Evaluation of Security Requirements Elicitation Techniques

Submitted by:

Surayya Siddiqui
(141-FAS-/MSSE/F06)

Supervised by:

Dr. Naveed Ikram

Department of Computer Science/Software Engineering
Faculty of Basic and Applied Sciences
International Islamic University Islamabad
2012

MS
301.15
SUE

psychological tests.

Social psychology.

(1)

(2)

International Islamic University, Islamabad

Faculty of Basic & Applied Sciences

Department of Computer Science/Software Engineering

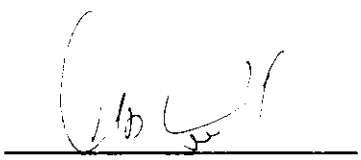
Dated:

FINAL APPROVAL

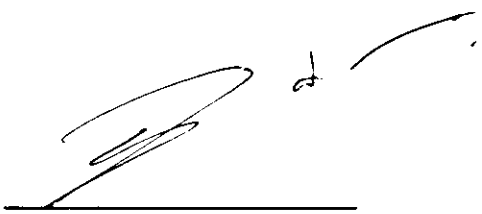
It is certified that we have read the thesis, entitled **"Evaluation of Security Requirements Elicitation Techniques"**, submitted by Surayya Siddiqui Reg. No. 141-FBAS/MSSE/F06 .It is our judgment that this thesis is of sufficient standard to warrant its acceptance by the International Islamic University Islamabad for MS Degree in Software Engineering.

PROJECT EVALUATION COMMITTEE

External Examiner:
Dr. Arshad Ali Shahid
Professor and Head,
Department of computer science,
National University of Computer & Emerging Sciences,
Islamabad



Internal Examiner:
Ms Salma Imtiaz
Assistant Professor,
DCS&SE, FBAS
International Islamic University Islamabad



Supervisor:
Dr. Naveed Ikram
Associate Professor, Faculty of Computing
Riphah International University
I-14, Islamabad

Declaration

I hereby proclaim that the completion of the thesis "Evaluation of Security Requirement Elicitation Techniques" is entirely my own effort under the earnest guidance and supervision of my respected supervisors. I further affirm that if any part this work proves to be plagiarized I shall be held responsible. Therefore, I firmly declare that no part of this presented work has been submitted earlier in support of any other degree, in this or any other university.

Surayya Siddiqui

141-FBAS/MSSE/F06

Acknowledgement

I am truly pleased for the completion of this wok and earnestly praise God Almighty, Who gave me the courage by conferring his blessings upon me to carry out this work.

I am greatly thankful to Dr. Naveed Ikram who has supervised this research work. I am indeed appreciative for his guidance and assistance which really encouraged me to proceed and overcome the difficulties in the completion of my research degree.

I am greatly thankful to the faculty of Basic & Applied Sciences (MS in Computer Science and Software Engineering), Islamic International University Islamabad, who provided me the required facilities and opportunities for the completion of this research..

Despite my sincere efforts, however, all the flaws and shortcomings are my own.

Surayya Siddiqui

Abstract

It is well recognized by the software industry that security requirements must be elicited at Requirement Engineering level. There are numbers of studies presented in literature to discuss security requirement elicitation techniques at RE stage. Similarly there are also numbers of studies that have comparatively evaluated these techniques but still there are no guidelines available for software community regarding selection of security requirement elicitation techniques in terms of situational characteristics. Current research work specifically focuses on this topic. It discusses underline theme of different security requirement elicitation techniques, reviews the literature that has explored these techniques comparatively and highlights their scope and limitations. It also sets limits of the work by selecting two techniques – MUC & IBIS and evaluates them in three types of situational characteristics on the basis of predefined criteria. Finally it presents guidelines regarding selection of these two techniques in three given situations to direct the software industry

Table of Contents

List of Tables:

CHAPTER 1: INTROUCTION

CHAPTER 1: INTROUCTION

Security threats and vulnerabilities have accelerated constantly during the last 10 years. Awareness of security requirements and related elicitation techniques at Requirement Engineering (RE) level is also tremendously growing since the last decade. This research work highlights the need of considering security requirements at RE level and identifies the disparities in this area of study. It is highlighted that there are number of techniques available in software industry for elicitation of security requirements at RE level but software industry facing difficulties in selection of security requirement elicitation techniques in different situations (Andreas & Guttorm, 2008). Besides, no guidelines regarding selection of these techniques for different situations are available in literature (Mamadou et al, 2004; Nancy et al, 2006; Daniel et al, 2006; Johan et al, 2007; Anders et al, 2007; Andreas and Guttorm, 2008; Inger et al, 2008; Benjamin et al, 2009; Umair & Zulkernine, 2009). There is a need to comparatively evaluate such techniques in context of different situational characteristics. This will lead to develop a consensus among software experts about which technique is more effective than other in different situation and help the less experienced security analysts in selection of the appropriate security requirements elicitation techniques for their specific project situation.

1.1. Security

Security is a quality factor, deals with protection of information system resources including hardware, software, data, communication network and people (Donald, 2003a). Security attributes are generally defined as confidentiality, integrity, availability and accountability (Charles et al, 2006). Security of information system is increasingly becoming critical in this era of information technology, where world has been turned into global village (Rudolph, 2007). Technology oriented development have influenced every area of human life like business, economy, medical, defense, space research etc. As people increasingly rely more on

use of information system, securing the resources of information system is becoming more important. Ignorance to security properties in software projects during system development life cycle (SDLC) may produce a vulnerable system that is easy target of attackers (NIST, 1995; Kenneth & Gary, 2005; Michael & Steve, 2006; Jose et al 2008). Moreover loss of security may results improper modification of system resources, unauthorized disclosure of personal information, denial of service or data, loss of repute, money (Guttorm & Andreas, 2000) and even loss of human life in a mission critical system (Donald, 2003a).

1.2. Security Requirements

Security requirements are defined as quality requirements (Donald, 2003a). Several authoritative studies are available regarding definitions of security requirements e.g. (Charles et al, 2004; Charles et al. 2004; Donald, 2003a; Nancy et al, 2005; Jonathan et al, 2004; NIST, 1995) where security requirements have commonly been discussed as protection of information system. Main focus of security requirements discusses "what must not happen" (Jonathan et al, 2004). A study (Donald, 2003b) highlighted that "security requirements are driven by security threats" and demands detailed risk assessment of project domain. The author of study (Donald, 2003b) contributed by defining attributes of security requirements as identification, authentication, authorization, immunity, integrity, intrusion detection, non repudiation, privacy, auditing, survivability, physical protection and system maintenance.

It is also well recognized that security requirements are negative requirements and need to be properly elicited and specified at RE level to assure that security requirements have been discussed and agreed explicitly (Rudolph, 2007; Firesmith, 2003a; Jonathan et al, 2004; Inger et al, 2008; Jose et al, 2008; Umair & Zulkernine, 2009). In fact elicitation of security requirements captures the protection of entire spectrum of information technology (NIST, 1995) with the concern of "what should not happen in the system" (Guttorm & Andreas, 2000).

1.3. Security Requirement Elicitation

Major focus of security requirement elicitation is identification of complete set of security requirements to define the scope of project and eliminate chances of the security violations in future (Donald, 2003a). It is a feature of system level application which is discussed by considering the factors of software operating environment, hardware environment and human cultural environment (Jonathan et al, 2004). It is a risk oriented approach (Donald,2003b), performed at various stages of system development life cycle (NIST, 1995), requires variety of artifacts from both RE and SRE communities (Nancy et al, 2005; Jonathan et al, 2004) and demands contribution from requirement engineer, security analyst, architect, designer, developer and customer stakeholders (Charles et al, 2006; NIST, 1995). Moreover it is an incremental, iterative and dynamic approach where security requirements are developed and updated as SDLC proceeds from initiation to dispose, (NIST, 1995; Axel, 2004). It is also highly recommended to elicit security issues at RE level because it serves as basis for system development life cycle (Charles et al, 2004; Axel, 2004; Lin, Eric and John, 2002; Seda et al, 2005). It plays role for developing design solutions and in trade off analysis of different design options as well (Ian, 2002b). Similarly security oriented requirement elicitation is used as a basis for security oriented testing (Meledath, 2006). Moreover, Security requirement elicitation has been used with different names in software industry as elaborating security requirement (Axel, 2004), deriving security requirements (Charles et al , 2004), analyzing security requirements (Lin, Eric and John, 2002), specifying security requirement (Mamadou et al, 2004) and elicitation of security requirements (Nancy, 2006a; Simara et al, 2005; Guttorm &Andreas, 2004). We will use the term security requirement elicitation throughout this literature.

1.4. Problem Domain

"Caring of security at RE time is a message that has finally received some attention recently" (Axel, 2004).Security requirement elicitation should be an integrated part of RE (Nancy et al, 2005; Donald, 2004a; Jonathan et al, 2004; Mamadou et al, 2004; Jose et al, 2008; Benjamin et al 2009). A handbook published by NIST in 1995 mentions that security should be considered at each stage of SDLC starting from RE to dispose. But instead of addressing security requirements at RE level, a common problem faced by software development industry is considering security in context of security policies or architectural mechanisms (Inger et al, 2008; Umair & Zulkernine, 2009). There are also number of techniques available in literature like Misuse Cases (Guttorm & Andreas 2000; Guttorm & Andreas, 2004), Security Requirements as Relationships among Strategic Actors (Lin, Eric and John, 2002), Elaborating Security Requirements by Construction of Intentional Anti models (Axel, 2004), Deriving Security Requirements from Crosscutting Threat Descriptions (Charles et al, 2004), Confidentiality Requirements Elicitation and Engineering - CREE (Seda et al, 2005), Requirement Elicitation Based on Goals with Security and Privacy Policies in Electronic Commerce (Annie, 2000; Simara et al, 2005) with the explicit focus of security requirement elicitation at RE level but there is a myth exists that "security area do not have techniques or templates for requirement elicitation" (Nancy et al, 2005). It is also revealed that requirement engineers are not aware about the domain of security requirements so they are not able to perform security requirement elicitation as early stage of RE level (Donald, 2003a; Jose et al, 2008). In addition, security requirements are more often treated as implicit requirements where they should be discussed explicitly (Rudolph, 2007). Moreover, (Rudolph, 2007) also indicates that there is "the lack of awareness and knowledge of the people writing the requirements" where author means security requirements.

Besides, the review of literature regarding comparative research of security requirements elicitation also indicate that different security requirement elicitation techniques have been compared by different researchers but no objective comparison of security requirements elicitation techniques regarding selection of these techniques in different situational characteristics is performed before (Nancy et al, 2006; Mamadou et al 2004; Johan et al 2007; Daniel et al, 2006; Anders et al, 2007; Andreas & Guttorm, 2008; Inger et al, 2008; Jose et al, 2008; Benjamin et al, 2009; Umair & Zulkernine, 2009). (Andreas & Guttorm, 2008) points out the need of comparing these techniques in different situational circumstances. But we found that all these mentioned studies have compared security requirement techniques in terms of "technique characteristics" not as comparative evaluation of security requirements elicitation techniques in situational characteristics except (Andreas & Guttorm, 2008) that has discussed this issue explicitly.

So it is difficult for software industry to appreciate the strengths and counter the weaknesses of security requirements elicitation techniques in terms of a given situation especially at RE level. In this scenario the industry demands a comprehensive study on security requirements elicitation techniques that will help to outline the philosophy of different security requirement elicitation techniques and also help to make decision in selection of which technique is more productive in particular situation. In this context the main research question of our work is:

- Which technique performs better in terms of effectiveness and coverage in different situations, MUC or IBIS?

Along this, we have also reviewed the literature that compares security requirement elicitation techniques and highlights scope and limitation of respected studies. In the light of identified limitations, described in chapter 2, we make an effort to contribute regarding situation based selection of security requirements elicitation techniques.

1.5. Research Scope

Though, we are interested to investigate the available security requirement elicitation techniques in literature with the focus of RE level and their evaluation in different situational characteristic, we selected only two of them named: Misuse case (MUC) and Issue Based Information System (IBIS) to compare in three situational characteristics (Low, Medium and High level of detail). Rationale for considering these two techniques is provided in chapter three sections (3.3 and 3.3.1). While Identification of three situational characteristics as low, medium and high level of detail is also presented in chapter three under heading of selection of situational characteristics (section 3.4) and details of these characteristics can be found in appendix B, C, D for low medium and high level of details respectively.

We admit that scope of our work is limited in terms of number of security requirements elicitation techniques and situational characteristics. We feel that investigation of security requirement elicitation techniques and evaluation of their practical application in different situation demands more comparison of more techniques with more situations or same techniques in some other situations.

1.6. Research Contribution

Primary contribution of this research work is development of guideline for both software community and security community about the selection of security requirements elicitation techniques in terms of different situational characteristics. By providing such guidelines, we are assisting analysts of both communities to understand security requirements elicitation techniques at RE level and to easily decide which technique is best suited in given situations. At the same time, it will also assist them to consider security requirements from the beginning of the project. As ignorance of security requirements at RE level produce a vulnerable design solution and ultimately a poor quality system (Nancy et al, 2005). This will also lead to increase the cost of the project because return on investment raises from 12 to 21

percent if security requirements are considered at RE level instead of design level (Soo Hoo et al 2001).

Moreover it will also contribute to the notion of (Andreas & Guttorm, 2008) by moving one step further regarding selection of security requirement elicitation techniques in situational characteristics at RE level. (Andreas &Guttorm, 2008) opens a new area of research by highlighting the need of security requirements elicitation techniques selection in different situations. Availability and detail level of artifacts at RE level sets different situations (Gary et al, 2002; Seda et al, 2005; Guttorm &Andreas 2000; Guttorm & Andreas, 2004; Charles et al, 2004b; Nancy et al, 2005; Lin, Eric and John, 2002; Annie, 2000; Simara et al, 2005; Donald, 2003a ; Axel, 2007; Axel, 2004 ;Nancy et al, 2004. So we identified important situational factors as low, medium and high level of project detail. Our work will be a source of motivation for other researchers to identify such characteristics and provide conceptual framework to investigate security techniques in different situations and development of guideline for future analyst for selection of security requirement elicitation techniques in different situations.

1.7. Research Method

We identified security as an important research area of software engineering community from literature (Betty & Joanne, 2007) and perform a literature survey in this subject. Survey revealed the need of considering security requirements during RE and situation based evaluation of security requirement elicitation techniques regarding selection of these techniques in different situations (Andreas & Guttorm, 2008).We also search for literature where security requirement elicitation techniques have been discussed comparatively.

A survey of available security requirement elicitation techniques was performed to identify techniques that have been proposed in literature as security requirement elicitation techniques and also have working support at RE level. These techniques were theoretically evaluated on

the basis of evaluation criteria introduced in (Axel, 2004) as important parameter for evaluation of security requirements elicitation techniques. After rating, two techniques MUC and IBIS were selected for further investigation. The parameters of situational characteristics were also identified from literature survey as situation of low level of detail, medium level of detail, high level of detail.

An experimental approach has been decided to compare the both techniques for research validation. Dependent variables were identified as effectiveness of techniques (number of security goals identified by each technique in given situation) and coverage of techniques (number of types of security goals identified by each technique in given situation and learning, executing & result interpretation time consumed by each technique in given situation). Hypothesis statements were developed and as the nature of the research work contains comparison of two techniques in three different situations so a comparative experimental method named – repeated measure design was selected and executed for research validation. It was performed with randomization and counterbalancing approach to control external and internal validity of the experiments. Finally the statistical results and hypothesis testing is presented in chapter 5 and summary findings and selection guidelines about MUC and IBIS are also provided in chapter 5, whereas chapter 6 provides conclusion and future directions.

1.8. Thesis Outline

Thesis out line follows: Chapter 2 provides review of literature that has been done by industry for comparative evaluation of security requirements elicitation context. It also high lights the limitations and gaps of respected studies. Chapter 3 lists the significant security requirement elicitation techniques used at RE level, describe them briefly, explain the important evaluation parameter & theoretically evaluate the identified techniques and selection of two techniques – MUC & IBIS for further evaluation. Besides this chapter 3 also

describes list of situational characteristics and provide rationale for their selection. Chapter 4 presents experimental design by describing dependent variables, hypothesis statements, research design & procedure and validity issues. Chapter 5 illustrates results of experiment on the basis of graphical patterns (bar graphs) and statistical findings leading to guidelines for future analysts about situation based selection of security requirement elicitation technique. Finally conclusion is provided in chapter 6 to discuss the paper contributions for industrial practitioners and future researchers.

CHAPTER 2: LITERATURE SURVEY

CHAPTER 2: LITERATURE SURVEY

There are number of studies available in literature that have identified the need of comparative evaluation of security requirement elicitation techniques (Mamadou et al, 2004; Nancy et al, 2006; Tor& Guttorm, 2007; Jose et al, 2008; Andreas & Guttorm, 2008). It is also noted that there is shortage of studies where security requirement elicitation techniques have been discussed specifically. However there are studies available where security engineering processes or security requirement engineering processes are subject of evaluation (Johan et al, 2007; Inger et al, 2008; Benjamin et al, 2009; Umair & Zulkernine, 2009).

Following section provides overview of such studies where security requirement elicitation techniques have been discussed in term of evaluation or comparison. It also highlights the focus of these comparative studies by identifying the techniques that have been evaluated or compared and criteria that have been used for this comparison and evaluation. Besides, we tried to identify the scope and limitations of such studies in order to contribute in the area of study by providing guidelines for selection of security requirement elicitation techniques in different situational characteristics.

2.1. Review of Comparative Evaluation of Security Requirement Elicitation Techniques

2.1.1. Evaluation Factors for Comparison of Security Requirement Elicitation Techniques Discussed by (Mamadou et al, 2004).

