A Goal based Framework by adopting SQUARE Process for Privacy and Security Requirement Engineering

Baber Hayat
University of Lahore
Department of CS/IT

Ribha Shakoor
University of Lahore
Department of CS/IT

Sahrish Mubarak
University of Lahore
Department of CS/IT

Komal Basharat
University of Lahore
Department of CS/IT

ABSTRACT
Identifying, categorizing and prioritizing requirements in terms of privacy and security is the main concern for software developers. Privacy requirement gathering is remain the challenge for software engineers for distributed and complex software. Privacy and security requirement engineering is important step in building these software systems. For this different privacy requirement engineering approaches has been proposed such as security quality requirement engineering (SQUARE) which provide a step for elicitation of requirements in terms of privacy. The purpose of this paper is to support the requirement engineers by modifying the SQUARE approach by providing a process of analysis and evaluate the goal based assets with a framework to identify security goals in accordance to the privacy and security requirements both.

Keywords
Requirement engineering; privacy and security requirement engineering; security goals

1. INTRODUCTION
At present, software engineering is highly concern with the privacy and security of data and trend is continuously widespread and increasing. Consequently, privacy needs to be considered early in software development process. Maintaining privacy and security during requirements gathering and analysis phase is still a challenging task even several privacy and security requirement approach are proposed.

Privacy and security measures while designing has a main concern for software designers. These are considering as technical choice made during implementation [1]. The different between security and privacy is that threats to individual privacy often rise from authorized users of the system rather than from unauthorized one [2]. Any delusion in analyzing and classifying privacy and security requirements can lead to the serious concerns that not only impact the software functionality but also results in loss of reputation, financial penalties and even long term legal prosecution and consequences [3]. Lack of adequate knowledge or expertise is one of the most common reason of flaws in privacy and security requirement engineering [3,4].

Goal is an important part in elicit, specify, analyze and validate the requirement [5]. Identifying goal is one of the initial step in requirement engineering [3,6,7]. These goals provide a reference frame for identifying privacy and security that implied to requirements that are initially identified [3].

This paper presents a goal based framework by adopting security quality requirements engineering. This framework helps in eliciting, categorizing and prioritizing the security requirements. The proposed framework also presents a pattern at the stage of identifying assets and goal in SQUARE approach with determining agents, scenarios, constraints and obstacle during analysis and evaluation of identified goals and assets.

The rest of the paper is organized as follows. Section 2 describe the goal based framework in identifying assets and security goals in the 2nd step of SQUARE process. Section 3 conclude the framework.

2. GOAL BASED FRAMEWORK
2.1 Elements of Goal Based Framework
The elements of goal based framework are following:

2.1.1 Assets
Assets is a list of inputs that are used and managed by software system. Assets can be a business or system assets. Identification of organization assets is an important step it could range from confidential data e.g. database to service availability. Different techniques can be used to identify the assets like interview, questionnaires or brainstorming. Assets can be categorized under the preferences of low, medium and high-level confidentiality, integrity and availability [13]. In our scenario, we do not assume to categorize the assets in terms of references.

2.1.2 Security properties
Security properties are related to the security goals of system in terms of assets and expect to have these properties to protect the assets. The definition of these security properties is identified and accepted by the participant involved in this process on the very first step of SQUARE process. We have identified the following categories of security properties [8] that are confidentiality (C), integrity (I), authentication and identification (ID), privacy (PR) and accountability (AY).

2.1.3 Actions
For each asset, we choose standard CRUD (create, read, update, delete) action with addition of search operation of information actions:

Search: action related to find some sort asset e.g. employee detail from specific city.

2.1.4 Security Action
Detecting and preventing a security breach is the ideal scenario [3]. Thus, to ensure the confidentiality and security of employee record is done into three security action goals: To prevent the breach, to detect the breach and to respond the breach.

Prevent (p): proactively prevent a security breach [9].

Detect (d): detect the breach in case of security breach [9].

Respond (r): respond to the detected breach [9,10].

