction with the safety-critical embedded systems? [2][19] and, (b) how can we consider the security of the system in the requirements engineering process of critical systems? [15]. In order to meet these challenges, we have developed the Persona Security technique.

III. THE PROPOSAL OF THE PERSONA SECURITY TECHNIQUE

The Persona Security technique is composed of a set of grouped activities that lead to the creation of personas and aid in the elicitation of security requirements. In order to minimize risks in the development of software, the Persona Security technique offers a categorized list of generic security requirements. Such requirements were extracted from the Marshall Space Flight Center (MSFC) [12] and have been classified according to Yang’s [14] approach. It is noteworthy, that this list was checked by another experienced software engineer.

To facilitate its application, the Persona Security technique also provides an execution guide, which explains the steps to be followed when applying it. This way, whoever uses the document will have both instructions and examples within a single document. In this sense, Fig. 1 and 2 show part of the categorized list of the security requirements and part of the execution guide, respectively.

<table>
<thead>
<tr>
<th>Category</th>
<th>ID</th>
<th>Generic Security Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human-Machine Interaction</td>
<td>SR01</td>
<td>The software must provide status on all controllable restrictions to the technical team, or to the control executive.</td>
</tr>
<tr>
<td></td>
<td>SR02</td>
<td>The software must incorporate the capability to identify and show status alerts for each software restriction related to critical commands.</td>
</tr>
<tr>
<td>Dangerous Command-Related</td>
<td>SR06</td>
<td>Rewriting commands must require multiple actions from the operator.</td>
</tr>
<tr>
<td></td>
<td>SR12</td>
<td>The software must provide a unique and independent command to control each controllable restriction.</td>
</tr>
<tr>
<td></td>
<td>SR13</td>
<td>All software restrictions that are associated to a command must have a unique ID.</td>
</tr>
<tr>
<td>Initialization-Related</td>
<td>SR17</td>
<td>The software must start and restart replaceable units in a safe state.</td>
</tr>
</tbody>
</table>

Figure 1: Part of the categorized list of the security requirements

You received two documents: (1) a scenario composed of a list of functional requirements for the persona (profile) and the safety-critical embedded systems; (2) the categorization of the generic security requirements. Based on that, you must map the functional and security requirements using the instructions contained within this document.

Initial Procedures:

- Describe the persona profile – see document (1) – scenarios with functional requirements
  - << The description of a persona is composed of: attitudes, goals, needs and behavior >>
  - Example: “John is a 64 year old man who values his family. He is an experienced driver. Other people see him as a rational, practical and self-confident man with authority. He can easily get annoyed with drivers of other vehicles and (…).
- Add the ID of the Functional Requirements of the persona (Profile) – scenarios with functional requirements
  - Example: FR01, FR02.
- List the ID of the Functional Requirements for the safety-critical embedded systems – scenarios and functional requirements
  - Example: FR11, FR09.
- Add the ID of the Security Requirements for the safety-critical embedded systems - see document (2) - categorization of security requirements
  - Example: SR01, SR02.

Figure 2: Execution guide for the Persona Security technique
Fig. 3 shows the execution process of the Persona Security technique, describing the interaction between its activities:

![Diagram of Persona Security technique](image)

**Figure 3- Activities for applying the Persona Security technique**

In this sense, the activities for applying the Persona Security technique are:

- **Activity 1 – Define Personas:** Based on the results from the previous activity, the users’ needs from the critical system are groups. In the end, each profile will represent a persona and will be used to create a persona document. This activity is included in the following phases [20]: Requirements Elicitation, Requirements Analysis, Requirements Specification and Requirements Validation;

- **Activity 2 – Select Security Requirements:** During this activity, a list of categorized generic requirements (as shown in Figure 1) is provided to the interviewees. Then, the interviewees must select the requirements that can be applied to the system;

- **Activity 3 – Identify security requirements patterns:** The main goal of this activity is to identify a list of security requirements that is representative of the SCES;

- **Activity 4 – Validate the existence of redundancies and integrity:** During this activity, the analyst or the client’s representative will verify the generated documents in order to identify the existence of redundancy or omission. This activity includes the requirements validation phase;

- **Activity 5 – Define Types of Personas:** The created personas will be prioritized to determine the most important user profile, or the primary persona [16]. In the case that the critical system possesses only one user profile (persona), that will be the primary persona. Then, we must add the list of representative security requirements (see Activity 3) in order to create a security persona. In this sense, the definition of a persona involves the activities of [9]: requirements analysis and requirements specification.