A comparative evaluation of three security specific requirement elicitation technique is presented in (Mamadou et al, 2004). The authors recognize the need of considering security requirements elicitation at early stages of RE and selected Common Criteria, Misuse Case & Attack Tree for "critical analysis and comparison" from security domain. They used all three techniques on same case study - wireless hotspot and evaluated the techniques against predefined criteria defined as learn ability, usability, completeness, clarity of output and analyzability.

The purpose of the literature (Mamadou et al, 2004) was comparison of security specific requirement elicitation techniques. But on final note we do not find which technique is better than others in order to provide guidance for future analyst. There are no findings about selection of security requirement elicitation techniques from this comparison but a suggestion to use all of them as combine methodology.

It is also noted that comparison was based on the characteristics of the techniques like clarity of output, usability etc. Authors did not add any situational attribute for evaluation to direct the readers about which technique is useful in which situation.

Finally, the literature (Mamadou et al, 2004) concluded that each technique performed well in security context with its specific strengths and weaknesses. It also recommends combined use of technique can improve efficiency of these methods. But does not provide any mean to combine all these technique to be more effective.

2.1.2. Evaluation Model for Assessing the Performance of Security Requirement Elicitation Techniques by (Nancy et al, 2006)

A comparative study under supervision of Nancy R Mead (Nancy et al, 2006) was conducted in context of SQUARE evaluation. At First, nine requirement elicitation techniques (Soft System Methodology (SSM), Quality Function Deployment (QFD), (Controlled Requirement Expression(CORE), Issue Based Information System (IBIS), Joint Application Development (JAD),Featured Oriented Domain Analysis (FODA), Critical Discourse Analysis (CDA), Accelerated Requirement Method (ARM)), Misuse Case were selected from literature and subjectively rated against predefined evaluation criteria. The attributes of criteria were identified as adaptability, case tool, client acceptance, complexity, graphical output, implementation duration, learning curve, maturity and scalability. Secondly, on the basis of this evaluation IBIS, JAD and ARM were selected for further comparison in context of security requirement elicitation. Case study based approach was used for research validation

and all the three techniques were applied to three different case studies. After performing case studies ARM, JAD and IBIS were also evaluated against a technique characteristics based criteria. As the technique evaluation was in context of security requirements, but the characteristics of criteria do not have particular focus on security relevant issues. Besides, critical analysis of the report (Nancy et al, 2006) shows that although the domain of the research was security requirement elicitation but all the selected nine methods were from domain of functional requirement elicitation except misuse cases. They were not designed or introduced in literature as security requirement elicitation methods and hence cannot be considered a good sample in security relevant issues.

Moreover on the basis of this subjective rating, they selected IBIS, ARM and JAD to apply on 3 different case studies. IBIS and JAD are high scorer on the table but ARM, Misuse Case and SSM got tie there is no justification that why ARM is selected for further investigation while Misuse case seem good candidate in terms of security requirement elicitation (Guttorm & Andreas, 2004; Mamadou et al, 2004; Jose et al, 2008). Comparison of techniques from both domains may also present more valuable results as (Donald, 2003a; Charles et al, 2006) indicate that security requirement elicitation at RE level demands combine effort from both domains.

In addition, review of evaluation criteria also shows that it is based purely on characteristics of elicitation methods e.g. adaptability, graphical output. It did not consider any situational characteristics to investigate the performance of selected techniques in different situations. Finally, the conclusion of the report that ARM is better than JAD or IBIS has some points to be raised.

Authors admitted that execution of JAD by team members was not fully performed and starting steps of JAD were omitted by them (Nancy et al, 2006). So how can they claim that

JAD did not perform well in security requirement elicitation when all the procedure of the technique was not even followed?

Moreover, it is also accepted by the authors that results may be biased as ARM method was performed by security experts who had knowledge about security domain & requirements as compare to other two teams of IBIS and JAD methodology who were not security experts (Nancy et al, 2006). Moreover authors of the report recognized the abilities of IBIS as "that the interview generated discussion between stakeholders and raised security issues that otherwise would not have been addressed" (Nancy et al, 2006) but did not recommend it for future because clients of the case study had difficulties in understanding of IBIS map structure. It seems that the main problem with the IBIS was understanding and execution of technique not with the technique itself. The team may be failed to convey the essence of technique to the client.

2.1.3. Technique Characteristics Based Evaluation Model for Security Requirement Elicitation at Various Stages of SDLC by (Daniel et al, 2006).

(Daniel et al, 2006) presents a theoretical comparison of eight security requirements elicitation techniques against a predefined evaluation criterion. Authors highlighted the common software industry problem of considering security as design level approach and strongly acknowledge the idea of eliciting security requirement at functional requirement elicitation level. In addition they also call attention to the fact that security issues should be taken in to account throughout all phases of system development lifecycle from inception to dispose (Daniel et al, 2006).

(Daniel et al, 2006) contributes to the software community by highlighting the need of security requirement elicitation at RE level instead of taking it as design or development level approach. Authors (Daniel et al, 2006) are interested in comparison of security requirement engineering processes but not only at RE level. Selected techniques are not specific to only

security requirement elicitation at RE level rather address security issues to all phases of SDLC. So the focus is comparison of security requirement engineering processes to the whole software development while scope of our work will be specific to only elicitation of security requirement at RE level.

Analysis of (Daniel et al, 2006) discovers that components of the evaluations criteria are also based on the technique characteristics e.g. degree of agility, help support, degree of integration with other software requirements, user friendliness, contribution of the proposals as regard security. Comparative evaluation does not contribute to community about selection of requirement elicitation technique in terms of situational factors as we will discuss these elements in our research work.

On final note, (Daniel et al, 2006) concludes that "it must be said that these approaches are not specific enough for a treatment of IS security requirements in the first stages of the IS development process" so there is no guidance for software industry to apply them at RE level as paper suggest none of them is being supportive at RE level.

2.1.4. Technique Activity Based Evaluation Factors for Security Engineering Process by (Johan et al 2007).

The article (Johan et al 2007) compares two secure software engineering processes – Comprehensive, Lightweight, Application Security Process (CLASP) and Microsoft's Security Development Lifecycle (SDL). The authors have highlighted that security engineering process should be considered and applied to the whole software development life cycle in order to provide trustworthy system. Theoretical evaluation was opted for research validation and techniques were selected for comparison as they both are introduced in literature as security engineering processes and explicitly focus on security relevant activities of SDLC (Johan et al 2007).

Authors have reviewed available material about both processes and developed a list of general characteristics and activities of each process. Activities are then organized into different phases of software development lifecycle e.g. education and awareness, project inspection, analysis, design, implementation, testing and verification, deployment. Then both processes are compared on the basis of technique activity base comparison. In general this comparison guides the community as checklist. For instance what activities are performed by each process at each phase of system development life cycle? What activities are common and what are different in each process?

Overall, (Johan et al 2007) presents theoretical evaluation of two security engineering processes. They did not support their findings through any empirical or experimental validation. Major focus of the article was to identify strengths and weaknesses of both processes in term of their general characteristics and activities performed by each of them in system development life cycle. No guidelines are available about strengths and weaknesses of these two processes in different situational characteristics.

It is discovered that presented comparison is of two secure software engineering processes with the focus of mapping security engineering cycle to the whole software development life cycle. It is not specific about security requirement elicitation techniques at RE level.

Moreover, comparative analysis of both processes on different phases of SDLC does not discuss security requirement elicitation specifically. There is no information found – how do both processes realize elicitation of security requirements? Which aspects of security elicitation they cover? How both processes differed in security requirement elicitation at early phase of software development life cycle? Instead report describes that "SDL seems to have no activities that are specific to the analysis phase" (Johan et al 2007). This makes readers confuse about when SDL elicit security requirements?

It is also described that CLASP recognized the need of elicitation of security requirement at early stage of SDLC to drive the security oriented design, implementation & testing and maintenance activities of project (Johan et al 2007). But does not describe what these activities are and what issues to be considered in context of security requirement elicitation at RE level.

2.1.5. Factors of Comparative Evaluation Model for Comparing Non Functional Requirement Elicitation Methods by (Andrea et al, 2007).

(Andrea et al, 2007) provides a comparative study of two requirement elicitation techniques named IESE – NFR and Misuse Oriented Quality Requirement Engineering (MOQARE), Authors selected both techniques form literature review in context of requirement elicitation and analysis of Non Functional Requirements (NFR). Both techniques were applied to a case study – wireless network system. IESE – NFR was used to identify efficiency, reliability and maintainability quality attributes while MOQARE was applied to identify security, interoperability, reliability, usability, maintainability, probability and efficiency.

Though authors applied both techniques to identify quality requirements but the comparison was of two NFR techniques, there is no explicit discussion of security requirement elicitation specific techniques. The evaluation criteria used was also about the characteristics of the techniques and defined as guided process, measureable NFR, Reuse of artifacts, intuitive and creative elicitation, focus effort and NFR prioritization, dependencies, integration of NFR with FR. It does not include any situational aspect for evaluation.

It is also discovered that authors explore the IESE – NFR for efficiency, reliability and maintainability attributes while the MOQARE was investigated for security requirements but at the end no security relevant comparison found because former technique was not explored for security relevant quality attributes.

Moreover, the objective of the (Anders et al, 2007) was not comparison of techniques in order to identify which one is better than others but to explore the characteristics of the techniques in terms of understanding how do they work to identify (NFR) at RE level and look at the possibilities to improve the technique by combining their strengths and excluding their weaknesses in terms of defined evaluation criteria. So the readers may not be able to interpret the results in terms of NFR technique selection in different situational characteristics. Besides, purpose was not developing guidelines for NFR techniques selection rather authors were interested to improve the described techniques.

2.1.6. Misuse Case Based Analysis Factors for Evaluation by (Tor & Guttorm, 2008).

(Tor & Guttorm, 2008) presents an experimental research work where misuse case text description and misuse case diagrams are comparatively evaluated to guide the software industry regarding which approach performs better than others. Nature of the compared approaches is security requirement elicitation and other security requirement engineering phases are out of scope of this research work. It does not add any situational aspect to compare the performance of both approaches and main contribution of the work is comparison to find advantages and disadvantages of text based description and diagram based notation of misuse cases to investigate which one is better than other. Performance of the misuse case text and diagram based approaches were measured by the number of failure mode (any event that could threaten to any actor's mode) and perception based evaluation criteria based on perceived ease of use, usefulness and intention to use.

Our work will contribute to (Tor & Guttorm, 2008) as instead of focusing on only two different faces of misuse cases we will discuss performance of diagram notations of misuse cases and IBIS in context of situational scenario and will contribute regarding selection of these two techniques in different situations.

2.1.7. Evaluation Factors for Situation Based Selection of Security Requirement Elicitation Techniques identified by (Andreas & Guttorm, 2008).

Another experimental comparison of two security specific requirement elicitation technique is conducted by (Andreas & Guttorm, 2008). It is a major contributor to software community in order to selection of security requirement elicitation especially at RE level. The names of the selected techniques are Misuse Cases and Attack Trees and experimental research approach has been used by authors to validate their proposal.

The authors point out the fact of growing need of security in software industry and rare empirical or experimental literature about security specific requirement elicitation technique. They compared above mentioned techniques in a pair of control experiment.

The evaluation criteria used for comparative evaluation was number and types of threats identified by each technique. While the performances of both techniques were measured in two experiments where authors defined situations as only use case description was provided in first experiment while in second experiment both use case description and use case diagram were provided. They also collected sample perception about the technique through questionnaire to match their performance and perception of the both technique. Finally they suggested Attack Trees to be used in future for requirement elicitation as it was better in both experiments.

Overall, the (Andreas &Guttorm, 2008) opens a new research era in requirement elicitation of software development industry by explicitly focusing on security requirement elicitation. It recognizes that software industry must consider security at RE level and there should be guidance about selection of security requirements elicitation techniques. For this purpose it presents evaluation of two security specific requirement elicitation techniques. It uses experimental approach to provide grounds for research results. It compares both techniques

on the basis of technique characteristics – number and types of threats identified by each technique

Threat identification is undoubtedly major building step of security requirement elicitation as (Donald, 2003b) mentions that security requirement elicitation is a threat oriented approach. Besides, (Andreas & Guttorm, 2008) elaborates situations on the bases of two factors defined as use case description and use case diagrams plus use case description.

Our work will contribute to (Andreas & Guttorm, 2008) by moving one step further and will compare two elicitation techniques on the basis of number and variety of security goal identification by each technique. It will discuss abilities of two techniques in analysis of security goal elicitation.

Moreover our work will also consider the time dimension as outcome variable to guide the software industry about time consumption of each technique in different situations. Time plays definite role in success or failure of software project. Most of the time security requirements are ignored at RE level because of time shortage. So there is need of guideline about security requirement elicitation technique in terms of time consumption. E.g. which technique takes more time to be executed?

Besides, (Andreas & Guttorm, 2008) elaborate situations on the bases of two factors defined as use case description and use case diagrams plus use case description. Our research specifically considers this issue by identifying three situational characteristics described in chapter 3 (section 3.3) and investigating performance of both techniques in these situational characteristics.

2.1.8. Security Attribute specific Evaluation Model for Different Phases of Requirement Engineering by (Jose et al, 2008).

(Jose et al, 2008) reports comparative survey of twelve security requirement engineering processes. The authors point out the common software industry problem of considering

security issues at later stages of SDLC and not taking it as RE level approach. They also high light the fact that there is lack of awareness in software community regarding existing security requirements engineering processes and a need to explore such processes comparatively in order to acknowledge their strengths and weaknesses. The research work specifically focuses on survey of security requirement engineering processes. The surveyed processes are Common Criteria, SQUARE, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Attack Trees, Usage-centric Security Requirements Engineering (USeR), CLASP, Misuse Cases, Abuser Stories, Secure TROPOS , i* agent based requirements for security, Security Problem Frames and Anti-Models (Jose et al, 2008). Similar to (Benjamin et al, 2009), selection of processes as security requirement engineering has points to be raised. For instance (Jose et al, 2008) discussed Misuse Cases & SQUARE both under category of security requirement engineering processes. However the discussion about the differentiation between Misuse Cases and SQUARE or among other surveyed processes in terms of scope or classification is out of scope of our research work. Authors of report divided security requirements engineering process into five phases and named them as security elicitation, analysis, specification, management and support to later stages of design and testing.

Evaluation criteria for each phase of security requirement engineering process were established to measure the performance level of each process to each phase. The contents of evaluation criteria based on certain security specific activities of each phase identified through literature review of researchers. Though the constituent factors of evaluation criteria do not include any situational aspects to measure the performance of surveyed processed in different situations, even than (Jose et al, 2008) contributes to security oriented software industry by discussing security specific requirement engineering processes in terms of security specific activity based comparison. It also discussed security requirement elicitation

phase explicitly. There is evaluation criteria specifically established for elicitation phase of security requirement engineering process. It explores the processes for their support to elicitation of security requirements phase and measure the scale of support as well. Besides, it also high lights how each process elicit security requirement by describing types of techniques used/ recommended by the process. Additional aspects of evaluation criteria relevant to security requirement elicitation phase are degree of stakeholder identification provided including customer/developer/end user, level of involvement of the customer, elicitation of other the other types of the requirements besides security, dynamics of the elicitation process (iteration of requirement elicitation or not) and support for establishing system boundaries (what are inside/outside boundaries of system being developed).

Finally, along the recommendations for each phase of security requirement engineering process and over all suggestion regarding performance of surveyed processes, (Jose et al, 2008) concludes misuse cases, Octave and User as high scorer in elicitation phase. Over all the survey report contribute to software industry by discussing security requirement engineering processes and also provide guidance regarding elicitation of security requirement phase specifically.

2.1.9. Security Oriented Activities Based Evaluation Model by (Inger et al, 2008).

A comparative study (Inger et al, 2008) performed a theoretical comparison of security requirement engineering processes. The selected processes were security requirement engineering methods e.g. SQUARE (Nancy et al, 2005), Security Requirement Engineering Framework (Charles et al,2006), XP Oriented Approach to Security Requirement Engineering (Gustav et al, 2006), CLASP (OWASP, 2006), Microsoft SDL (Michael & Steve, 2006) Secure Software Development process by (Axelle & Makan , 2005), (Kenneth &Gary, 2005) and (Gunner, 2004) and a Methodology for Secure Software design by (Eduardo, 2004), and do not discuss security requirement elicitation specifically. The

contents of evaluation criteria were characterized as definition, objectives, Misuse/ threat, asset, coding standard, categorize & prioritize, inspect and validate and process planning.

It is revealed that comparison of security requirement elicitation techniques is not the subject of the work but the introduction of a new technique for security requirement engineering that is easy to use and provide stepwise guidance to its users to be executed. Moreover, evaluation criteria contains security relevant activities performed at RE level e.g. definition, misuse/ threat etc and does not include any situational characteristics. Furthermore, the comparison may be used as guideline in selection of a particular security requirement engineering process whether it support certain activities or not but provides not guidance about selection of security requirement elicitation techniques.

2.1.10. Security Specific Attribute Based Evaluation Model by (Benjamin et al, 2009)

(Benjamin et al, 2009) highlighted the importance of security requirements and need to must consider them before design as well. Authors performed a comprehensive literature review of security related concepts and security requirements elicitation and engineering processes. They categorized security requirement engineering processes in multilateral approaches, UML based approaches, goal oriented approaches, problem frame based approaches, risk analysis based approaches and common criteria based approaches. Major focus of the paper was introduction of a Conceptual Framework (CF) in order to explicitly high light the context of security and relevant security properties that security requirement engineering methods should have or whether they have it or not. The contents of CF based on security relevant activities like security goals & security requirements identification, security specification, stakeholder's view, domain knowledge, asset, threat, vulnerability and risk analysis. On the basis of CF authors evaluated other security requirements engineering methods to evaluate whether they have such properties or not.