By seeing the more security action during the requirement gathering phase helps in determining more comprehensive set of security goals.

2.2 Agree of Definition

First stage of square process which covers the list of comprehensive technical and non-technical terms with definitions by stakeholders and software requirement team that will benefit the both participants by reducing ambiguity, increase communication effectiveness, speed up the process and solve problem in early stages.

Table 1. Terms for Privacy

Access	Cookie	Functional
Aggregation	Credential theft	manipulation
Anonymity	Confidentiality	Identification
Anonymous	Data breach	Identity fraud
Authentication	Data privacy	Information
Authorization	Disclosure	monitoring
Accountability	Distortion	Integrity
Graphics	Exposure	privacy

2.3 Identify Assets and Security Goal

The second step in SQUARE process is to identify assets and security goals. This step is the initiation of the discussion between stakeholders and requirement engineers regarding assets and associated goals of the project and organization. We divide this step into two stages of analysis and evolution.

2.3.1 Analysis

Analysis is the process of exploring and gathering documentation, ranging from information about organization to the system specific information for identifying, organizing and classifying goals. Assets may be sensitive resource of software system or services that can be mutually related, for instance or can be composed of other assets [3]. However, there are several related techniques scenarios analysis, identification of goal obstacles and constrains, and goal operationalization [19]. Agent and scenarios are two things that are identified during analysis process.

2.3.1.1 Agents

Agents are the entities or process that seeks to achieve goals within an organization or system with responsibility for achieving certain goal.

2.3.1.2 Scenarios

Scenarios are behavioral description of system and its environment arising from situations. These scenarios are useful for evaluating design alternative and validating designs.

3.3.2. Evaluation

The goal requirements and assets needs to remain as stable as possible. Although it is true that requirements can be variate by being misunderstood or misinterpreted. Goal should be more stable than process, organizational structure and operation [19] but goals change gradually by changing needs, circumstances and goal prioritization. The evaluation of goal can be done by goal elaboration and refinement. Goal elaboration is done by identifying obstacle and analyzing scenarios. Where obstacles are the behavior that prevent or restrict the achievement of a goal and Constraints are the requirements or condition that must be met for the achievement of goal.

Goal refinement occur when same goals are merge, or merge into sub-goal categories', when goals are identified and operationalized.

2.4 Elements of Goal Based Framework

To support the analysis of security goal associated with the assets a security pattern has been proposed that covers all security properties and security actions discussed earlier and help in risk analysis stage of SQUARE process [3]. This pattern indicates list of actions by determining security properties for specified security goals. For example, <read | store > indicate needs of confidentiality. To abbreviate, each pattern is identified as:

<SecurityActions–SecurityProperty–Assets–Actor–Action>

Through this security goal pattern, we can determine the security goals for software system assets. For example, reading asset of organization "employee's salary record", associated with security properties of confidentiality, integrity as well as identification and authentication. For each security property, we also consider all four security actions. Security goals using the identified privacy terms shown in figure 1 are generated using the security goals patterns as follow:

Table 2. Goal Pattern

Security Actions	Security Properties	Asset	Actor	Action Type
<prevent> | <detect> | <respond> to a breach	Privacy (PR)	Of <asset >	When <actor> performs	<read>
	Accountability (AY)			<create | read | delete | update >
	Confidentiality (C)			<read | store>
	Integrity (I)			<create | update | delete >
	Id & Authentication (ID)			<create | read | delete | update | search>

The identified security goals for employee salary record are following:

Goal A: System needs to prevent a breach of confidentiality of employee salary record when user reads the data.

Goal B: System needs detect a breach of Privacy of employee salary record when user reads the data

Goal C: System needs respond to breach of Accountability of employee salary record.

Steps for Applying Security Goal Pattern

The functional requirements, software system's assets are the input of this security goal based framework. The output of this goal based pattern is the identified security goals that are associated with assets. It is necessary to properly consider the assets to identify security goals by apply security goal based patterns.

Step: Apply security goal pattern to identify set of security goals.