**IV. THE EXPERIMENT**

Our main motivation for performing this study is to verify if the Persona Security technique aids in the elicitation of security requirements in safety-critical embedded systems. Since this was a preliminary evaluation of the technique, the pilot study was performed in an academic environment. We choose an academic environment since we would not require spending real software practitioner’s hour costs. Also, an academic environment is smaller and allows the observation and testing of new technologies to be transferred from academy to industry [22].

This pilot study was performed following three well-defined activities which will be explained below:

**Planning:** First, we defined the goal of this study based on the GQM (Goal-Question-Metric) [23] paradigm, as shown in Table 1.

**TABLE I. GOAL OF THE PILOT STUDY BASED ON THE GQM PARADIGM**

<table>
<thead>
<tr>
<th>Analyze</th>
<th>Persona Security Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>For the purpose of</td>
<td>Characterize</td>
</tr>
<tr>
<td>With respect to</td>
<td>The perception over: (a) ease of use/assistance for the elicitation of security requirements; (b) aspects that aid or constrains in the application of the technique; (c) recommendations in the utilization of the technique to elicit security requirements</td>
</tr>
<tr>
<td>From the point of view</td>
<td>Software Engineering researchers</td>
</tr>
<tr>
<td>In the context of</td>
<td>A security requirements elicitation of a safety-critical embedded system performed by a high experienced doctorate student</td>
</tr>
</tbody>
</table>

After defining the goal of this study, we characterized it by describing the activities to be performed, the resources and the trainings to be ministered in order to carry out the study. Finally, we prepared the characterization form, the Consent Term, and post-experiment questionnaire. The characterization form serves to verify: a) knowledge level in requirements elicitation and critical systems; b) their working experience in projects and software development to critical systems (measured in number of projects); c) working time in software development. The consent term informs about data confidentiality and voluntary participation. Lastly, post-experiment questionnaire aims to gather the practitioners’ opinions.

**Execution:** We carried out the pilot study with a highly experienced doctorate student from Federal University of Amazonas (Ufam). He was enrolled in one of the Informatics
doctorate programs in Brazil. According to his characterization form, this student had more than 4 years’ experience in developing software (both industrial and academic). Also he had worked in several development projects as an analyst and had prior knowledge with the development of non-functional requirements, mainly usability.

We handled the subject instructions on how to apply the technique. Also, we provided the guide for using the Persona Security technique, which is shown in Fig. 2. Such guide already illustrates an utilization example. The guide for using the Persona Security technique shows examples on how it should be filled. We also provided a scenario of a safety-critical embedded system composed of functional requirements and a persona (profile). Such scenario is from a real software development process from an Unmanned Ground Systems. In this sense, part of the scenario is shown in Fig. 4.

<table>
<thead>
<tr>
<th>1. Description</th>
</tr>
</thead>
</table>
This document describes the requirements for a robotic mobile vehicle, which represents an example of unmanned system where even if it has automated actions, it still depends on the control of an operator. (…)

The system shall meet the following functional requirements:

- FR08: The system shall allow the robotic vehicle to send data and that it is remotely controlled following wireless networks patterns (Wi-Fi);
- FR09: The system shall provide the operator with an adequate way to control the vehicle;
- FR10: The system shall allow the vehicle to be remotely controlled through a computer;
- FR11: The system shall allow the vehicle to be remotely controlled through a cellphone;
- FR18: The system shall allow the vehicle to transport an object in order to perform specific activities;
- FR24: The system shall allow the operator to remotely start, or interrupt the vehicle’s functioning.

Moreover, the subject received a list of categorized generic security requirements. Fig. 1 shows part of the categorized generic security requirements list. Then, we gave the subject the template of the Persona Security technique so that he could list: (a) the critical system functional requirements; (b) requirements for the personal profile; and (c) security requirements relevant to the analyzed scenario. Finally, the subject answered a questionnaire regarding ease of use, aspects that could aid and any constrains with the applicability of the Persona Security technique. Fig. 5 shows part of such questionnaire.

