Global Journal of Multidisciplinary Studies Available online at www.gjms.co.in

Volume 3, Issue 3, February 2014

ISSN: - 2348-0459

REQUIREMENT ENGINEERING PARADIGM

Shweta Sankhwar[1],Virendra Singh[2],Dr.Dhirendra Pandey[3]

Department of Information Technology

[1,2,3]BabasahebBhimraoAmbedkarUniversity,Lucknow,India

,

ABSTRACT

Requirement Engineering is an important phase of any software development. The requirements should be unambiguous (measurable and testable), traceable, consistent, and approved. Now-a-days the importance of security is growing with the rise of phenomena such as e-commerce and nomadic and geographically distributed work. Therefore, it becomes necessary to apply requirement engineering practices in every phase of software development. Requirements engineering for software development process is a complex exercise that considers product demands from several viewpoints, roles, responsibilities, and objectives. In this paper, we propose an effective requirement engineering process model to generate appropriate, accurate, consistent requirements.

Keywords: Security Requirement (SR), requirement elicitation, requirement analysis, requirement prioritization, requirement management.

I. INTRODUCTION

Requirement engineering involves finding, maintaining and managingrequirements for developing quality software. Requirement engineering aims to collect good requirements from stakeholders in the right way. It is important for every organization to develop quality software products that can satisfy user's needs. The purpose of this paper is to give a review of requirements engineering and to present a research agenda based on this review. The review is not intended to be comprehensive, on the contrary it is based on a particular framework and highlighting principal issues and it relies on a personal assessment of the contributions in each of the key areas.The principal of requirements engineering activities and their relationships could be described i.e., to introduce techniques for Security requirement elicitation, Security requirement analysis, Security requirement prioritization, Security Requirement Management. Several techniques that can be used to gather the requirements, but some key points to remember are that the requirements must be systematic, verifiable, related to identified business needsor opportunities. [1] This paper reviews the area of requirements engineering in elaborated form.Requirements engineering is gleaning a comprehensive and accurate understanding of the project's business need. It including strong understanding of the business need will help and guard against scope creep and gold plating, as well as select the proper stakeholders and techniques. Eliciting requirements is ensuring that an adequate amount and mix of stakeholders are secured for the project's duration. All requirements likewise functional requirement including behaviour of software i.e., performance, physical requirement, and environmental conditions are considered to develop the software. In this paper, we propose an effective requirement engineering process model to generate appropriate, accurate, consistent requirements. [2] The organization of this paper is, section-I represents the introduction, section-II represents proposed framework and table details, section-III represents conclusion, and section-IV shows the References.

Volume 3, Issue 3, February 2014
ISSN: - 2348-0459

II. THE FRAMEWORK

This section of the paper describes a model of Requirement engineering that represents a generalization of all known sub phases and their methodologies and techniques. It explicitly highlights the role knowledge plays in performing both requirement engineering sub-phase and its technique selection. It provides a unified framework for understanding the purpose and role of requirements elicitation in software development; it describes how sub phases could be represented in terms of the proposed model. Requirement Engineering (RE) is the process of gathering, evolving and managing requirement. Requirement Engineering sub-phases are shown in the figure- Sub-phases of Requirement Engineering.