Using the CF, evaluation of security requirement engineering methods provides understanding of such methods that what security relevant properties they have? How do they work? What aspects they do consider in order to elicit security requirements and drive the security requirement elicitation process. The study also covers a wide range of methods for evaluation but considers conceptual properties of these methods and does not add any situational perspective to compare the effectiveness of such methods. Besides, selection of methods for comparison is also questionable. For instance SQUARE and misuse case may not be directly comparable as SQAURE is a security requirement engineering process and scope of the process capture nine comprehensive set of activities while misuse case is an individual technique that can be used as a tool to elicit security requirements as part of SQUARE.

2.1.11. Evaluation Models for Security Development Lifecycles, Security Specification languages and Security Requirement Engineering Processes discussed by (Umair & Zulkernine, 2009).

Another recent literature (Umair & Zulkernine, 2009) also discussed comparative evaluation of security related processes. Major focus of the paper is considering security throughout SDLC. It compares security software development life cycles on the basis of their activities. Furthermore it also performed technique characteristics based comparison of security specification languages and activities wise comparison of security requirement engineering processes such as security Requirement Engineering Framework by (Charles et al, 2006), Secure Tropos, SQUARE, CLASP, SREP (Umair & Zulkernine, 2009). Authors emphasis on security of whole system development life cycle. Besides, they also highlighted the need of comparing and selecting security requirement engineering process and are not interested in evaluation of security requirements elicitation techniques and selection of such techniques in different situational characteristics.

2.2. Overall Synthesis

Analysis of literature review reveals that there is shortage of comparative studies evaluating the effectiveness of security requirement elicitation techniques in different situational characteristics. Summary of related evaluation work that has been discussed in previous section is described in Figure 1

Table 2.1: Summary of Related Comparative Evaluation Factors of Security Requirement Elicitation Techniques

Research Approach	Compared Approaches	Nature of Approach	Evaluation Criteria Based on:	Main Focus	Findings
Case Study (Mamadou et al, 2004)	Common Criteria Misuse Case Attack Trees	Security Requirement Elicitation Processes	**Technique Attributes** Learn ability, Usability Completeness, Clearity of Output, Analyzability	Comparison to Find advantage & disadvantage	Apply these techniques together to complement Sec RQ Elicitation
Step one Theoretical Evaluation (Nancy et al, 2006)	SSM,QFD, CORE, FODA, CDA, ARM,JAD, Misuse Case, IBIS	Functional Requirement Elicitation Processes except Misuse Cases	**Technique Attributes** Adaptability, Case Tool Client Acceptance, Complexity, Graphical, Output, Implementation duration, Learning Curve, Maturity, Scalability	SQUARE Evaluation	IBIS, JAD are high scorer, while ARM, SSM & misuse case got tie. IBIS JAD & ARM were selected for further comparison.
Step two Case Study	ARM, JAD, IBIS	Functional Requirement Elicitation Processes	**Technique Attributes** 33 characteristics were identified, not specific to security domain but form functional requirement engineering area of study	SQUARE Evaluation	ARM is better than JAD or IBIS in Sec RQ Elicitation
Theoretical Evaluation (Daniel et al, 2006)	Security RQ Engineering Processes based on Models of i*, Agile, Threat, Barrier Analysis Diagrams, Object Driven Use Cases, SIREN, OCTAVE & Risk Driven Security Use Cases	Security Requirement Engineering Processes	**Security Specific Technique Attributes** Degree of Agility, resources Help & Support, Degree of Integration with other Software Requirement, User Friendliness, Contribution of the Proposal as regard Security	Comparison of Security Requirement Engineering Processes Introduced for Different Phases of SDLC	None of them is suitable for Security Requirement Elicitation at RE level

Theoretical Evaluation (Johan et al 2007)	CLASPS & SDL	Security Software Engineering Processes – cover whole SDLC	**Technique Activities to SDLC** Education & Awareness Project Inspection, Analysis, Design Implementation, testing & verification, Deployment	Comparison to find strength and weaknesses on the basis of common & different activities performed by each process in each phase of SDLC	No information: what activities are performed by each process for security requirement elicitation at RE level.
Case study (Andrea et al, 2007)	IESE MOQARE	Non Functional Requirement Elicitation Processes	**Technique Attribute** Guided Process, Measureable NFR, Reuse of Artifacts, Intuitive and Creative Elicitation, Focus Effort and NFR Prioritization, Dependencies Integration of NFR with FR	Comparison to look at the possibilities to improve the techniques by combining their strengths and excluding their weaknesses	Comparison for security requirement elicitation is not possible as IESE was not explored for security issues
Experimental Comparison (Tor & Guttorm, 2008)	Misuse Case Text Description Misuse case Diagram	Security Requirement Elicitation Processes	**Technique Attribute** Number of Failure Mode (any event that could threaten to any actor's mode) **Perception Based Factors including:** Perceived Ease of Use, Usefulness & Intention to Use	Find advantages and disadvantages of text based description & diagram based notation of misuse case to investigate which one is more useful	Textual is better in performance Textual and diagram are same on usability
Theoretical Evaluation (Inger et al, 2008)	SQUARE Security Requirement Engineering Framework (Charles et al,2006), XP Oriented Approach, CLASP, Microsoft SDL, Secure Software Development Process by (Axelle & Makan , 2005), And Security Engineering Processes by (Kenneth &Gary, 2005) & (Gunner, 2004)	Security Requirement Engineering Processes	**Security Specific Technique Activities of Security Requirement Engineering Processes** Definitions, Security Objectives Identification, Misuse/ Threats or Assets Oriented Security Requirement Engineering, Coding Standards, Categorize & Prioritize Security RQ, Inspect & Validate Security RQ, & Process Planning for Security Requirement Identification	Comparison of available Security Requirement Engineering processes at RE level to develop new Security Requirement Engineering Process.	Different level of support of each process to attributes of evaluation criteria. Introduction of new Security Requirement Engineering process that is easy to use and provide stepwise guidance

Experimental Evaluation (Andreas &Guttorm, 2008)	Misuse case Attack Tree	Security Requirement Elicitation Processes	**Technique Attribute** No & Types of Threat **Perception Factors** Perceived ease of use, Usefulness, Intention to use **Situation Factors** 1.Use case description 2.Use case description plus use case diagram	Explore both techniques in order to guide the software community about their selection in different situation	Over all, Attack Tree was high scorer in all situations
Theoretical Evaluation (Jose et al, 2008)	Common Criteria, SQUARE, (OCTAVE), Attack Trees, Usage-centric Sec RQ Eng (USeR), CLASP, Misuse Cases, Abuser Stories, Secure TROPOS , i* Agent based RQ for Sec, Security Problem Frames and Anti-Model	Security RQ Elicitation and Security Requirement Engineering both Approaches	**Security Specific Activities for each Phase of RE including:** Elicitation, Analysis, Specification Management, Integration Support to later Stages of SDLC Total 33 activities were identified and distributed in above mentioned phases	Explore Security Requirement Engineering and Elicitation Processes Comparatively in order to Acknowledge their Strengths and Weaknesses.	Different Level of performance of different level of processes for different phases of Security Requirement Engineering. Misuse Case is high scorer at elicitation phase specifically.
Case Study (Benjamin et al, 2009)	Multilateral approaches, UML based approaches, goal oriented approaches, problem frame based approaches, risk analysis based approaches and common criteria based approaches.	Security Requirement Engineering Processes	**Security Relevant Activities Performed by Techniques at RE level** security goals, and requirements identification, security specification, stakeholder's view, domain knowledge, asset, threat, vulnerability, risk analysis	Comparison of Security requirement engineering processes on the basis of this conceptual framework (CF) to provide guidance how each process realize the attributes of C F	Introduction of a conceptual framework to highlight the security relevant concepts. Different level of performance for different attributes of conceptual framework
Theoretical Evaluation (Umair & Zulkernine, 2009)	11 Secure SDLC such as CLASP, MS SDL 11SecuritySpecification Language such as Secure UML 5 Sec RQ Eng Processes Secure Tropos, SQUARE CLASP , Charles et al, 2006 SREP	Security Development Life Cycles Security Specification Languages Security Requirement Engineering Processes	**Secure SDLC** Security relevant activities performed by each Phase of Secure SDLC **Security Specification Languages** were compared by technique characteristics **Security RE Processes** Activity wise comparison, 23 security specific activities for evaluation	Provide overview of security development life cycles, specification languages and requirement engineering processes & help in their selection	Different SDLC processes, specification languages and requirement engineering processes have different level of performance to respected criteria. Overall: MS SDL & CLASP, UML sec SQUARE &CLASP are better in respected category

On the whole, there are some work in this area where security requirements elicitation have been discussed empirically (Nancy et al, 2006; Anders et al 2007; Benjamin et al, 2009), theoretically (Daniel et al, 2006; john et al, 2007; Inger et al, 2008; Umair & Zulkernine, 2009; Jose et al, 2008) or experimentally (Tor & Guttorm, 2008; Andreas & Guttorm, 2008) but the context of evaluation mostly focuses on technique characteristics base comparison.

Moreover each study has different intention of evaluation. (Mamadou et al, 2004) perform evaluation of such techniques with aim of using them together to improve their effectiveness. (Nancy et al, 2006) highlighted the need of selection of security requirement elicitation process but the assessment of technique was based on predefined criteria that totally contain general characteristics of techniques like graphical output, scalability etc. Another study by (Daniel et al, 2006) makes analysis of security requirement elicitation techniques with consideration of discussing security issues at the whole system development life cycle instead of RE level. They conclude that their selected studies did not have support to elicit security requirements at RE level.

There is also comparative evaluation reported in (johan et al, 2007) that draws attention to emphasize security requirements at RE level but they take into account two security engineering processes and their focus is activity wise comparison of both processes and evaluating their security relevant activities performed at each stage of SDLC. Then experimental comparison of two security requirement techniques described in (Andreas & Guttorm, 2008) focuses on identifying the capabilities of selected techniques for threat oriented analysis in two different scenarios where scenarios were defined on the basis of use case description and use case description plus use case diagrams.

One more comparative research work presented in (Inger et al, 2008) discussed security requirement engineering processes comparatively with the ultimate objective of developing new security requirement engineering process that is easy to use. Similarly, (Benjamin et al,

2009) also presents comparative work where activity based comparison of security requirement engineering processes is conducted in order to provide guidance regarding how each process realizes the activity based attributes of evaluation criteria. Besides, (Umair & Zulkernine, 2009) also highlighted the need of considering security to the whole SDLC and explicitly focus on comparison of security development life cycles, security specification languages and security requirement engineering processes.

Over all, synthesis of literature review reveals that there is shortage of comparative work available about situation base evaluation of security requirement elicitation technique. There are no guidelines suggested in literature for new or less experienced analysts regarding such techniques that which one will be more productive in specific project situations. Ultimately there is a need to comparatively evaluate security specific requirement elicitation techniques from different situational perspectives and guide the software community in selection of these techniques that which one is appropriate for given situation.

CHAPTER NO 3: SELECTION OF SECURITY REQUIREMENT ELICITATION TECHNIQUES & SITUATIONAL CHARACTERISTICS

CHAPTER NO 3: SELECTION OF SECURITY REQUIREMENT ELICITATION TECHNIQUES & SITUATIONAL CHARACTERISTICS

3.1. Security Requirement Elicitation Techniques with RE Level Support

For the evaluation of security requirement elicitation techniques, we researched the relevant literature where security issues have been discussed purposely. We came across variety of studies in this regard such as (Jonathan et al, 2004; Nancy et al, 2005; Donald, 2003a; Cynthia et al, 2002; Gustav et al, 2006; Ambrosio et al, 2002; Michael &Steve, 2006; OWASP, 2006; Inger et al, 2008; Charles et al, 2006; Axelle & Makan , 2005; Gunner, 2004; Kenneth &Gary, 2005; Guttorm and Andreas 2000; Guttorm and Andreas, 2004; Lin, Eric and John, 2002; Axel, 2004; Charles et al, 2004; John, 2004; John, 2004; Seda et al, 2005; Annie, 2000; Simara et al, 2005; Nancy et al, 2006; Nancy, 2006a; Axel, 2007; Charles et al, 2004b;Gary et al, 2002; Nancy, 2006b).

We do not take account all of them as we are interested in evaluation of techniques that have been proposed in literature for security requirement elicitation at RE level specifically while some of the studies have different nature of job. For instance we surveyed (Jonathan et al, 2004; Nancy et al, 2005; Cynthia et al, 2002; Gustav et al, 2006; Ambrosio et al, 2002; Charles et al, 2006; Inger et al, 2008) but do not discuss them in detail as they are security requirement engineering methods and do not specifically discuss notion of security requirement elicitation.

Besides, we did review (Donald, 2003a) but did not take it into account as it discussed security requirement engineering process by introducing information model of it. Similarly we also left out Michael &Steve, 2006; OWASP, 2006; Axelle & Makan, 2005; Gunner, 2004) because they are security engineering processes and focus on security activities of whole system development life cycle.

Finally, the numbers of security requirement elicitation techniques investigated in detail were reduced to seven techniques. These were selected on the basis of following reasons:

- These techniques have been proposed specifically as security requirements elicitation techniques and meet the objective of our research work as we are interested in evaluation of security requirement elicitation techniques.
- These techniques also have support of elicitation of security requirements at requirement engineering level and go up with the goal of our research work as we have aim to guide the software community regarding techniques that discuss security requirements elicitations at requirement engineering level.
- Last but not least, it helps to comprehend the scope of comparative evaluation within manageable size.

In this context, we decided to rate and discuss the following techniques:

- Misuse cases
- Analyzing Security Requirements as Relationships among Strategic Actors
- Elaborating Security Requirements by Construction of Intentional Anti
- Deriving Security Requirements from Crosscutting Threat Descriptions
- Confidentiality Requirement Elicitation and Engineering (CREE)
- Requirement Elicitation Based on Goals with Security and Privacy Policies in Electronic Commerce
- Security requirement elicitation by Issue Based Information System (IBIS)

3.1.1. Misuse Cases

Misuse cases have been introduced in literature as extension of use cases – negative use cases (Guttorm & Andreas, 2000; Guttorm & Andreas, 2004; Ian 2002a; Ian, 2002c) to "describing

behavior that system/entity owner does not want to occur" (Guttorm & Andreas, 2000).The major contribution of Misuse case is "security requirement elicitation" by identification and presentation of threats to system from both outside and inside attackers who intentially abuse the system (Guttorm & Andreas, 2000; Guttorm & Andreas, 2004; Lillian, 2005).

The context of the misuse case model explicitly deals with system functional properties (Ian, 2002c) .Use cases are considered as focal point with the intention of analysis of attacker's capabilities (Meledath, 2006). Output of such analysis is called threat and modeled as "Misuse case" in Misuse case diagram. There is literature available to discuss graphical notations grammar and technique guidelines of misuse case technique in order to elicit security requirements (Guttorm &Andreas, 2000; Guttorm &Andreas, 2004; Meledath, 2006; Lillian, 2005). It is discovered by that literature that misuse case has three structural elements named misuse case, misuser, linking arrows and simple relationships such as – between use case and misuse case as threaten, and between misuse case and security use case as mitigation.

The notion of misuse cases and security requirement elicitation has been discussed by different authors in previously mentioned literature. The review of (Guttorm &Andreas, 2000) suggests that identify threats to use cases without providing any further clarification. Latter the same authors in (Guttorm &Andreas, 2004) reveals that to identify security requirements one first need to identify system assets, define security goals for assets, threats to each security goals as misuse cases, identify and analyze risk for the threats and define security requirements. Here they clarify assets as information, virtual location and activities. This (Guttorm &Andreas, 2004) portray the image that threats are identified only to security goals. Another finding is discovered from (Meledath,2006) with the focus of threat identification as misuse case to each use case including threat against each of the functions, areas, processes, data and transactions involved in the use case. Further analysis of (Lillian,

2005) added more in terms of attacker's classification as insider, & outsiders, and weak points of the system in use case - vulnerabilities.

Moreover, Ian Alexander discusses the effectiveness of misuse case in (Ian, 2002c) by stating that it helps to identify security threats and mitigations. It also support analysis of cause and effect of failure mode and tradeoff between mitigation and system constraints, justification of design options in future reviews, exception handling scenarios. the idea of tradeoff analysis is explored in more detail by same author in literature (Ian, 2002b) where he introduces relationship of conflict with and aggravate to better understand the proposed situation, to avoid conflicts, and guide the stakeholders towards a better economic (cost/benefit) solution.

3.1.2. Analyzing Security Requirements as Relationship among Strategic Actors

The paper (Antonio et al, 2006) proposes a framework for requirement elicitation based on strategic dependency relationship. It applies agent oriented concepts along with Language Extended lexicon (LEL), scenarios and i* structures to support requirement elicitation process. Similar approach is introduced in (Lin, Eric & John, 2002) in context of security requirement elicitation. It (Lin, Eric & John, 2002) contributes to security requirement elicitation community by introducing a new concept relationships among strategic actors to security requirement elicitation at early stages of RE. It defines security requirements in context of social actors e.g. stakeholders, attackers and software components and dependency relationships among them. It also claimed that "analyzing strategic relationships help to understand the impact and extent of threats and the effectiveness of mitigating measures" (Lin, Eric &John, 2002).

Goal oriented analysis is used to identify goals, objects, operations and list of involved agents. Basically it provides domain properties, goal hierarchy, functional & structural view of the proposed systems and set of agents responsible to realize the. It also provides links between different kinds of goals (contribute/conflict), goals and other Requirement models

such as objects/ scenarios/operations/agents. In short goal based analysis helps to understand domain properties, system functional requirements, list of key system agents and roles played by them.