1. In your opinion, the Persona Security technique facilitated/assisted in the elicitation of security requirements? Please Comment.

**Figure 4: Part of the scenario of the robotic vehicle**

**Figure 5: Evaluation Questionnaire**

**Analysis and Results:** In this stage we analyzed the results from this study using qualitative analysis procedures. Qualitative studies allow a wider comprehension of the studied phenomenon, which is necessary for analyzing complex questions in software engineering [24]. Besides the possibility of answering research questions that involve variables that are difficult to quantify; and supporting answering the reason for research questions that were approached in other quantitative studies, qualitative methods allow the researcher to deepen into the complexity of the problem instead of abstracting it [24]. We have analyzed the data from the evaluation questionnaire using concepts from Grounded Theory (GT) [25].

GT is a qualitative method for data analysis, in which a theory is derived from data, systematically gathered and analyzed by means of the research process. The GT method is based on coding – the analytic processes through which data are fractured, conceptualized, and integrated to form a theory [25]. The data analysis began with the open coding of the questionnaires (Fig. 5). The qualitative analyses of the results from the study are described as follows.

**V. RESULTS FROM THE PILOT STUDY**

During the execution of the study, two researchers observed the subject while he applied the Persona Security technique. Through observation, the researchers were able to verify and make notes regarding how the subject applied the technique. Right from the beginning of the application of the technique, the subject asked if he could relate (map) the requirements from the persona profile with the robotic mobile vehicle. Since, we were interested in verifying improvement opportunities and understand how would the Persona Security technique would be applied, the researchers answered that the subject could list the requirements in the way that would be more suitable and easier to use for him.

In this sense, the researchers notes that the subject applied the following strategy:

- First, the subject created a representation to relate the requirements using arrows allowing make the traceability between requirements involved, where:
  a) \( A \rightarrow B \): meaning that \( B \) is necessary in order to achieve \( A \);
  b) \( A \leftrightarrow B \): meaning that \( A \) and \( B \) are mutually necessary for each other.

- Then, the subject identified the requirements regarding the persona profile and related such requirements using the approach described above;

- After that, the subject identified the requirements regarding the critical system and related them using the same approach. In this sense, the relationship was made for both the persona and the critical system functional requirements;

In Fig. 6 we show part of the document as how it was filled by the subject.

When analyzing the results from the elicitation and the relationships created by the subject, we noticed the importance of requirements traceability. The fact that it is necessary to first
identify the persona requirements and then map such requirements with critical system made it easier for the subject to understand how the system works and what it must do.

<table>
<thead>
<tr>
<th>Document TEMPLATE for the Persona Security technique</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Persona description</strong></td>
</tr>
<tr>
<td><strong>Functional Requirements of the Persona (Profile)</strong></td>
</tr>
<tr>
<td><strong>Functional Requirements of the Mobile Robotic Vehicle</strong></td>
</tr>
<tr>
<td><strong>Security Requirements for the Mobile Robotic Vehicle</strong></td>
</tr>
</tbody>
</table>

Figure 6: Requirements List on Persona Security

In this sense, when comparing the list of requirements from the subject with those in the oracle (in this context, a document containing the corrected elicited requirements, which is used to verify the subjects answers), we verified that the subject managed to identify all requirements from the persona and the robotic system correctly. On the other hand, the subject was not able to trace four requirements (three from the persona and one from the system). Therefore, one identified future research question for this research is: “Tracing the requirements from the persona with those for the critical system allows a better understanding of how the system works?” Moreover, another research question is: “Relating the requirements facilitates the identification of which security requirements are more critical for the system?”

When identifying the security requirements for the system, the subject ended up selecting and rejecting the requirements directly in the provided document. Thus, we verified that such document should be improved. Initially, we thought this document would be used as a reference document (see the original version in Fig. 1), however, it acts as a checklist and we must add check squares in order for it to be operationalized. By doing such change, software engineers applying the Persona Security technique will not waste time listing the requirements.