Figure-Sub-phases of Requirement Engineering

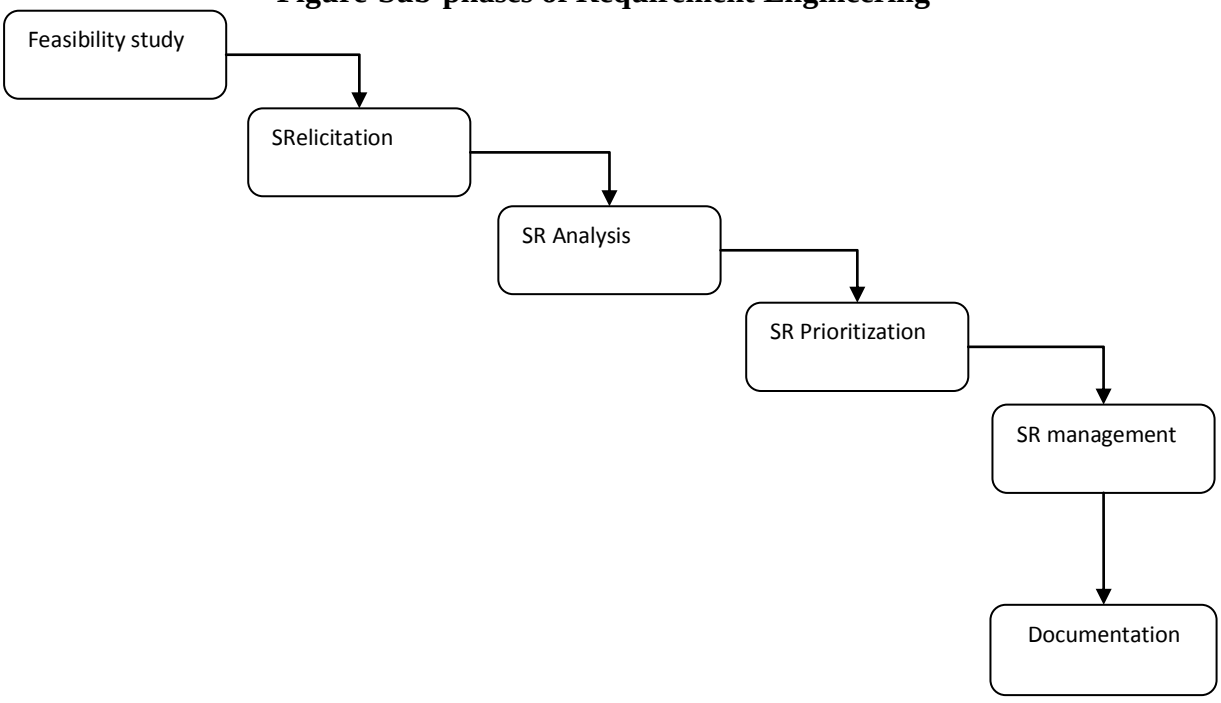

Table. Methodology and Techniques of SecurityRequirement Engineering

Security requirement elicitation	**Security requirement analysis**	**Security requirement prioritization**	**Security Requirement Management**
• Stakeholder identification • Identification of security requirement (functional and non- functional) • Asset identification • Threat identification • Security requirement analysis • Security requirement prioritization • Security requirement management	• Data comprehensive ness • Conflict resolution • Grouping of requirement	• Threat evaluation • Vulnerabilities measurement • Asset rating • Risk Estimation • Threat prioritization	• View point identity • Traceability of security requirements • Functional and non-functional requirements • Design constraint

Feasibility analysis should take into account operational, technical, and financial feasibility prior to starting and during a software development project. Requirements ambiguity needs to be avoided when gathering and documenting requirements. The three most common sources of requirements ambiguity are missing requirements, ambiguous words, and introduced elements. The systems analyst is responsible for eliminating ambiguity in the final requirements specification document. The framework, or methodology used to gather requirements, there are three generally accepted ways to answer the

questions needed to build the requirements list:

(1) Global research, such as reviewing reports, forms, and files, and reviewing the performance of other companies by contacting or visiting them;

(2) Individual interviews, surveys, observation, research, site visits, and so on; and

(3) Group sessions in the form of JAD, EJAD, and/or rapid analysis techniques. Each of these approaches requires that the systems analyst ask appropriate questions, provide feedback to the user, and have good communication skills. [3]

Requirement elicitation

Effective requirements elicitation is essential to the success of software development projects. The systems analyst uses this activity to gather the essential requirements through the variety of techniques, such as interviews, questionnaires, group brainstorming meetings, and voice and e-mail.

The process of stakeholder analysis involves identification of individuals or roles that should have a voice in the requirement engineering process. Stakeholder could be clients, users and other beneficiaries, they may also be people involved in subsequent design, implementation, maintenance of the system. Stakeholder analysis involves understanding their responsibilities, capacities and the organizational relations between them.Common stakeholders for all projects include such as Architecture Office (AO), Testing & Certification Office (TCO), DBMO, Records Management Team, Application Support Group, and Information Security Office (ISO). .

Requirement elicitation method can help in producing a consistent and complete set of security requirements. Stakeholder identification is base point for gathering of requirements. Identification of functional and non-functional requirement is accomplished in elicitation phase. Functional Requirements defines the processes, information, and interactions of software. Non-functional Requirements specific parameters of the software project which include interface, performance, usage, security, capacity, back-up, audit, availability, physical, and site requirements. Non-functional specifications also address likewise security, hosting, encryption, environment, disaster recovery, performance, physical, capacity, supportability.[4]

Requirement analysis

Security requirements engineering should be precise, adequate, complete and non-conflicting with other requirements. Requirement could be implemented and maintained if they are consistent and accurate [4]**.**Requirements analysis are of two different activities i.e., capturing requirements and analysing requirements.