Agent oriented analysis concentrate on system agents such as software components, hardware devices and human entities (Emmanuel &Axel, 2002).They explicitly demand to identify major system agent and dependency relationship between each pair of agent in order to achieve system goals. Scope of dependency relationship is defined as goals, tasks, soft goals and resources (Lin, Eric & John, 2002). The underlying idea is that system is combination of agents and agents depend on each other in order to provide complete system functionality (Antonio et al, 2006). In context of security requirement elicitation dependency relationship between agents is specifically focused with intention of attackers, their motivation, possible attacks and outcome effects of attacks (Lin, Eric &John, 2002).

3.1.3. Elaborating Security Requirements by Construction of Intentional Anti Model

A technique for security requirement elicitation is proposed in literature (Axel, 2004), based on goal oriented requirement engineering framework and obstruction analysis discussed in (Axel & Emmanuel, 2000). The report of (Axel, 2004) explicitly focus on elicitation of security requirement at RE level while literature (Axel & Emmanuel, 2000) and (Axel, 2007) provides conceptual grounds to it.

Proposed technique used goal model of the system to be as a major driver for eliciting security requirements as artifacts of goal elaboration, goal base negotiation, conflict management, goal verification, goal validation and goal obstacle identification and resolution are critically analyzed to have a deep understanding of the current system and develop security specific obstacle model (Axel &Emmanuel, 2000).

Another building block of this framework is security goal model of the system to be. According to perceived understanding of technique (Axel, 2004), security requirements

elicitation is divided in to two parts. At first, preliminary set of security requirements named security goals are elicited by considering generic specification patterns of security goal meta class including all relevant security attributes, Instantiation of these generic specification patterns to sensitive objects of object model, Goal refinement/ abstraction of these security goals to find preliminary set of security requirements and developing object, operation & agent models to compliment security goal model of the system

At this stage when functional requirements, domain properties, security requirements with specification and scenario support, involved objects, agents and operations to achieve them has been identified, Requirement Engineer can step forward towards threat obstacle analysis where obstacles are goal violation statements "whose satisfaction may prevent the goal from being achieved" (Axel, 2004). In fact it compliments security requirement elicitation by considering goal obstruction in terms of attacker's negative goals. It proceeded as negation of security requirement or negation of functional requirement, named root anti goal, Linking of negated goals to class of attackers, Motivation of attackers, Attacker's capabilities (he can monitor & control). Besides this analysis of domain properties exploitable by attackers and software properties exploitable by attackers are also performed to identify necessary conditions in the domain and software that can support attacker's goals. Security requirements are identified to eliminate vulnerable domain and software properties.

3.1.4. Deriving Security Requirements from Crosscutting Threat Description

Security Requirement Elicitation discussed in (Charles et al , 2004), proposed framework of security requirement engineering of (Charles et al, 2006) and role of trust assumption in elaboration of security requirements in (Charles et al, 2004b) provides a general context of security requirement elicitation at early stage of RE. The basic idea is that derive security requirements parallel to architecture development. The synthesis of above mentioned literature shows that security requirement elicitation has iterative nature, it requires

contribution of requirement engineers, designers and security analyst. It uses combined artifacts from both requirement engineering (goals, functional requirements, context diagram & problem frame diagrams) and security engineering community (security attributes, assets, threats of harms to those assets, security requirements). It must consider management control principles in reference of application business goals to identify security goals (Charles et al, 2006).

It is question plus Analysis based approach and demand skills and experience of security analyst regarding security goals attributes – properties, architecture level design and nature of question to raise questions about domain structure and phenomena. It also has support of trust assumptions to end requirement / architecture spiral. Security requirement are elicited by analysis of RE artifacts, review of organization management control principles, identification of sensitive assets, development of threat description to these assets, assessment of domain structure and domain interfaces frame to determine whether they create vulnerabilities in context of threat description.

3.1.5. Confidentiality Requirements Elicitation and Engineering (CREE)

It (Seda et al, 2005) defines security requirements as non functional requirements and emphasize on "systematic methods for specifying security requirements and their consistent integration with system functional specifications". It (Seda et al, 2005) exclusively discusses confidentiality requirements and proposes a technique named Confidentiality Requirement Elicitation and Engineering CREE to elicit and define confidentiality requirements.

Literature of (Seda et al, 2005) only discusses confidentiality requirements, other security requirements are out of scope of this paper. It discusses confidentiality in terms of unauthorized disclosure of sensitive system information. It contributes as a primary note in research of confidentiality requirement elicitation and specification along with functional specification.

The presented technique based on analysis of system functional requirements (use cases), stakeholder hierarchy, domain properties and assumption in which the proposed system is supposed to run on the basis of use cases the system functionality is understood while use cases and stakeholder hierarchy both helps to figure out roles & responsibilities of each stakeholder.

It can be inferred that confidentiality requirements are elicited when a confidential stakeholder show his/her concerns about some data. Modeling technique to represent these concerns is class diagram. Obviously data is processed by the system and at RE level use cases are natural choices to represent system functionality. So use cases are grouped on the basis of data commonality – called episodes. Further analysis considers episodes with list of involved stakeholders and high lights confidentiality requirements as confidentiality goals or confidentiality consent as negative restriction or positive acknowledgement respectively

3.1.6. Requirement Elicitation Based on Goals with Security and Privacy Policies in Electronic Commerce.

A technique for security requirement elicitation based on goal oriented requirement engineering concepts by Simara, Zair and Eduardo is published in (Simara et al, 2005). Proposed technique bases goal oriented requirement engineering concepts (Annie, 2000) and risk analysis approach (Gary et al, 2002). Although the main domain is electronic commerce, for which the proposed technique is suggested in this particular paper, but technique can be used as a guideline for other domains as well. The paper strongly suggests that requirement engineer must consult the existing security and privacy policies (Annie, 2000) in order to find any possible differences and conflicts between existing and newly created security and privacy policies (Annie, 2000; Simara et al, 2005).

Main contribution of the paper is creation of security / privacy policy and their conformance to already developed security/ privacy policies. Security & privacy policies and their role in

security requirement elicitation can be understood by literature reading of (Annie, 2000; Simara et al, 2005; Gary et al, 2002). The survey of this literature indicates two important considerations of security requirements. According to (Annie, 2000) security requirements are produced, after identification of functional requirements and risk assessment. Moreover elicitation of security requirement is parallel to identification of security and privacy policies. It is also strongly recommended by (Annie, 2000) that security requirements must be in compliance with security and privacy policies of organization. This compliance is ensured by adding a striking step Assess Compliance in the proposed framework of (Annie, 2000). It also removes any future risk of contradiction between security requirements of organization and security features of proposed system.

(Annie, 2000) Suggest compliance of security requirements with organization's security and privacy policies while (Simara et al, 2005) recommends compliance of new security policies with existing security and privacy policies. The proposed framework of (Simara et al, 2005) complements framework of (Annie, 2000) by suggesting that new security policies must be analyzed with existing security policies of organization in order to resolve contradictions among them.

3.1.7. Security Requirement Elicitation by Issue Based Information System (IBIS)

IBIS is a question based approach to elicit functional requirement from stakeholders. Originally it was developed in 1979 "to support coordination and planning of political decision processes" (Werner &Horst, 1979), latter, it has been used as tool in dialogue mapping (Jeff, 2008; Jeff, 2003; Kailash, 2009d; Kailash, 2009a) as medium of global online deliberation (Jeff, 2008) and as security requirement elicitation technique by (Nancy et al, 2005; Nancy, 2006a) while working on SQUARE project.

General context of IBIS is claimed to be a supporting tool to elicit requirements in mutilatory system where multiple stakeholders with multiple priorities are involved (Werner &Horst,

1979; Kailash, 2009b. Literature (Werner & Horst, 1979) also mentions it as a source of contradiction resolution by presenting "a very precise picture of the state of discourse". It is also discovered from (Kailash, 2009d) that IBIS has the ability to be molded according to the nature of the given problem and its live examples are (Nancy, 2006a; Jeff, 2008; Jeff, 2003) where the IBIS maps have been used in different context and little modification of original structure of (Werner & Horst, 1979).

Another highlighted finding from (Kailash, 2009c) shows that IBIS framework has two modes of execution. It supports requirement elicitation from group of stakeholders, gathered in conversation meeting to arrive at common consensus or requirement elicitation of an individual person , analyzing the available artifact, identifying problem, propose solution and arguments on the basis of analysis of available artifacts.

Literature review of IBIS with respect to security requirements (Nancy, 2006a) reveals that technique uses rules of questions, group discussions, arguments and model/map theories to elicit a complete set of security requirements. It also support conflict resolutions among diverse stakeholders (through group discussion), specification pattern – map table to describe issue, associated positions, arguments, conflicting issues, originated requirements to document security requirements and their relationships with each other and with other work products e.g. issue sheet and issue map. Besides this quality of questions including types, scope and organization is very important to consider (Nancy, 2006a).

3.2. Evaluation Parameters

There are number of techniques available in literature that are used for security requirement elicitation at requirement engineering level. Though the ultimate objective of these techniques is elicitation of security requirements but they use different perspective to achieve this goal. They differed in terms of artifacts used, artifacts produced, overall context and process to be followed. Similarly not all the attributes of security requirement elicitation

techniques are spelled out explicitly, but only emerge during the practical use of the particular technique.

There are also several attempts made by researchers to explore the typical characteristics of such techniques and discover their strengths and weaknesses on the basis of predefined evaluation criteria as well. In fact, evaluation criteria help to review the security requirement elicitation technique's capabilities for the purpose of establishing whether the technique meets appropriate characteristics.

(Mamadou et al, 2004) propose s a technique characteristics based evaluation criteria for comparison of three security requirement elicitation techniques – common criteria, misuse cases and attack trees. Research support the idea that different security requirements elicitation techniques have different level of strengths and weaknesses and need to be explored and combined in order to be more productive. In this context, authors considered learnability, usability, completeness, clearity of output and analyzability as important attributes of evaluation criteria and illustrated the effectiveness of respected techniques on the scale of these properties. (Nancy et al, 2006) addresses comparison of techniques for security requirement elicitation by introducing evaluation criteria considering the factors of adaptability to security requirement elicitation, tool support, complexity, graphical output, implementation, learning curve, maturity and scalability.

(Daniel et al, 2006) discusses evaluation criteria from another perspective by adding attributes to review the capabilities of technique in terms of its contribution to security requirements engineering, degree of integration with other software requirements, support of tools, procedures and guidelines, degree of agility and user friendliness. Although the criteria has been proposed and used to evaluate security requirement engineering processes but can be used for assessing usefulness of security requirement elicitation techniques as well.

Another different perspective of evaluation have been elaborated in (johan et al, 2007) where two security engineering processes named – CLASP & SDL were compared on the basis of different phases of system development lifecycle. Evaluation criteria contains attributes on the basis of SDLC activities e.g. education and awareness, project inspection, analysis, design, implementation & testing and deployment. The primary contribution of the criteria is to establish guidelines whether described processes perform certain activities in each phase of SDLC.

(Andrea et al, 2007) introduced evaluation criteria keeping in view of learning and understanding of two non functional requirement elicitation methods. It explicitly focus on exploring the underlying process of methods by discussing what guided process use by the method, what means are used to provide measureable non functional requirements, what approach is followed to reuse artifacts, what means are used for intuitive and creative learning, focus effort and prioritization, to handle dependencies to support tradeoff analysis.

Several other authoritative studies have also discussed security specific evaluation criteria to assess the effectiveness of existing security requirement elicitation or engineering processes. (Andreas & Guttorm, 2008) considers number and types of threats identified by security techniques as critical factors for evaluation of security requirement elicitation techniques. Similarly (Tor & Guttorm, 2008) emphasize on identification of more number of failure mode as core element of evaluation criteria to measure the value of misuse case diagram and text notations.

(Inger et al, 2008) addresses security specific activities as significant features for assessing security requirement engineering process and discover activities like perform definition of security relevant concepts, identification of security objectives, Misuse/ threat, asset & their values and coding standard, categorization & prioritization & inspection & validation of security requirements and process planning of security activities to take in to account as

evaluation criteria. (Benjamin et al, 2009) also suggested security relevant activity based evaluation criteria to measure the effectiveness and usefulness of security requirement engineering processes. Authors explicitly focus on identification of stakeholder's view, asset, threat, vulnerability and risk analysis, security goals & security requirements identification, security specification and understanding of domain knowledge as important components of evaluation criteria. (Jose et al, 2008) provides security activity based set of criteria for each phase of security requirement engineering (security requirement elicitation, analysis, specification, management and later stages support). As for as security requirement elicitation phase is concerned, (Jose et al, 2008) figured out seven security specific activities as distinctive properties of evaluation criteria. They include measuring the degree of support for requirements elicitation & stakeholder identification, description of elicitation technique used or recommended customer involvement level, support for elicitation of other types of requirements besides security, dynamics of the elicitation in terms of iterative or non iterative process and support for establishing system boundaries to define the scope of project.

(Axel, 2004) proposed evaluation criteria and suggested that security requirement engineering processes should have support of the general security relevant parameters as compare to activity specific comparative attributes. We decided to consider this criterion for theoretical evaluation of seven security requirement elicitation techniques because it is more logical as:

- It discusses general attributes of security in particular, and composed of security relevant characteristics such as early deployment of security issues to SDLC cycle, incremental building of security from project inception to dispose etc. Whereas other criteria such as (Mamadou et al, 2004; Nancy et al, 2006) discussed evaluation of security requirements elicitation techniques by addressing non security specific

features e.g. tool support, graphical output or learnability rather security oriented aspects are emphasized.

Contents of the evaluation parameters (Axel, 2004) are described as below:

1. **Early deployment:** In view of the criticality of security requirements, the technique should be applicable as early as possible in the RE process, that is, to declarative assertions as they arise from stakeholder interviews and documents (as opposed to, e.g., later state machine models).
2. **Incrementality:** The technique should support the intertwining of model building and analysis and therefore allow for reasoning about partial models.
3. **Reasoning about alternatives:** The technique should make it possible to represent and assess alternative options so that a "best" route to security can be selected.
4. **High assurance:** The technique should allow for formal analysis when and where needed so that compelling evidence of security assurance can be provided.
5. **Security-by-construction:** To avoid the endless cycle of defect fixes generating new defects, the RE process should be guided so that a satisfactory level of security is guaranteed by construction.
6. **Separation of concerns:** the technique should keep security requirements separate from other types of requirements so as to allow for interaction analysis

3.3. Theoretical Evaluation of Security Requirement Elicitation Techniques

We evaluated the security requirement elicitation techniques on the basis of above mentioned parameters:

	Elaborating security requirements by construction of intentional anti models	Deriving security requirements from crosscutting threat descriptions	Analyzing security requirements as relationships among strategic actors	Confidentiality Requirement Elicitation and Engineering (CREE)	Requirement elicitation based on goals with security and privacy policies in electronic commerce	IBIS	MUC
Early deployment	✓	Partial	✓	✓	✓	✓	✓
Incrementality	✓	✓	✓	✓	✓	✓	✓
Reasoning about alternatives	✓	✓	✓	✓	✓	✓	✓
High assurance	✓	×	×	×	×	×	×
Security-by-construction	✓	✓	✓	✓	✓	✓	✓
Separation of concerns	✓	Partial	partial	✓	✓	✓	✓

Table3.1: Theoretical Evaluation of Security Requirement Elicitation Techniques

Theoretical evaluation of security requirement elicitation techniques is presented in table 1 on the basis of criteria selected in section of 3.2. The symbol of (✓) indicates that technique has support of respected attribute while (×) means technique does not provide support to that attribute. Besides this (partial) show that technique has not fully support but some form of support to the respected attribute.

3.3.1. Selection of MUC and IBIS

Results of table 1 are purely based on theoretical analysis of the respected techniques by the author from literature. Technique described in column 2 (intentional anti model) has support of high assurance attribute, indicating use of formal method so it will be difficult to understand and use at RE level. While technique in column 3(crosscutting threat description) partially support early deployment attribute, showing technique does not fully support security requirement elicitation at RE level. Moreover techniques in column 3 (crosscutting

threat description) and column 4 (relationship among strategic actors) do have partial support of separation of concerns describing that both techniques do not keep security requirements separate from other requirement.

Furthermore technique in column 5 (CREE) has been introduced and used in literature for only confidentiality requirement elicitation and does not cover other security attributes where column 6 (requirement elicitation based on goals with security and privacy policies in electronic commerce) contains technique that has been suggested for E commerce domain in (Annie, 2000; Simara et al, 2005).

Finally we decided to evaluate techniques from column 7(IBIS) and column 8 (MUC) for situation based evaluation of security requirement elicitation techniques as rating of both of them shows their support to respected attributes except high assurance. In addition, both techniques have support of visual notations and produce diagrams as output. Visual representations are less ambiguous and display problem at a glance.

Moreover, both techniques explicitly demands representation of all stakeholders' viewpoints in order to elicit complete set of requirements. Further, several studies have exercised MUC and find it meaningful approach for security requirement elicitation. (Mamadou et al, 2004) discovered MUC as simple to learn, use and analyze that provide complete solution. (Jose et al, 2008) suggested MUC as best approach for security requirement elicitation phase as it scored higher rating level among twelve other surveyed approaches.

(Nancy et al, 2006) evaluated MUC along with eight other techniques on the basis of technique characteristics based criteria, where MUC identified as technique that has high rating to be performed in different phases of SDLC with ability of excellent learning power as well. (Andreas & Guttorm, 2008) illustrated that performance level of MUC varies from one situation where only use case description is provided to the other situation where use case

description and use case diagram both elements are provided. MUC performed better in second scenario where situation changed from one to second situational scenario.