We noticed that the subject had difficulties in identifying which security requirements would be suitable for the system, as he considered that all of them were important. The following quote shows such concern:

“(..) I don’t know where exactly the security requirements would fit, since I actually want to accept and include them all” – Subject

Regarding **ease of use / assistance** of the Persona Security technique to elicit security requirements, the subject stated that the technique facilitates its use.

“The fact of dividing the requirements both for the persona and the automated part allowed me to have a clearer view of the system…” – Subject

It is noteworthy that when knowing about the criticality of the system, the subject also became insecure regarding the identification of security requirements.

“(..) when I knew how critical the system was, and imagining use situations, I wanted to mark all security requirements” – Subject

Based on these answers, we noticed that the list of generic security requirements will need to be modified. In this sense, when asked about if he would change the Persona Security technique, the subject answered:

“Yes, I would change it. I would categorize the security requirements according to their priority and would verify with the client” – Subject

To make this changes, we will map the security requirements that are more relevant to the problem domain, and which are its interrelated requirements and which are not necessary. For instance:

- For the mobile robotic system the SR01 requirement is essential. When selecting that requirement, the requirements SR08, SR09 and SR22 are mandatory. Moreover, requirements SR34 and SR35 are not important for this problem domain. Then, requirements SR01, SR08, SR09 and SR22 will be selected.

When asked about **Using the Persona Security technique** Again, the subject added:

“Yes, I would use it to know the system. But I am not quite sure in which part the security requirements would fit…” – Subject

The subject’s answer to this question allowed us to verify the need to improve the list of generic security requirements. In this sense, a further research question would be: “Categorizing the list of generic security requirements by essentiality and priority would facilitate the elicitation process?”

The subject also stated that he would **Recommend the Persona Security technique**:

“Yes, but a generic approach to aware the development team of the importance of the security requirements, which can be defined based on the list” – Subject

Although, the subject was able to correctly identify all requirements regarding the persona profile, it was not clear for him why this was necessary:

“Why do a need a single persona? What is the influence of such persona in the elicited requirements? This was not clear.” – Subject

The creation of a persona profile allows the presentation of the user needs and how an interface must be designed to meet them. The scenario presented in this pilot study was limited to just one persona, which restricted the analysis of the integration
of the Personas technique to the proposed Persona Security technique. After improving the Persona Security technique, we will perform a feasibility study to verify the acceptance of the approach. In this context, a new scenario will be investigated with more than one persona profile in order to verify the importance of such profiles in the elicitation of security requirements.

VI. CONCLUSIONS

This paper presented the Persona Security technique, which proposes to support the elicitation process of generic security requirements of Safety-critical embedded systems. We have carried out a pilot study to verify the way in which the technique can be applied to identify the system’s requirements of the persona profile, as well as the security requirements. Such study was performed with a doctorate student in the Informatics program at Federal University of Amazonas. The subject had knowledge in the requirements elicitation process.

We have analyzed the results using qualitative analysis approaches. Thus, we identified that the Persona Security technique aided the subject in understanding the critical embedded system as a whole, and even have a view of what risks can be involved in the chosen scenario. An interesting fact was that the subject traced/mapped the requirements, and this helped him to get to know the system. Moreover, the subject had difficulties in identifying which security requirement was needed in the critical embedded system, showing that there is still room for improvement in the development of the proposed technique.

As future work, we intend to: (a) perform a systematic review on security requirements elicitation in SCES, to make possible to compare the technique with other proposals in the field of security requirements elicitation, and evolve the list of generic security requirements, providing an indicator of which security requirements can be applied depending on the specific context of the application; (b) carry out a new empirical study with a higher number of subjects to validate and evaluate the improvements on the Persona Security technique; (c) verify whether the addition of traceability to the technique is feasible; (d) figure out if it is possible to automate parts of technique. Thus, by adding such suggestions in Persona Security technique, we intend to improve its value, allowing software development teams may add greater certainty for safety-critical embedded systems.

ACKNOWLEDGMENTS

We would like to thank the financial support granted by: CAPES (Doctorate); FAPEAM through process number 01135/2011 (PRONEX Project); and Project N.021/2011 (Universal Amazonas). We would like to thank Luis Rivero for the translation and textual revisions of this paper and also the practitioner who participated in this study.

REFERENCES