Capturing requirements is the process of communicating with stakeholders to conclude what the requirements are. This is basically accomplished through interaction, meetings and with the help information communication technologies. Requirement analysis is the process via standard tools and practices to generate a single unambiguous baseline of the requirements. [5] Once all the stakeholders agree on the requirements, the baseline is created and becomes the formal requirements source. Security requirement analysis helps developers and all other stakeholders with a clear understanding of the requirements which define the boundaries of the system and prioritize features to provide a basis for possible iterations**.**

Requirement analysis is the process of reasoning about the requirements that have been elicited; it involves activities such as investigative requirements for conflicts or inconsistencies, combining related requirements.

Requirement prioritization

Prioritization identifies the most appropriate requirements for a specific delivery of a software project. Generally, projects face limited resources such as short timelines, small budgets, restricted human power, and limited technology. It becomes necessary that stakeholders prioritize the requirements to implement first. Requirements prioritization helps the project developers to select the final requirements within their resource constraints.

Requirement Management

It could be more expensive to fix delivered defects than those captured earlier in the lifecycle, and pitiable requirements are mainly responsible for delivered defects. Therefore an effective requirements management should be at the top priority in the requirement phase. The goal of requirements management within an organization is to provide consistency of the activities. Security requirement analysis controls the costs, prioritize requirements, and standardize requirement analyses methods. It is easy to understand where the problems start. Many organizations still use text-based documents to inform their elicitation and requirements review and do so outside of a change management control or workflow system.Effective requirements management is built on key pillars i.e., through visualization**,** Collaboration, Change management, and traceability. Traceability of security requirements is the amount of information about requirements

relationships that is maintained.A viewpoint is a process of structuring the requirements to represent the perspectives of different stakeholders. [6]Requirement change management is a significant activity to produce an accurate and consistent software product. It identifies the rationale of the changes in the requirements specificationand responsible parties for the change. It Trackthe change history in the requirements specification and applying impact analysis on the effect of the change to communicate the change among team members and reporting changes in the requirements specification. [7]

Requirements specification is the process of recording the requirements in one or more forms, including natural language and formal, symbolic, or graphical representation. [8] Requirement validation is the process of confirming with the customer or end user of the software that the specified requirements are valid, correct, and complete.[9]

IV. CONCLUSION

In this research, we have focused security requirement and avoidance of anti-requirements. Security requirement engineering is a crucial activity in the development of secure systems. It is also recognized as a crucial activity by the RE community and new methodologies are proposed for handling security aspects. In this paper, we propose a framework that incorporates security requirement and technique. It improves the security requirement engineering activity at the earliest stages of development.

****

V.REFFERENCES

1. Dhirendra Pandey, UgrasenSuman& A. K. Ramani, "Security Requirement Engineering Issues In Risk Management", *International Journal Of Computer Applications, Foundation Of Computer Science*, USA, ISBN: 978-93-80747-89-4, Vol. 17, No. 5, Pp.11-14, 2011.
2. Roger S. Pressman (Fifth Edition), Software Engineering-A Practitioner's Approach, McGraw Hill,p.20- 24.
3. Dhirendra Pandey, "International Journal of Computational Intelligence And Information Security", *IJCIIS*, Australia, Vol. 1 No. 8, Issn: 1837-7823.
4. Donald G. Firesmith, (2003) "Engineering Security Requirements", Journal of object technology, vol 2, no.1, pp.53-68.
5. Dhirendra Pandey, UgrasenSuman and A. K. Ramani, "Security Requirement Engineering Framework for Developing Secure Software*", International Journal of Computational Intelligence and Information Security*, *IJCIIS* Australia, Vol. 1 No. 8, Issn: 1837-7823, Pp.55-65, 2010.
6. Agarwal A, Gupta D, (2008) "Security Requirement Elicitation Using View Points for online
7. System", *IEEE Computer Society*.
8. Kotonya G. and Sommerville I.: Requirements Engineering: Processes and Techniques. John Wiley & Sons, 1998.
9. Alexander I.: Misuse Cases Help to Elicit Non- Functional Requirements, Position paper for Policy Workshop 1999, Bristol, U.K., and November 1999