On the other hand, IBIS belongs to functional requirement elicitation area of study but has the flexibility to learn and use in different problem domain (Nancy et al, 2006; Jeff, 2008; Kailash 2009d). In context of security requirement elicitation, IBIS claimed to be a top scorer approach on scale of evaluation criteria among other eight techniques (Nancy et al, 2006). It is the only technique that had not been reported as poor on even one attribute of evaluation criteria. It is reported very good on scale of support to tool, client acceptance, complexity management, and learning abilities. Besides it had fair performance on scale of adaptability, graphical output, implementation duration, maturity and scalability.

IBIS also recognized as outstanding performer in support of security analysis by the authors of (Nancy et al, 2006) but case study client were not satisfied with IBIS map structure. Though the report (Nancy et al, 2006) recommended JAD as a security requirement technique for future but this suggestion has some biases that have been discussed in literature review of chapter two. In this scenario we decided to investigate that how these diagrams or analyses of these diagrams facilitate security requirement elicitation in a given situation, at RE level.

3.4. Selection of Situational Characteristics

Literature review of security requirement elicitation techniques described in section 3.1 discovers that security requirement elicitation at RE level demands support of RE level artifacts e.g. business goals, functional requirements, stakeholder hierarchy etc.

It is also identified that security requirement elicitation process based on availability of RE level artifacts. These artifacts provide system understanding and are used as building driver of security requirement elicitation process. As we are interested to investigate the MUC and IBIS at stage of RE, and availability of different types of system artifacts at RE level sets different situational characteristics to elicit security requirements, so we define situational

characteristics on the basis of availability of different types of system artifacts. Only these three situations are included because :

- Firstly, we are interested to evaluate the effectiveness and coverage of mentioned techniques at early stages of requirement engineering.
- Secondly, it also helps to comprehend the scope experiment in manageable way.
- Thirdly, it is also impossible to anticipate all types of situations like size, domain, available resource etc of project and investigate them against selected techniques. Our future work will possibly deal in this context

Following table describe these three situational characteristics:

Situation Name	Artifacts that Defined Situations
Low level of detail	1. Problem statement 2. Position statement 3. Project goals 4. Scope 5. Use case description
Medium level of details	1. Problem statement 2. Position statement 3. Project goal 4. Scope 5. User hierarchy 6. Use case description 7. Use case diagram 8. Overall description of the responsibilities of system users
High level of details	1. Problem statement 2. Position statement 3. Project goal 4. Scope 5. User hierarchy 6. Use case description 7. Use case diagram 8. Overall description of the responsibilities of users' Online Shopping Mall 9. Action sequence (flow chart) 10. Deployment diagram

Table 3.2: List of Situational Characteristics

Situations are presented in form of problem scenarios. Details of three situations can be found in Appendix B, C and D. The contents of problem scenarios are filled out according to the artifacts described in each situation.

CHAPTER 4: EXPERIMENTAL DESIGN

CHAPTER 4: EXPERIMENTAL DESIGN

Experimental research provides more generalized results as compare to case study based research validation (Nigel & Mike, 1989). It is useful approach where comparison of two or more factors involves and primary concern is to investigate the difference between them instead of examining relationships between them (Andy, 2005). Besides, it also has support of descriptive statistics, inferential statistics and variety of graphical representations to provide statistically meaningful measurements of in question research project.

4.1. Identification of Dependent Variables

Major objective of our research work is comparative evaluation of two security requirement elicitation techniques selected in chapter 3 (section 3.3.1) in three different situations identified in chapter 3 (section 3.4) and development of guidelines for future analyst about performance of techniques in given situation. Following section describes dependent variables used as outcome variable to measure the coverage and effectiveness of both techniques in three respective situations. We explicitly focus on:

Dependent Variable	
Effectiveness of Technique	1. Number of security goals
Coverage of Techniques	1. Number of types of security goals 2. Time ▪ Time taken to interpret/understand technique ▪ Time taken to exercise the technique ▪ Time taken to analyze and translate the results of technique in unambiguous and user understandable documents

Table 4.1: Dependent Variables

4.1.1. Rationale for Concentration on Security Goals in Selection of Dependent Variable

Now an obvious question raises that why evaluation criteria explicitly focus on security goals?, Analysis of security requirement elicitation highlights that security goal identification is first step of security requirement elicitation as security goals "establishes a security

foundation in order to justify its discoveries and recommendations" (Nancy et al, 2004). Moreover security goals plays important role in security requirement elicitation process as they are utilized in successive activities of the process. Utilization of security goals helps us to comprehend what will happen if different types of security goals and their conflicts are not identified. For better understanding we classify utilization of security goals in context of two disciplines:

4.1.1.i. Utilization of Security Goals – One

First, describe utilization of security goals in security requirement (Axel, 2001) same as utilization of business goals in requirement engineering (Nancy et al, 2005). It is revealed that security goal: Present organization's ultimate security objective, Used as catalogue for security requirement traceability, Support to identify the priority and relevance of any security requirements, Scopes the whole RE process - & obviously SDLC cycle. Corresponding problem with respect to previous points may be raised if security goals are not identified:

- Irrelevant security requirements are identified.
- Irrelevant security requirements increase the scope of RE process – results are wastage of resources like time, cost and effort.
- Security requirements cannot be traceable to customer's security objectives.
- Security requirements prioritization suffers.

4.1.1.ii. Utilization of Security Goals – Two

Second, description of utilization of security goals specific to security requirement elicitation process. From security requirement elicitation community it takes the concept of "security goals operationalize security requirements" (Charles et al, 2006) so security goals directly contribute in the identification of security requirements. Now---- how do security goals

contribute in security requirement identification varies technique to technique. Different techniques use security goals to identify security requirements from different perspective.

- Negate security goals to produce intentional anti model and refine them to identify domain oriented goal violation condition. (Axel, 2004)
- Instantiate security goals to sensitive objects, perform critical analysis on them, raise questions about them and develop threat descriptions in form of answer to these questions. (Charles et al. 2004)
- Browse the security goal model in order to determine whether there are any goal negations that could be wished by attackers (Axel, 2004)
- Use security goals as a catalogue in order to identify security goals dependencies between system agents and their trust, privacy or security expectations on each other. Then threats are identified in context of "break of security goals dependencies" and corresponding security requirements are elicited. (Lin, Eric, John, 2002)
- Describe each confidentiality goal and consent in form of attribute of confidential requirement: goal owner, degree of agreement, counter stakeholder, strictness of goal, information, owner's rationale, temporal range, context. Mention contextual facts and assumptions specific to security goals and consents in given domain. (Seda et al, 2005)
- Consider security attributes e.g. CIA & A, to investigate the security requirements of system (Nancy et al, 2006)

4.1.2. Rationale for Selection of Time

(Nancy et al, 2006) explicitly suggested the future analyst to evaluate the security requirement elicitation technique on the basis of time needed to learn and implement the respected technique. (Mamadou et al, 2004) also focused on time scale in terms of time taken to learn the security requirement elicitation technique in their study where they evaluated

three security requirement elicitation techniques on the basis of predefined criteria. To evaluate the coverage of MUC and IBIS, we also identified time as key outcome variable. It will assist the current practitioners and future analyst in technique selection process as they are usually interested to select the elicitation technique that provides maximum performance in minimum amount of time. By measuring the coverage of techniques in terms of time we mean time taken to learn the technique, time taken to execute the technique and time taken to interpret the technique in simple language that is understandable to all stakeholders. We divided the time scale on three phases as in some situations less learning time misguide the analyst because they perceived that it will also take less time to apply and analyze the results from the technique, where in reality application and result interpretation may be more complex and time consuming

4.2. Hypothesis Development

Following section described hypothesis statements for situation of low level of detail. Hypothesis for situation of high level of detail & situation of high level of detail can be found in Appendix H.

H0 = there is no significance difference in number of goals identified using MUC and IBIS, in situation of low level of detail
H1= there is a significance difference in number of goals identified using MUC and IBIS, in situation of low level of detail
H2= MUC is greater than IBIS, in terms of number of goals identified in situation of low level of detail
H3= IBIS is greater than MUC, in terms of number of goals identified in situation of low level of detail

Table 4.2: hypothesis for comparing MUC and IBIS regarding no of goals in situation of low level of detail

H0 = there is no significance difference in number of goal types identified using MUC and IBIS, in situation of low level of detail

H1= there is a significance difference in number of goal types identified using MUC and IBIS, in situation of low level of detail

H2= MUC is greater than IBIS, in terms of number of goal types identified in situation of low level of detail

H3= IBIS is greater than MUC, in terms of number of goal types identified in situation of low level of detail

Table 4.3: hypothesis for comparing MUC and IBIS regarding no of goal types in situation of low level of detail

H0= there is no significance difference in learning time using MUC and IBIS, in situation of low level of detail

H1= there is a significance difference in learning time using MUC and IBIS, in situation of low level of detail

H2= MUC is greater than IBIS, in terms of taking less learning time situation of low level of detail

H3= IBIS is greater than MUC, in terms taking less learning time in situation of low level of detail

Table 4.4: hypothesis for comparing MUC and IBIS regarding learning time utilization, in situation of low level of detail

H0 = there is no significance difference in technique execution time using MUC and IBIS, in situation of low level of detail

H1= there is a significance difference in technique execution time using MUC and IBIS, in situation of low level of detail

H2= MUC is greater than IBIS, in terms of taking less execution time situation of low level of detail

H3= IBIS is greater than MUC, in terms taking less execution time in situation of low level of detail

Table 4.5: hypothesis for comparing MUC and IBIS regarding execution time utilization, in situation of low level of detai

H0 = there is no significance difference in technique result interpretation time using MUC and IBIS, in situation of low level of detail
H1= there is a significance difference in technique result interpretation time using MUC and IBIS, in situation of low level of detail
H2= MUC is greater than IBIS, in terms of taking less result interpretation time situation of low level of detail
H3= IBIS is greater than MUC, in terms taking less result interpretation on time in situation of low level of detail.

Table 4.6: hypothesis for comparing MUC and IBIS regarding result interpretation time utilization, in situation of low level of detail

4.3. Research Design

"The choice of an experimental design depends on the objectives of the experiment and the number of factors to be investigated" (Gary et al, 2002). Section of 1.4 (problem domain) 1.5 (research scope), 1.6 (research contribution), 3.2.1 (selection of MUC and IBIS), 3.4 (selection of situational characteristics), 4.1 (Identification of Dependent Variables) and 4.2 (hypothesis development) reveals the objective and factors of our research work as we are interested to investigate the difference between two security requirement elicitation techniques in three different situations, on the basis of predefined criteria and develop guidelines for community which technique is most effective in which situation. So the comparative design is preferred approach for our research validation.

4.3.1. Pilot Study

Before executing a real experiment, a pilot study was conducted to assess the research design and sufficiency of experimental material such as introductory presentations of both techniques and situational scenarios. Six final year bachelor level students were requested to take part in pilot study, but only three members arrived on the decided day. So we conducted the session with one participant for each situation.

The outcome of the pilot experiment suggested some changes in experimental material. Primary finding was using some simple and uncomplicated system to develop situational scenarios. As we used project documentation of a virtual network server for emergency medical care domain and participants had difficulties to understand the system and related technicalities. After discussing with supervisor, we changed the system domain and used project documents of online shopping mall to develop situational scenarios. We purposely selected this domain so the participants can understand the real purpose of the situation and apply the techniques on it.

Besides, second major advice was about technique introductory tutorials. Participants were satisfied with the introductions and definitions of techniques but recommended that tutorials should include example diagrams of MUC and IBIS to demonstrate complete picture of techniques. In response to this issue we added two example diagrams for each technique so the participants can better visualize the working of technique's diagrams.

Further, an additional improvement was also pointed out to include an introductory presentation about security to brief the participants regarding context of security & security requirements. so as a final change, we added a concise introduction of security in start of real experimental sessions.

4.3.2 Sampling

As the population of this experimental research are the subjects who are from software development community and able to learn the techniques and apply them in given situation. We collected sample of the experiment from bachelor students of Software Engineering degree. At first, list of final (8th) semester students was taken containing name and role numbers of students. Keeping in mind that we were totally unaware about the intellectual abilities of the students, we randomly contacted them to participate in the experiment. In response of this contact some students committed to be the part of experiment but ratio was

too small. Then we decided to contact 7th semester students too. Finally 30 students of 8th and 7th semester agreed to participate, on the basis of their willingness to participate and considering the fact that they have taken Requirement Engineering course in first two semester of their degree and are able to learn and apply techniques. This random selection of sample may involve some biases that can affect the results of the experiment, but as student of social science we know that 100% perfect results can never be established. We always try to control different nature of biases up to maximum level as we did in our experiment. Details discussion about them is described in section 4.5, where we addressed different types of threats to the validity of our experimental result and also mentioned how we tried to control them.

4.3.3. Selection of Research Design

Repeated measure design is selected to perform this comparative evaluation. It is strongest design to be followed when we have small number of sample. Moreover, repeated measure design also has limitations named – unsystematic variations and two more under category of systematic variation named – practice effect and boredom effects and (Andy, 2005).To overcome these limitations we used random assignment of subjects to groups and counterbalancing approach respectively. Sample was randomly selected and all the subjects (30) were randomly assigned into 3 groups of 10 each for each situation. We used first come first serve approach to assign subjects to groups. Then in each situation they were further randomly assigned into 2 groups of 5 each. Further, in each situation all the subjects perform both techniques but with different order due to counterbalancing. For instance, in situation of low level of detail, group A performed order of technique MUC – IBIS while group B performed IBIS – MUC. Same is the case with situation of medium and high level of detail respectively.

Design to be Followed		
Techniques / **Situation**	MUC	IBIS
Situation of low level of detail	Group A Group B	Group B Group A
Situation of medium level of detail	Group C Group D	Group D Group C
Situation of high level of detail	Group E Group F	Group F Group E

Table 4.7: Design Pattern to be Followed

4.4. Research Procedure

Experiment was performed in 2 consecutive sessions, on 10 Feb 2011 in university lab no 25, the total expected time for each session was around 4 hours. We were interested to investigate performance based measurements of both techniques in this experiment, where time calculations are important part of it. So we did time stamps for each activity of this experiment.

First session was started with participation of 15 subjects. They were randomly assigned to 3 groups of 5 subjects each and were seated with reasonable distance so no one can see each other's sheet. 2 invigilators were also appointed to make check on participants so they were not be able to cheat. In this session the order of the technique execution was MUC – IBIS but each group was presented from 3 different situations – situation of low level of detail, situation of medium level of detail, situation high level of detail respectively.

- First, introductory presentation of security requirements were presented to participants of three groups
- Second, Group1 was given situation of low level of detail scenario, group 2 was given situation of medium level of detail scenario and group 3 was given situation of high level of detail scenario.

- Third, technique introduction was presented to three groups in form of multimedia presentation
- Fourth, learning task description was presented to three groups and asked them to read it and make a diagram of presented technique
- Fifth, after completing learning activity, three groups were asked to develop diagram of given technique by considering situation based scenarios, given to them at step 2.
- Sixth, after developing diagram, the next activity is to analyze the diagram and identify security goals and write them in simple English.
- Seventh, Steps of third, forth, fifth, sixth, seventh are repeated for second technique with the same groups.

Second session was also started with the 15 participants, randomly divided into three groups. The order of technique is now IBIS and MUC. All the steps mentioned above has been repeated for second session with only difference of technique execution order ~ IBIS – MUC. Detailed description of research procedure with time stamps has been described in appendix I

4.5. Validity

4.5.1 Internal Validity

"Internal validity assesses whether the observed outcomes were due to the treatment or to other factors" (Andreas & Guttorm, 2008). It is usually not possible to control 100 % all threats to internal validity so we tried to eliminate them as feasible. We strictly followed approaches of random selection, random assignment, counterbalancing to remove threats of selection bias or learning effects of participants that may influence internal validity. 2 invigilators were engaged and sitting arrangement of participants was also organized as they were not able to communicate with each other. Another internal validity problem is previous knowledge or history of participants that may change the results. In our knowledge, participants are studying in final year of Software Engineering bachelor degree program.

They have taken Requirement Engineering course in First year but have not been taught Misuse case, IBIS or any security relevant course yet. So we can anticipate that they have no previous history of these factors and are from same level of pool.

They were also provided same material of technique introduction and task description. The total time of session for each group was estimated as 4 to 5 hours and no time pressure was imposed on participants to complete the activities. so we may claim that findings of experiments are not influenced by content bias or time pressure

4.5.2. External Validity

"External validity is the degree to which the conclusions in your study would hold for other persons in other places and at other times" (William, 2006). Using repeated measure design we divided the sample in 2 groups for each situation and conducted the experiment with different people in each group. Though the all 2 groups in each situation followed the same manipulation procedure but the time of session was different as group one of situation 1 performed in morning session and group two of situation 1 performed in evening session. Further, counterbalancing was used as tool to remove order and learning effects. Participants were asked to reference each identified security goal to relevant point of diagram to make sure they have identified task specific security goals and not general text book based security goals. Sample selection and assignment of participants to the groups was completely randomized to remove threats of individual's personal abilities. Participants' motivation was maintained by promising refreshment after completing session. We also considered the availability of participants on the basis of their convenience – experiment session was conducted before starting new semester when participants are free from their previous semester exams.

4.5.3. Conclusion Validity

"A threat to conclusion validity is a factor that can lead you to reach an incorrect conclusion about a relationship in your observations" (William, 2006).To conduct this experiment session we need to have different types of data like task description of each situation, introductory presentation of each technique, description of task for technique learning. In pilot study, two recommendations came into sight – add practical example diagrams of both techniques in introduction & use some straightforward system with simple language as situation based task scenarios. In this context, we added examples in introduction of both techniques and supply contents of all these items in unambiguous format so they can be easily read and understood.