1. Identify all assets of an organization.
2. Identify and agree on definition of security properties.
3. Identify all security actions for managing organization's assets.
4. Identify goals related to various security properties based in the actions that are performed on the assets.
5. Identify goals related to different security actions.

6. Set the goal pattern to the asset.
7. Identify any new functionality based on step 6.
8. Identify any new assets that might be created in system based on step 6 and 7.

2.5 Develop/Design Artifact

In this step requirement engineer design artifacts to support the security requirement definitions of the system being developed. These artifacts may describe existing system or define the purpose and environment for the proposed system. According to the privacy and security of system, the potential artifacts are: system architecture diagram, use case scenarios, misuse case, attack trees, user role hierarchy, models, templates and forms.

2.6 Perform Risk Analysis

To perform the risk analysis requires experts in risk assessment methods, support from stakeholders and requirement engineers. It identifies the vulnerabilities and threats that the system face. Assets and artifacts from the step 2nd & 3rd of SQUARE process are the input of this stage. This step is also help by the security goal patterns that are identified in step 2nd. Risk analysis step also consider the policies, regulation, and laws for privacy it tends to be different from goal of security risk assessment [2].

2.7 Select Elicitation Technique

In general elicitation is a process of sitting down with stakeholders to try to understand the stakeholders' security requirement needs [11]. Requirement engineers determine and test various requirements elicitation techniques and model that will work best for the given system, project team, and project environment. The selection of elicitation technique is based on various factor e.g. expertise of requirement engineer, the size and scope of client project, level of security to achieve, cost effort benefits and organizational policies [11]. According to the Hubbard, Wood "Accelerated Requirements Methods", "Joint Application Design" or "structured interviews" has been successful methods in eliciting security requirements and almost applicable under all circumstances [12, 11]. These techniques help in overcoming communication issues between stakeholders from different backgrounds. Other than these some of elicitation techniques are interviewing, brainstorming, sketching and storyboarding, use case modeling and questionnaires and checklist [13].

2.8 Decompose & Categorize Requirements

Requirement engineers decompose the elicit requirements or other constraints and categorize as system and software level by creating an initial requirement architecture. It helps the requirement engineers to separate essential requirements, goals and constraints. By choosing system architecture prior to the requirement process distinguish constraints over requirements [11]. This further helps in categorizing requirements such as essential system level, non-essential system kevel, essential software level, non-essential software level and architecture constraint [13].

2.9 Prioritize Requirement

There are many factors that are directly and indirectly effect the prioritization of requirements. The prioritization of requirements may not only depend on prior steps but also on risk assessment of associated threats. Lack of resources, time, cost changes in project, changes in goals also security breaches, such as loss of life, loss of reputation and loss of consumer confidence have influence on prioritization. A good requirement prioritization has some advantages, such as following [14,15].

- Clarify for developer which requirements are important and mere embellishments.
- Can make tradeoff between conflicting goals such as quality, cost and time.
- Help the manager to release the plan that will meet customer expectations.

There are many structured and un-structured techniques can be used to for requirement prioritization. Unstructured is a process of simple discussion between stakeholders for prioritization while structure techniques are Pair-wise comparison method, method of prioritization of legal requirements [2].

2.10 Inspect Requirement

Inspection of requirement is a last but critical step in requirement engineering. The goal of inspection step is to remove the defect, clear ambiguities and ensure the accuracy and verify the requirements.

There are number of methods to do requirement inspection, from ad hoc to checklist, Fagan review, scenario based inspection, peer review inspection [2]. Over all inspection methods Fagan inspection technique is consider as effective in identifying defects in requirements [11]. The outcome of this process is the final requirement document that has been verified by all stakeholders and requirement engineers.

3. CONCLUSION

We have proposed a goal based framework for identifying security goals related to the assets of an organization's system by adopting SQUARE process. We also expand the step of identifying assets and goals of square process by distributing it into two categories of analysis and evaluation. This framework is supported by system assets, security actions or properties. This framework helps in identifying area where goals have not been specified in the very early stage of SQUARE process for determining system requirement specifications. Our research contributes towards the identification of security goals which supports in identifying the security properties that are associated with the requirements at the early stages that help as more definite inputs for later stages of SQUARE process.