A predefined experimental procedure was also followed and time stamps were properly recorded for each activity to remove threats of "poor reliability of treatment implementation" (William, 2006). Participants were also provided comfortable environment with no outside disturbance in order to avoid "random irrelevancies in the settings" (William, 2006). Personal possessions of participants were tried to control by selecting participants randomly, from final year students of 4 year graduate degree program. Credibility of the results was also assured by considering 0.05 significance value to decide results are significantly proven or not.

4.5.4. Construct Validity

As for as in our knowledge, there is no research has been conducted to compare security requirement elicitation techniques in situation based circumstances. Our research work contributes by providing guideline to software community regarding effectiveness and coverage of two techniques to elicit no security goals, variety of security goals and time utilization of both techniques in 3 different situations at RE level. Though scope of our work

is limited to comparison of two techniques in only three situational scenarios but we are hopeful to continue this work with other techniques and situations in future.

It is also a fact that situation based scenarios and technique introduction tutorial cannot be replacement of real project or conceptual framework of technique, but we tried to overcome these threats. As introduction of the technique was provided them in presentation form and queries were answered by the author during presentation and following activities of session. Session time was set around 4 to 5 hours to provide flexible time frame to participants so they can perform by considering all factors of situations. The contents of situation based scenarios were also filled with all important factors that need to be added to provide a complete version of relevant situation.

Participants with same background were randomly selected and as for as in our knowledge they have not attended any security oriented course before. Moreover they also have not been taught MUC or IBIS before. so we cannot say that observed measurements are due to interaction of participants to security relevant background knowledge. Moreover participants were also unaware the real purpose of the experiment, we did so to eliminate the bias where participants know the purpose of research work and try to perform accordingly

CAPTER 5: RESULT & ANALYSIS

CAPTER 5: RESULT & ANALYSIS

5.1. Data Preparation

Measurements of both techniques for effectiveness (number of security goals) and coverage (number of types of security goals, time) in each situation was coded in order to develop a database of outcome variables for further analysis. Individual responses of each participant for each outcome variable were coded and rechecked for inaccuracy by the author. It involves coding of total number of security goals and total number of types of security goals identified by two techniques in each situation. Taxonomy of (Donald, 2003b) was used to categorize security goals into different types. Moreover time stamps were also coded as technique learning time, technique execution time, technique result interpretation time and rechecked for accuracy.

5.2. Data Analysis

A repeated measure design with support of complete randomization and counterbalancing tools was used to execute the experiment. Screening of obtained data was performed using normality tests - Kolmogorov-Smirnov and Shapiro-Wilk in SPSS, indicating that data of 3 situations is normally distributed and meet the assumptions of parametric statistical testing class. Besides this dependent nature of design indicates to use dependent t – test (Andy, 2005) to analyze the difference between two techniques in given situations. Significance value of 0.05 was selected to assure validity of results because "as social scientist we are prepared to accept as statistically meaningful anything that has less than a 5% chance of occurring by chance" (Andy, 2005) and SPSS was used as medium to perform t – test.

5.2.1. Analysis of "number of security goals" identified using MUC and IBIS in situation of low level of detail, situation medium level of detail & situation of high level of detail

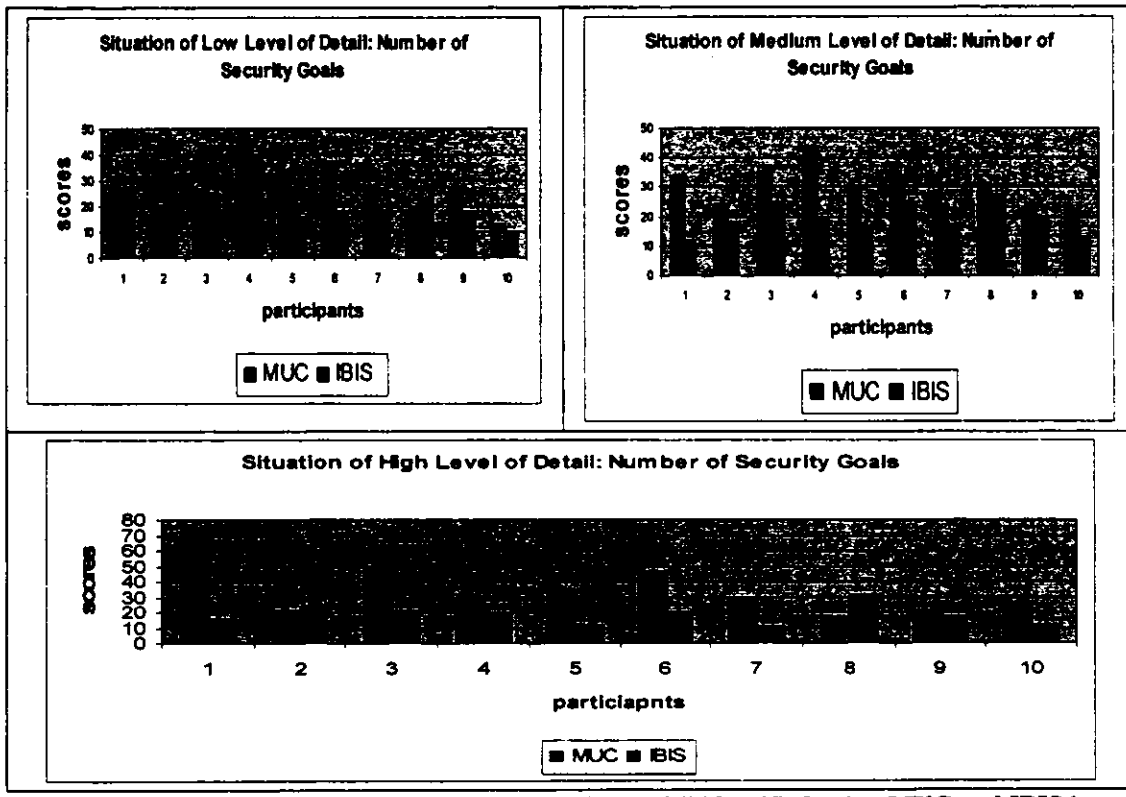


Table 5.1: Graphical summary of "no of security goals" identified using MUC and IBIS in situation of low, medium & high level of detail

Graphical summaries of all 3 situations in table 10, regarding effectiveness of techniques, shows that in majority of the cases more security goals have been identified using MUC as compare to IBIS. In a situation of low level detail, 6 cases identify more security goals by using MUC while in 3 cases IBIS score is higher and in one case result are equal. The difference of performance is so obvious in situation of medium & high level of details where score of all 10 cases is higher using MUC in situation of medium level of detail while 9 cases in situation of high level of detail scored higher using MUC and only 1 case performed higher in IBIS than MUC. Descriptive part of table 11 also indicates the similar result. As we can see mean differences of MUC and IBIS in situation of low level of detail (25.7 & 21.8), in situation of medium level of detail (29.9 & 18.8) and in situation of high level of detail (34.8 & 18.4) respectively describes that MUC performed well in identification of security goals as compare to IBIS.

Paired sample statistics						Paired sample test						
	Descriptive statistics					Paired differences						
		Mean	N	Std. Dev	Std. Error Mean	Mean	Std. Dev	Std. Error Mean	95% Confidence Interval of the Difference Lower Upper	T	df	Sig(2 tailed
Sit of LW	T1-no.g	25.7000	10	8.83239	2.79305	3.90000	7.88036	2.49199	-1.73 9.53	1.565	9	.152
	T2-no.g	21.8000	10	8.28385	2.61958							
Sit of MD	T1-nog	29.9000	10	6.88719	2.17792	1.11000	7.53437	2.38258	5.71 16.48	4.659	9	.001
	T2-no.g	18.800	10	4.89444	1.54776							
Sit of HG	T1-nog	34.800	10	17.1516	5.42382	1.6400	19.75517	6.24713	2.26 30.53	2.625	9	.028
	T2-no.g	18.400	10	6.4152	2.02868							

Table 5.2: Statistical summary: of "no of security goals" identified using MUC and IBIS in situation of low & high level of detail

Statistical findings of no of security goals in table 11 reveal that no significance difference was observed (t (9) = 1.56, p>.05) between two techniques in situation of low level of detail in terms of effectiveness measured as no of security goals. It shows that difference between the MUC and IBIS in terms of effectiveness attribute is not significantly proven and performance of MUC = IBIS in a situation where low level of project detail is available, as calculated value of t (1.56) falls in acceptance region of tabulated value of z ± 2.26 and value of p is greater than .05%, we accept (H0) null hypothesis from list 1 (Appendix H).This will also serve as guideline that if security requirement analyst have a project at RE level with situation of low level of project detail (problem statement, position statement, project goals, scope and brief description of use cases) both techniques have equal chance of selection.

In situation of medium level of detail, significance difference is indicated by (t(9) = 4.65, p<.05) where calculated value of t (4.65) falls in rejection region of tabulated value of z ±

2.26 and p value is less than .05 so we reject H0 and accept H1 in situation of medium level of detail from list 6 (Appendix H). Further we can also accept H2 from list 6 (Appendix H) and can be concluded that on average, use of MUC identified significantly greater security goals (M = 29.90, SE = 2.17) than to IBIS (M = 18.80, SE1.54, t(9)) = 4.659, p<.05) in situation of medium level of detail. It indicates that a project at RE level with a situation of medium level of documentation detail where artifacts like Problem statement, Position statement, Project goal, Scope, User hierarchy, Use case description, Use case diagram, Overall description of the responsibilities of system users are presented, MUC provides high effectiveness in terms of identifying more number of security goals as compare to IBIS e.g. (MUC (M=29.90) vs IBIS (M=18.80))

Statistical results of 3rd situation that contains high level of project details at RE level, are also described in table 11. These findings reveal that there was a significance difference between two techniques where calculated value of (t(9) = 2.62, p<.05) falls in rejection region of tabulated value of z ± 2.26 and p<.05, we reject H0 and accept H1from list 11 (Appendix H), regarding situation of high level of detail. Beside this it can also be anticipated that on average use of MUC identified significantly greater security goals (M=34.80, SE=5.42) than to IBIS (M=18.40, SE=2.02, t (9) = 2.625, p<.05) in situation of high level of detail.

Statistics of 3rd situation clearly demonstrate that if a project situation is such that high level of documentation details are available including (Problem statement, Position statement, Project goal, Scope, User hierarchy, Use case description, Use case diagram, Overall description of the responsibilities of users' Online Shopping Mall ,Action sequence (flow chart) ,Deployment diagram), MUC is appropriate technique to be selected as it provides significantly greater effectiveness indicated by bar graphs of table 10 and proven by statistical summary of table 11 e.g. (MUC(M=34.80) vs IBIS (M=18.40)).

5.2.2. Analysis of no of types of security goals identified using MUC and IBIS in situation of low level of detail, situation of medium level of detail & situation of high level of detail

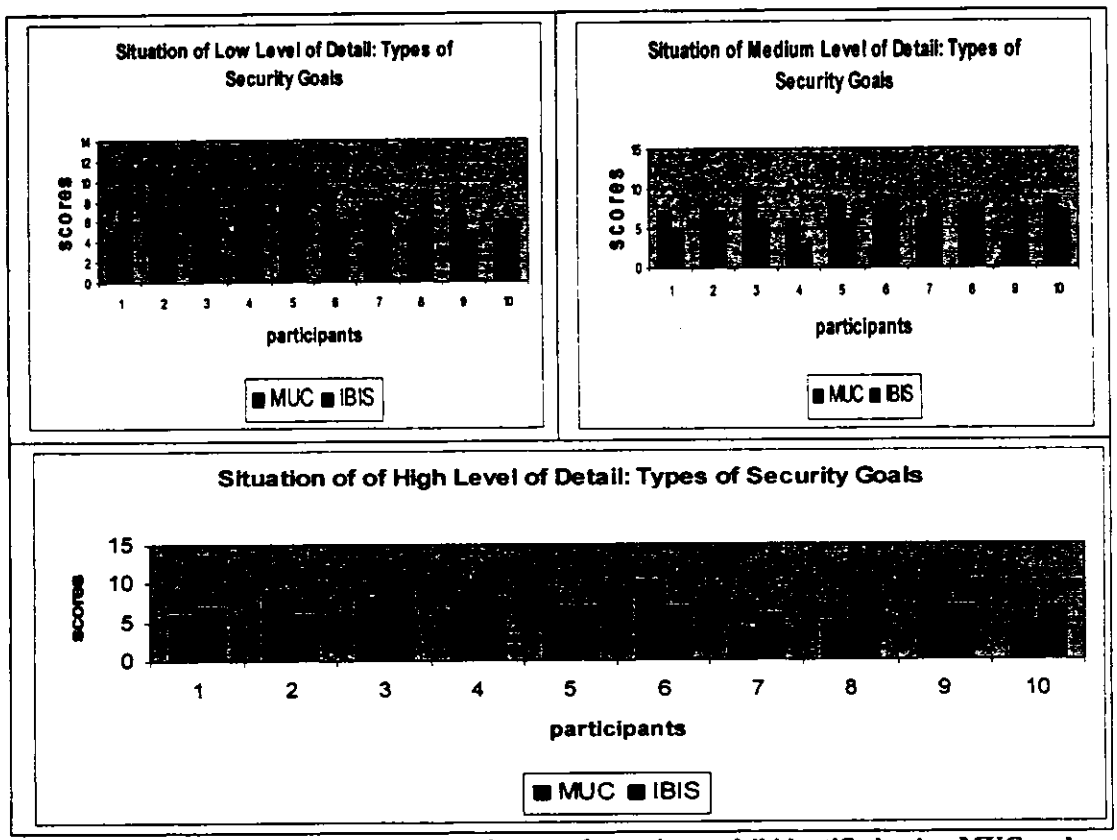


Table 5.3: Graphical summary of "no of types of security goals" identified using MUC and IBIS in situation of low, medium & high level of detail

Analysis of table 12 summarizes scores of number of different types of security goals in situation of low level of detail, situation of medium level of detail and situation of high level of detail respectively. it can be visualized by the graphs of each situation that both techniques have mix scores in terms of variety of security goals. In situation of low level of detail, 4 cases have higher score by using IBIS than MUC, where 3 cases performed well using MUC than IBIS and in 3 cases scores are same. In situation of medium level of detail, it is indicated by the graph that 6 cases performed better in MUC, 3 in IBIS and 1 identical result was found. Similar results are found in situation of high level of detail where MUC performed higher than IBIS in 3 cases and IBIS score is greater than MUC in 5 cases whereas 2 cases have same results. Descriptive statistics of table 13 also describes that the difference between

two techniques in terms of different types of security goals is not so noticeable e.g. mean difference between MUC and IBIS is (7.5000 & 8.1000), (7.4000 & 6.7000) and (7.000 & 7.5000) in situation of low level of detail, situation of medium level of detail and situation of high level of detail respectively.

Paired sample statistics						**Paired sample test**						
	Descriptive statistics					**Paired differences**						
		Mean	N	Std. Dev	Std. Error Mean	Mean	Std. Dev	Std. Error Mean	95% Confidence Interval of the Difference Lower Upper	T	df	Sig(2 tailed
Sit of LW	T1-nog	7.5000	10	1.43372	.45338	-.60000	2.91357	.92135	-2.68 1.48	-.651	9	.531
	T2-nog	8.1000	10	2.23358	.70632							
Sit Of MD	T1-nog	7.4000	10	1.77639	.56174	.70000	2.62679	.83066	-1.17 2.57	.843	9	.421
	T2-nog	6.7000	10	1.76698	.55877							
Sit of HG	T1-nog	7.0000	10	1.94365	.61464	-.50000	2.63523	-2.38513	-2.38 1.38	-.600		.563
	T2-nog	7.5000	10	1.50923	.47726							

Table 5.4: Statistical summary: of No of Types of Security Goals identified using MUC and IBIS in situation of low, medium & high level of detail

Results of statistical calculation of t test for no of types of security goals are described in table 13 for all three situations. No significance difference was found between two techniques in situation of low level of detail with the values of ($t(9)=-.651$, $p>.05$) As calculated value of t (-0.65) falls in acceptance region of tabulated value of $z \pm 2.26$ and value of $p = .531$ we accept (H0) null hypothesis, in situation of low level of detail from list 2 (Appendix H). Similar results are concluded for situation of medium level of detail where calculated value of t (0.843) falls in acceptance region of tabulated value of and $p = .421$ which is greater than .05%, we accept (H0) null hypothesis, in situation of medium level of detail from list 7 (Appendix H).

Furthermore, in situation of high level of detail, calculated value of t (-0.6) also falls in acceptance region of tabulated value of z ± 2.26 with p=.563, we accept (H0) null hypothesis, in situation of high level of detail from list 12 (Appendix H) so on the basis of graphical summaries described in table 12 and statistical findings of table 13, it is concluded that no significance difference was found in both techniques regarding identification of different types of goals in all three situations. It is anticipated that both techniques have equal chance of selection in terms of variety of goal identification for technique coverage capabilities.

5.2.3. Analysis of "learning time utilization" using MUC and IBIS in situation of low level of detail, situation of medium level of detail & situation of high level of detail

Review of table 14 describes the data distribution of MUC & IBIS in terms of technique learning time, as time spent in security requirement elicitation session is a key outcome variable to measure the coverage of techniques in given situation. The objective of measuring such time is to guide the future analyst regarding how much time it takes to learn and use the respected technique in given situation. This will help them to estimate their effort in terms of time distribution needed to manage the total allocated time of project.

For MUC and IBIS we evaluated learning time as introductory presentation of each technique including question & answer activity plus brief task description described in appendix E. firstly, in start of experimental session, technique introduction was carried out in form of multimedia presentation. Total expected time for this introduction was 20 minute. During presentation Question of participants were also entertained, then at the end of presentation, total time of presentation was recorded as part one. Secondly, a learning task description was provided to all groups and asked them first to read it for 10 minutes. Then, they were given 15 minutes to make diagram of respected technique as draft note to assure that they have learned the technique and able to apply it for situation specific task scenario. Time stamps were noted for individual participant on their sheets as they completed this activity. Finally,

total learning time of technique was calculated as time spent for technique presentation and time consumed in learning task activity for each individual participant

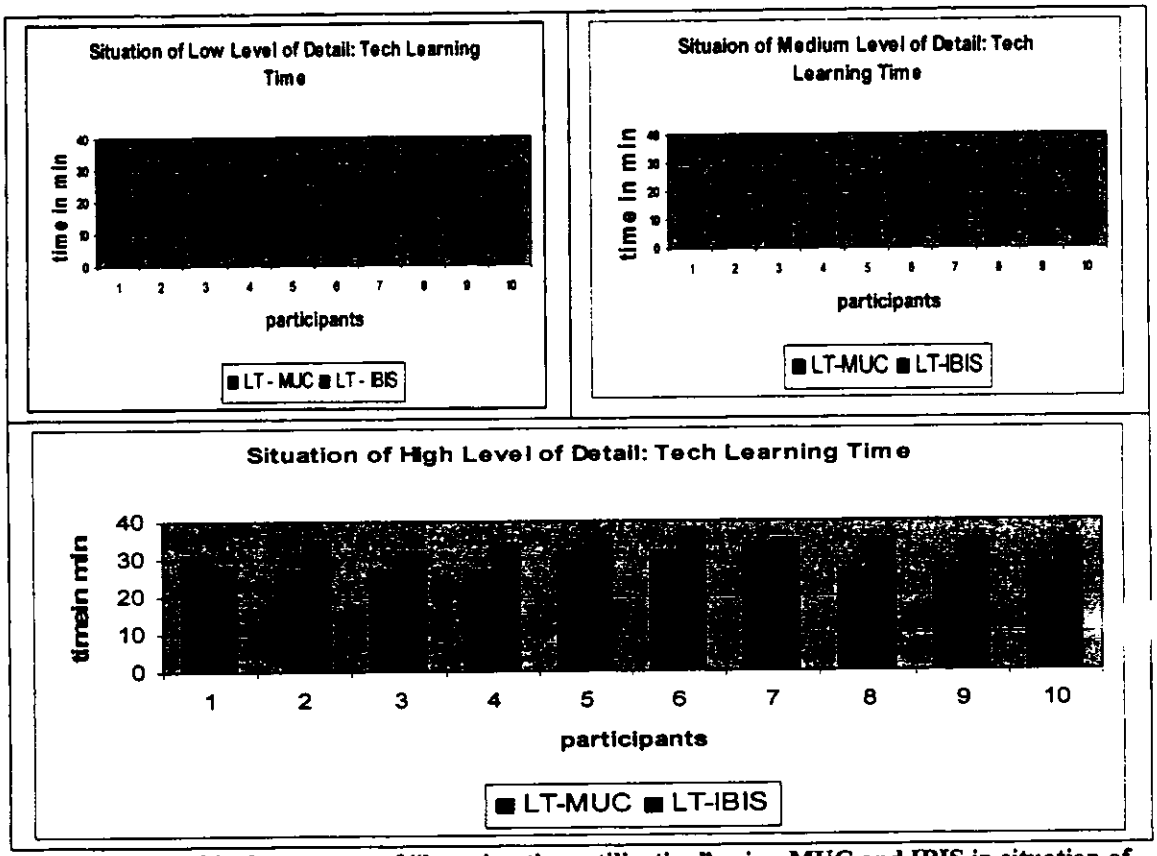


Table 5.5 graphical summary of "learning time utilization" using MUC and IBIS in situation of low, medium & high level of detail

It is observed that bars of learning time for IBIS in situation of low level of detail are higher than MUC in 7 cases while in 2 cases MUC is greater than IBIS but the observed difference between two techniques is very low in each case. Descriptive statistics in table 15 also predicted similar results where calculated mean for both techniques has very small difference of (31 & 32.9). However graphs of situation of medium level of detail and situation of high level of detail in table 14 and descriptive statistics of table 15 indicate difference between two techniques for learning time. In situation of medium level of detail, 8 cases took more time to learn the IBIS while only one case took more time for MUC and 1 case had identical bars. Descriptive statistics found this difference as (29.5000 & 33.0000) for MUC and IBIS in situation of medium level of detail. Graph of situation of high level of detail in table 14 also

shows that 9 cases took more time to learn the IBIS while bar of only one case is higher for MUC than IBIS. This difference is also mentioned in descriptive statistics of table 15 as mean difference of (29.3000 & 34.3000) for MUC and IBIS respectively.

Paired sample statistics						Paired sample test						
	Descriptive statistics					Paired differences						
		Mean	N	Std. Dev	Std. Error Mean	Mean	Std. Dev	Std. Error Mean	95% Confidence Interval of the Difference Lower	Upper	T	df	Sig(2 tailed
Sit of LW	T1-no.g	31	10	3.26598	1.03279	-1.9000	3.51030	1.11006	-4.411	.611	-1.711	9	.121
	T2-no.g	32.9	10	2.46981	0.781024								
Sit Of MD	T1-no.g	29.5000	10	3.17105	1.00277	-3.5000	2.36878	.74907	-5.19	-1.80	-4.672	9	.001
	T2-no.g	33.0000	10	1.63299	.51640								
Sit of HG	T1-no.g	29.3000	10	2.66875	.84393	-5.0000	3.52767	1.11555	-7.52	-2.47	-4.482	9	.002
	T2-no.g	34.300	10	2.6687	.84393								

Table 5.6: Statistical summary of learning time utilization by using MUC and IBIS in situation of low, medium & high level of detail

Statistical findings of learning time consumed by both techniques in table 15 highlight that no significance difference ($t(9) = -1.711$, $p>.05$) was found in situation of low level of detail. As calculated value of t (-1.71) falls in acceptance region of tabulated value of $z \pm 2.26$ & $p>.05$, we accept (H0) null hypothesis, in situation of low level of detail from table 13. In situation of medium level of detail, there was a significance difference between two techniques regarding how much time is taken to learn each technique with the values of t test ($t(9)= -4.672$, $p<.05$). As calculated value of t (-4.67) falls in rejection region of tabulated value of z $\pm$ 2.26 and $p<.05$, we reject H0 and accept H1 in situation of medium level of detail from list 8 (Appendix H)

Further it is also anticipated that on average, MUC took significantly less time to be learned ($M=29.500$, $SE= 1.00$) than IBIS ($M=33.00$, $SE=.51$, $t(9)=-4.672$, $p=.001$) so we also accept

H2 from list 8 (Appendix H) and concluded that MUC is better than IBIS regarding learning time in situation of medium level of detail. Similar findings are observed in situation of high level of detail for analysis of learning time where statistical significant difference (t (9)= -4.482, p<.05) was found between MUC and IBIS for "learning time". As value of t test (-4.482) falls in rejection region and p=.05 we reject H0 and accept H1 in situation of high level of detail from list 13 (Appendix H). Moreover, on average, MUC took significantly less time to be learned (M=29.30, SE=.84) than IBIS (M= 34.30, SE=.84, t(9)= -4.672, p=.002) so we accept H2 from list 13 (Appendix H) in situation of high level of detail to conclude that MUC is better than IBIS in respected situation.

Overall findings of learning time utilization using MUC and IBIS in 3 given situations suggested that in situation of low level of details, MUC and IBIS have equal chance of selection. Although bar graphs of table 14 indicate the difference between learning time utilization of two techniques but that difference is not statistically proven in output of t- test described in table 15 where mean difference between MUC (m= 31 & IBIS(m= 32.9)) and t value (t (9)-1.711 and P>.05) indicate no significance difference found in both technique. However the bar graphs of table 14 for situation of medium and high level of details and statistical findings of respected situations in table 15 provides different result. It is obvious from learning time bar graphs of table 14 that difference in time consumption does exist in both techniques in situation of medium or high level of details. This difference is statistically verified in table 15, where statistical figures of medium level of details are (M=29.500, SE= 1.00) than IBIS (M=33.00, SE=.51, t(9)=-4.672, p=.001) and high level of Detail are (M=29.30, SE=.84) than IBIS (M= 34.30, SE=.84, t(9)= -4.672, p=.002) indicate that performance of MUC and IBIS have significant difference as situation of project changes from low of detail to medium or high level of detail and it also captures that MUC is more

effective in terms of learning time consumption as compare to IBIS in situation of medium and high level of detail.

5.2.4. Analysis of execution time utilization using MUC and IBIS in situation of low level of detail, situation of medium level of detail, situation of high level of details

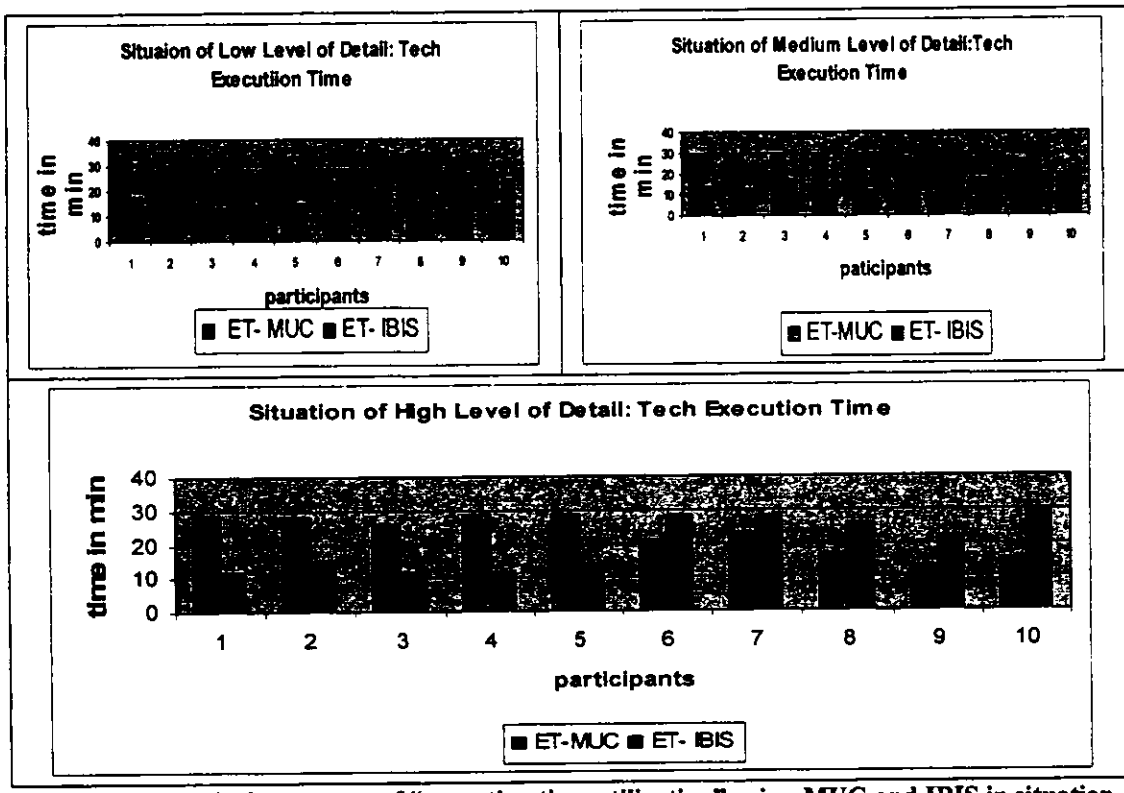


Table 5.7 graphical summary of "execution time utilization" using MUC and IBIS in situation of low, medium & high level of detail

Technique execution time concerns with the time taken to develop diagram of each technique. Graphical summaries of this data for all three situations are presented in table 16 while descriptive data and values of t test are described in table 17. analysis of the graphical charts did not provide clear estimation of comparison in all three situations while descriptive statistics shows mean of the MUC (21.9) is higher than IBIS (19.9) in situation of low level of detail while mean of MUC (25.2) is also higher than IBIS (19.2) in situation of medium level of detail and same observations are recorded for situation three of high level of detail where mean of MUC (23) was larger than IBIS (19.9). as described in (Andy, 2005) "knowing the mean difference alone is not useful" so we need to be statistically assured that

"difference between the means of the condition was large enough not to be a chance result" (Andy, 2005).

Paired sample statistics						Paired sample test						
	Descriptive statistics					Paired differences						
		Mean	N	Std. Dev	Std. Error Mean	Mean	Std. Dev	Std. Error Mean	95% Confidence Interval of the Difference Lower Upper	T	df	Sig(2 tailed
Sit of LW	T1-no.g	21.9000	10	9.08540	2.87305	2.0000	14.499	4.58500	-8.37 12.37	.436	9	.673
	T2-No.g	19.9000	10	5.8777	1.85861							
Sit Of MD	T1-no.g	25.2000	10	4.66190	1.47422	6.0000	10.1324	3.20411	-1.24 13.24	1.87	9	.094
	T2-no.g	19.2000	10	6.17882	1.95391							
Sit HG	T1-no.g	23.000	10	6.20036	1.96073	3.1000	13.0507	4.1270	-6.23 12.43	.751	9	.472
	T2-no.g	19.900	10	7.60774	2.40578							

Table 5.8: Statistical summary of execution time utilization by using MUC and IBIS in situation of low, medium & high level of detail

Analysis of t test in table 17 tells us that difference between two techniques in all three situation regarding execution time is not statistically meaningful with the values of (t (9) = .436, p>.05), (t (9) = 1.87, p>.05), (t (9) = .75, p>.05) for situation of low level of detail, situation of medium level of detail and situation of high level of detail respectively. In situation of low level of detail, as value of t .436 falls in acceptance region with p =.673 so we accept (H0) null hypothesis, in situation of low level of detail from list 4 (Appendix H). Besides in situation of medium level of detail, value of t (1.87) falls in acceptance region with p=.094 so we accept (H0) null hypothesis too from list 9 (Appendix H). Similar results are shown for situation of high level of detail where value of t (.75) also fall in acceptance region with p = .472 so we retained null Hypothesis H0 from list 14 (Appendix H).

It captures the fact that situational attributes of project as low, medium and high level of details at RE level have no importance in terms security requirement elicitation technique selection for MUC and IBIS as statistical findings in table 17 denote there is no significant difference in both techniques in all three situations regarding technique execution time consumption. So no comparative selection may be suggested for future analyst in this regard.

5.2.5. Analysis of result interpretation time utilization by using MUC and IBIS situation of low level of detail, situation medium of level, situation high level of detail.

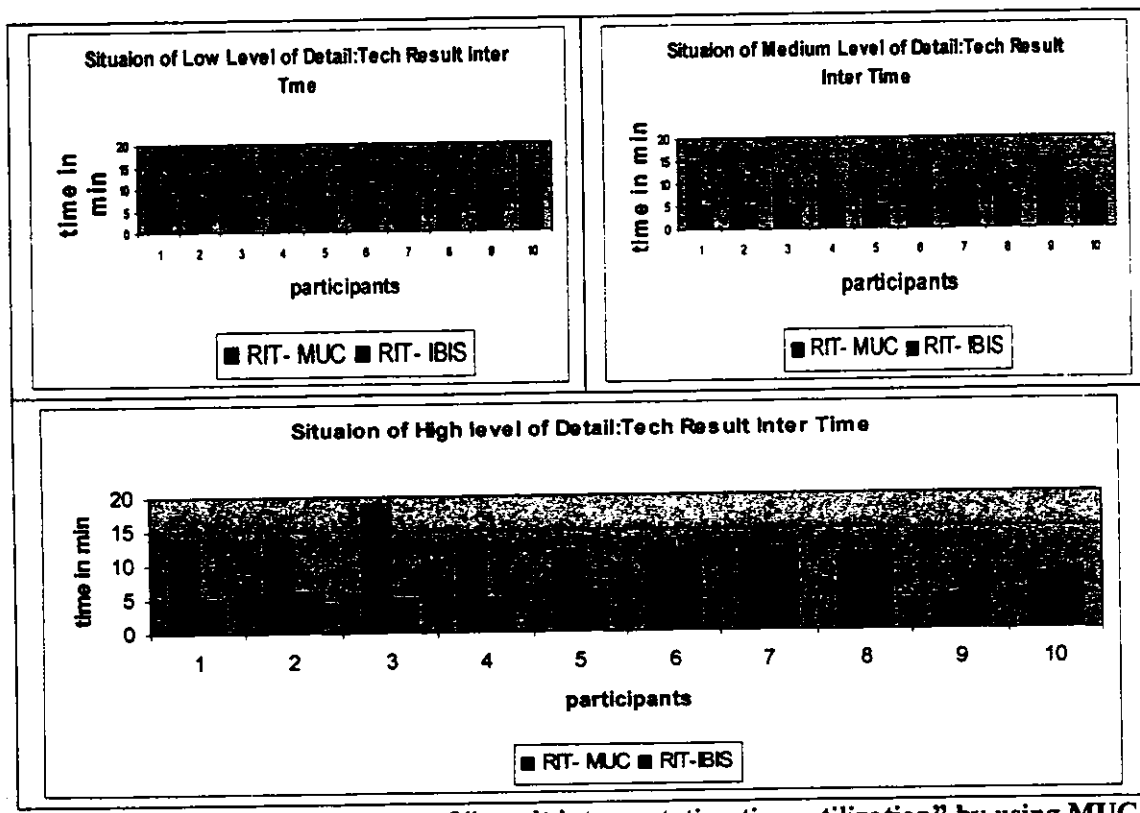


Table 5.9: Graphical summary of "result interpretation time utilization" by using MUC and IBIS in situation of low, medium and high level of detail

Table 18 describes graphical summaries of result interpretation time consumed by both techniques in all situations. Bar graph of situation of low level of detail shows consumed time of result interpretation for MUC was higher on 9 cases while one case has identical bars of time consumption. Similarly mean of MUC in descriptive statistics is also higher (13.4) than mean of IBIS (8.7) which shows MUC consumed more time to be interpreted than IBIS.