4. ACKNOWLEDGMENTS

In the name of Allah, the Most Gracious and the Most Merciful Alhamdulillah, all praises to Allah for the strength and blessings. This dissertation would not have been possible without the guidance and the help of teachers of computer department of UOL. We are also thankful to our friends and families whose silent support led us to complete our paper.

5. REFERENCES

[1] A. Souag, R. Mazo, C. Salinesi and I. Comyn-Wattiau, "Reusable knowledge in security requirements engineering: a systematic mapping study", Requirements Engineering, vol. 21, pp. 251-283, 2015.

[2] A. Bisjwe, N. R. Mead, "Adapting the SQUARE Process for Privacy Requirement Engineering", July 2010.

[3] M. Riaz, J. Stallings, M. P. Singh, J. Slankas, L. Williams, "DIGS-A Framework for Discovering Goals

for Security Requirement Engineeing", Empirical Software Engineering and Measurement, Sept. 2013.

[4] G. S. Walia, J. C. Carver, "A systematic literature review to identify and classify software requirement errors", Information and Software Technology, vol. 51, Issue. 7, pp. 1087-1109, July 2009.

[5] Q. He and A. I. Anton, "A Framework for Modeling Privacy Requirement in Role Engineering".

[6] A. I. Anton and C. Potts, "The Use of Goals to Surface Requirements for Evolving Systems", Proceedings of the 20th International Conference on Software Engineering, pp.157–166, April 1998.

[7] N.R. Mead, E. D. Houg and T. R. Stehney. "Security Quality Requirements Engineering (SQUARE) Methodology", Software Engineering Institute, 2005.

[8] M. Riaz, J. King, J. Slankas and L. Williams. " Hidden in plain sight: Automatically identifying security requirements from natural language artifacts", 22nd International Requirements Engineering Conference (RE), pp. 183–192, 2014.

[9] M. Schumacher, E. Fernandez-Buglioni, D. Hyberston, F. Buschmann and P. Sommerlad, "Security Patterns: Integrating Security and Systems Engineering", 2006.

[10] D. Firesmith, "Specifying Reusable Security Requirements", Journal of Object Technology, vol. 3, 2004.

[11] N. Mead, "SQUARE Process", Software Engineering Institute, Jan 2006.

[12] R. Hubbard, N. Mead and C. Schroeder, "An Assessment of the Relative Efficiency of a Facilitator-Driven Requirements Collection Process with Respect to the Conventional Interview Method." Proceedings of the International Conference on Requirements Engineering, June 2000.

[13] P. Salini, S. Kanmani, "Security Requirement Engineering Process for Web Application", Procedia Engineering, vol. 38, pp. 2799-2807, 2012.

[14] K. Joachim. "Software Requirements Prioritizing", Proceedings of the Interna-tional Conference on Requirements Engineering (ICRE ‟96), pp. 110-116, April 1996.

[15] K. Joachim & R. Kevin, "A Cost-Value Approach for Prioritizing Software Requirements." IEEE Software, vol. 5, pp. 67-74, 1997.

[16] Y. Ito, H. Washizaki, M. Yoshizawa, E. B. Fernandez, "Systematic Mapping of Secirty Patterns Research", 22nd Conference on Pattern Language of Programs Conference, 2015.

[17] R. Salvin, J. M. Lehker, J. Niu, "Managing Secuirty Requirements Patterns Using Feature Diagram Hierarchies", Requirement Engineering Conference (RE), 2014 IEEE 22nd International, 2014.

[18] M. Riaz, L. Williams, "Secuirty Requirements Patterns: Understanding the Science Behind the Art of Pattern Writing", Requirement Patterns (RePa), 2012 IEE Second International Workshop, 2012.

[19] A. I. Anton, "Goal Based Requirement Analysis", 2013.