Besides this, bar graph of situation of medium level of details inform us MUC score is higher on 8 cases while one case scored more in IBIS than MUC and score of one case is same for both techniques. Same results are predicted by descriptive statistics as mean difference for MUC and IBIS is (12.6 & 8.1) which shows that MUC took more time to be interpreted than IBIS. It is also visualized that in situation of high level of detail, seven cases scored higher by using MUC, two cases have larger bars of IBIS than MUC where one case has identical bars of time consumption. Descriptive statistics also indicate the mean difference of (12.3 & 7.8) for MUC and IBIS which tells us that MUC took more time than IBIS.

Paired sample statistics						**Paired sample test**						
	Descriptive statistics					**Paired differences**						
		Mean	N	Std. Dev	Std. Error Mean	Mean	Std. Dev	Std. Error Mean	95% Confidence Interval of the Difference Lower	Upper	T	df	Sig(2 tailed
Sit of LW	T1-no.g	13.400	10	2.7162	.85894	4.7000	3.0203	.95510	2.53	6.86	4.921	9	.001
	T2-no.g	8.7000	10	1.7029	.53852								
Sit of MD	T1-no.g	12.600	10	2.0110	.63596	4.5000	4.3269	1.3682	1.40	7.59	3.289	9	.009
	T2-no.g	8.1000	10	3.7550	1.1874								
Sit Of HG	T1-no.g	12.300	10	3.7727	1.1930	4.5000	5.4006	1.7078	.636	8.36	2.635	9	.027
	T2-no.g	7.8000	10	2.9363	.92856								

Table 5.10:Graphical summary of "result interpretation time utilization" by using MUC and IBIS in situation of low, medium & high level of detail

Statistical findings of table 19 support the prediction of graphical summaries and descriptive statistics of previous section. In situation of low level of detail, Significant difference is identified as value of t (4.92) falls in rejection region and p<.05%, we reject H0 and accept (H1), in situation of low level of detail from list 5 (Appendix H). it is also noted that on

average, MUC took significantly more time to be interpreted (M=13.4, SE= .858) than IBIS (M=8.7, SE= .53, t(9)= 4.921, p<.001) so we accept H3 from list 5 (Appendix H) and it is anticipated that IBIS is better than MUC regarding result interpretation time in situation of low level of detail.

Patterns of bar graphs in table 18 and statistical figures in table 19 conclude the guidance for future analyst that in a situation of low level of detail, MUC and IBIS have difference in performance regarding result interpretation time consumption and IBIS is better choice to be selected as it takes less time to be interpreted In situation of medium level of details, significant difference between two techniques was also noted as value of t (3.28) falls in rejection region with p<.05%, we reject H0 and accept H1 in situation of medium level of detail from list 10 (Appendix H). Further, it is also anticipated that IBIS is better than MUC as on average, MUC took significantly more time to be interpreted (M=12.6, SE=.63) than IBIS (M=8.1, SE=1.1, t (9)3.28,p=.009) so we retained H3 in situation medium level of detail from list 10 (Appendix H).

These statistical figures about situation of medium level of detail and graphical summary of bar graphs also serve as guideline for future analyst that in such a situation MUC took significantly more effort in terms of time taken to analyze and translate the diagram in simple english document that is understandable for all stakeholders as compare to IBIS so IBIS is suggested approach to be selected in this regard.

Statistical findings of situation of high level of detail regarding result interpretation time consumption reveals that value of t (2.63) falls in rejection region and p<.05%, we reject H0 and accept H1 from list 15 (Appendix H). Besides this it is also noted that on average, MUC took significantly more time ((M=12.30, SE=1.1) than IBIS (M=7.8, SE=.92, t (9)= 2.63,p=.027) so we accept H3 from list 5 (Appendix H).

As graphical summaries of low and medium level of detail denote that IBIS is preferred approach to be selected as it take less time to be interpreted, similar findings are explored in situation of high level of detail where bar graphs of the technique performance shows that in majority of the cases IBIS took less time to be interpreted while this will be further verified by statistical findings described in table 19 where figures proved the significant difference between two techniques and conclude that IBIS is better choice to be selected in such situation .

5.3. Summary of Statistical Findings

Following section provides guidelines regarding selection of security requirement elicitation technique in variety of situation at RE level. The primary contribution of the research is a comparative evaluation of MUC and IBIS in 3 situational attributes presented in table 20, that can be used as guidelines to establish whether a respected technique (MUC or IBIS) is appropriate for given situation (low level of detail, medium level of detail, high level of detail) in terms of coverage and effectiveness.

⇩ \ ⇨	Situation 1		Situation 2		Situation 3	
	MUC	IBIS	MUC	IBIS	MUC	IBIS
No of security goals	~	~	✓		✓	
No of types of security goals	~	~	~	~	~	~
Learning time	~	~	✓		✓	
Execution time	~	~	~	~	~	~
Result interpretation time		✓		✓		✓

Table 5.11: Summary of Main Findings Using MUC and IBIS in all 3 Situations

Table 20 describes summary of main findings that are inferred in previous sections of chapter 5. Symbol ~ is used where no statistical difference was found between MUC and IBIS so we anticipate that both techniques performed equally. ✓ is used where statistical difference was found between MUC and IBIS, besides this one technique is greater than other in terms of performance in relative outcome variable.

Analysis of table 20 reveals that difference does exist between performance of both techniques on the scale of outcome variables in three different given situations. It leads to the idea that different security requirement elicitation techniques works differently in different situation. It also highlights the point that same techniques should not be used in all types of situations as their level of performance varies situation to situations. In this context, there is an urgent need of guidelines for software industry about selection of security requirement elicitation techniques in specific situations, so they can select an appropriate technique from plethora of available techniques that may suit their project situation well by performing better and improve their ability to perform security elicitation at RE level. Following section describes such guidelines in the light of table 20. Though these guidelines are limited in scope and discuss only two techniques MUC & IBIS in three situations (low, medium and high level of detail) but it can be taken as an opening step in this area of research.

5.4. Development of Guidelines

1. Consider security requirement elicitation at requirement engineering level. Consideration of security requirements at early stage of requirement engineering can improve the success record of software projects.
2. Consider two techniques Misuse case and IBIS, as, currently, we are interested to investigate coverage and effectiveness of these two technique
3. Review the section 3.3 to recognize the situational characteristics that will help in selection of appropriate security requirement elicitation technique. As selection of

security requirement elicitation technique demands to understand important characteristics of project situations

4. On the basis of step 3, identify project specific situational characteristics by using section 3.3.as guideline whether its low level of details, high level of details or high level of details
5. Select appropriate technique according to techniques' capability in given situation. Using table 20

Use table 20 from section 5.3 to identify the effectiveness and coverage of techniques in different situations. Situation based selection of security requirement elicitation techniques demands understanding of both situational characteristics of the project and underlying process of available security requirement elicitation techniques. We defined situational characteristics of the projects as situation of low level of detail(Problem statement, Position statement, Project goals, Scope, Use case description), situation of medium level of detail (Problem statement, Position statement, Project goal, Scope, User hierarchy, Use case description, Use case diagram, Overall description of the responsibilities of system users)& situation of high level of detail (Problem statement, Position statement, Project goal, Scope, User hierarchy, Use case description, Use case diagram, Overall description of the responsibilities of users' Online Shopping Mall, Action sequence (flow chart), Deployment diagram) where contents of each situation contains artifacts available to the project.

Summary analysis of this situation based evaluation of MUC and IBIS is illustrated in table 20. It indicates that in situation of low level of detail, both techniques have no statistical difference in terms of all outcome variables except "result interpretation time". IBIS take less time to be interpreted in simple language. So decision of selection of technique in situation of

low level of detail depends on result interpretation time and IBIS is suggested technique to be used in this situation.

Analysis of situation of medium level of detail in table 20, reveals that both techniques have no difference in terms of no of types of goals and utilization of execution time. It is also identified that MUC performed well in terms of no of security goals and learning time utilization while IBIS took less result interpretation time. Decision of selection in situation of medium level of detail may be suggested as use of MUC because it performed well on scale of two outcome variable (identified more security goals and takes less time to learn) as compare to low performance on one out come variable (take more result interpretation time). The selection decision may also depends on the specific condition of project where no of goals or learning time is not considered as important as result interpretation time and selection decision is made on the basis of which technique take less time to be analyzed and in this case IBIS is suggested technique in situation of medium level of detail.

Findings of situation of high level of detail in table 20 are similar to the discoveries of situation of medium level of detail. it is come to know that MUC and IBIS has no statistically meaningful difference regarding identification of no of types of security goals and utilization of execution time while MUC performs better in terms of no of security goals and learning time utilization. Besides, IBIS is better than MUC in terms of taking less result interpretation time. So in situation of high level of detail, MUC has more chance of selection as it performed well on two outcome variables (no of security goal, and learning time) where IBIS has good performance on only one outcome variable (result interpretation time). similar to situation of medium level of detail, technique selection decision may depends on the condition where no of security goals or learning time utilization is considered less important and IBIS may be selected as it takes less time to be interpreted.

Over all, the summary of Table 20 indicates that both techniques have no difference in terms of performance regarding identification of no of different types of security goals and execution time utilization. IBIS is consistently better than MUC as takes less time to be interpreted in all three situations. Moreover MUC is better than IBIS in identification of no of goals and learning time utilization in situation of low level of detail and situation of medium level of detail.

6. CONCLUSION & FUTURE WORK

6. CONCLUSION & FUTURE WORK

6.1. Conclusion

In this research work, we have described a comparative experiment aimed at situation based evaluation of security requirement elicitation techniques and development of guidelines for current practitioners and future analyst regarding selection of these techniques in given situation. Focusing on this primary notion, we have analyzed two security requirement elicitation techniques MUC and IBIS in terms of their capability of coverage and effectiveness in three different situational attributes identified as low level of details, medium level of details and high level of details.

Firstly, The results of the experiment reveal that in a situation of low level of details, performance of MUC and IBIS did not show a significant difference in terms of both effectiveness (number of security goals) and coverage (number of types of security goals, technique learning time consumption, technique execution time consumption) except one attribute of coverage called technique result interpretation time consumption. Graphical summaries and statistical findings demonstrate that the result interpretation time consumption was higher when using MUC as compare to IBIS. So a project at RE level with a situation of low level of detail, IBIS is preferred approach to be selected as a quick and intuitive technique.

Secondly, the results of the experiments are different for situations of medium and high level of details, where use of MUC and IBIS demonstrate obvious differences regarding effectiveness (number of security goals) and coverage (number of types of security goals, technique learning time consumption, technique execution time consumption, technique result interpretation time consumption). A number of interesting findings are elaborated in these situations where it is captured that MUC and IBIS have no significant statistical difference in terms of number of types of security goals and technique execution time

consumption. Besides this It is also noticed that MUC is a preferred choice of selection in both situations of medium and high level of details, as it provide higher effectiveness by identifying more security goals and great coverage by taking less learning time. Another noticeable findings also emerged from the results that in situation of medium and low level of detail, technique result interpretation time is higher for MUC as compare to IBIS, so on this scale IBIS may be a suggested approach to be selected in respected situation. Current practitioners and future analyst may take these findings as guideline regarding selection of MUC and IBIS. Moreover technique selection decision depends on the choice of practitioner whether they select MUC on the basis of its performance of identifying more number of goals and taking less time to be learnt or IBIS by ignoring the facts of more number of goals and less learning time and only considering the capability of technique on scale of less effort in terms of taking less result interpretation time.

6.2. Future Work

This research work evaluated MUC and IBIS in 3 different situations at RE level. Future work may include identification of more situational characteristics in order to establish broad categories of relevant security characteristics. In addition MUC and IBIS could be evaluated to these categories of situational characteristics in order to provide more comprehensive evaluation of these two techniques for potential selection. Another future direction may be evaluation of other security requirement elicitation techniques described in section 3.3 of chapter 3 on the same criteria as we evaluated MUC and IBIS and development of detailed guidelines regarding more techniques.

APPENDIXES

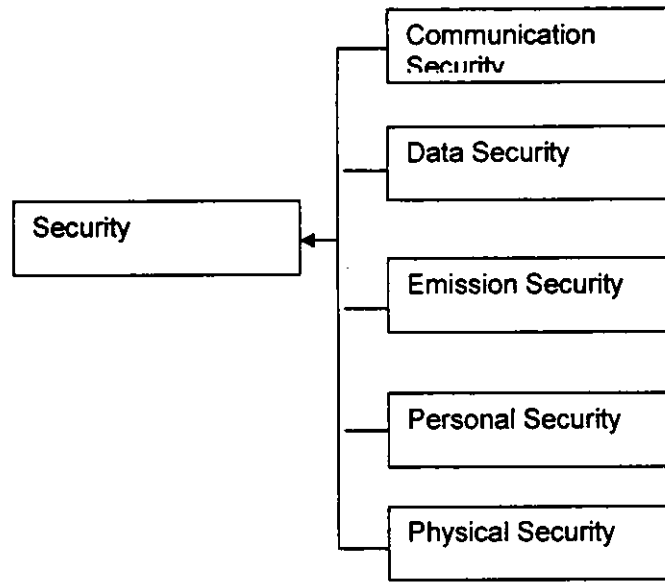
Appendix A: Presentation About Security

Contents of appendix A are taken from (Donald, 2003a; Donald, 2003b). Original contents are rearranged & reorganized to make the presentation more logical.

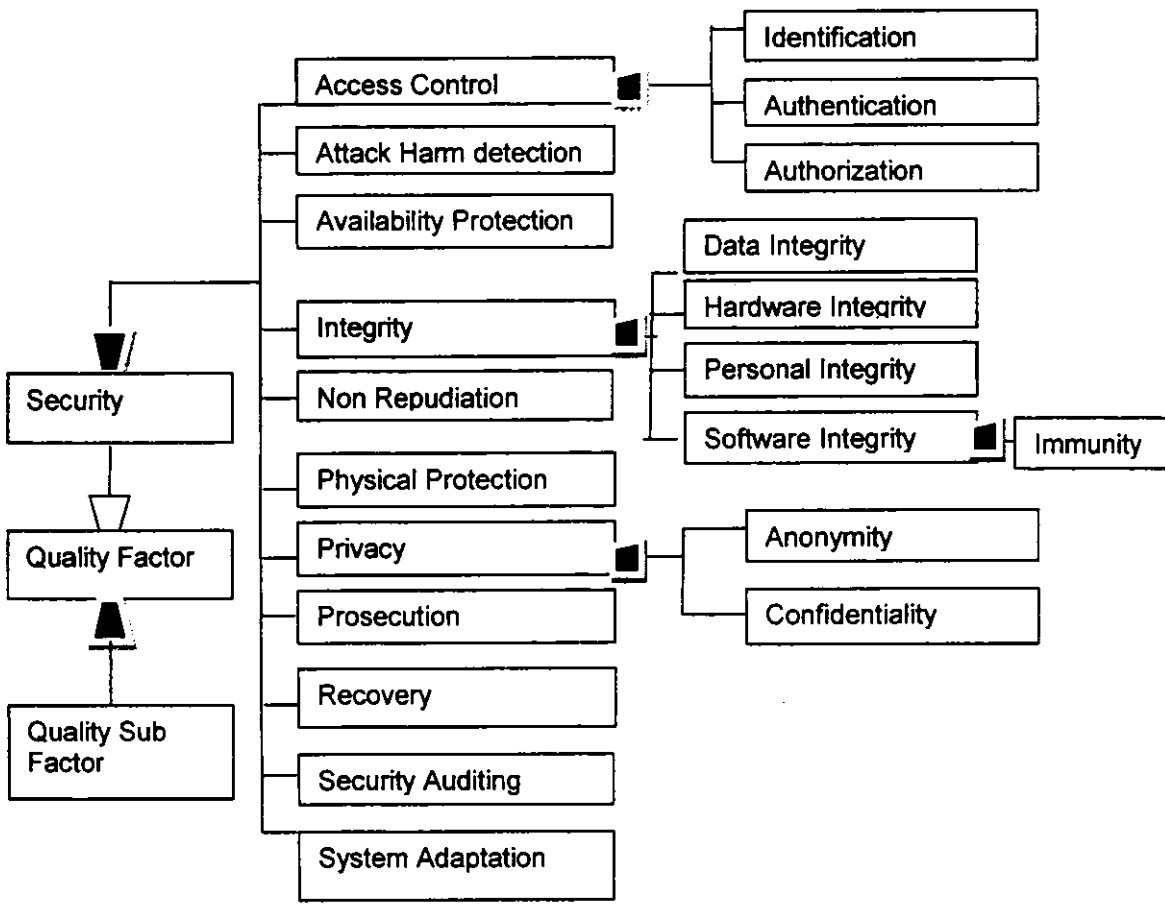
Presentation Title: Computer Security

- **Outline**
  - Introduction
  - Security subclasses
  - Types of security requirements
  - Context of security
- **Introduction**
  - "Computer Security:
    - The protection of information system
    - in order to preserve the integrity, availability and confidentiality of information system resources (includes hardware, software, information/data, and network - communication)"
  - Integrity: protection from unauthorized addition, modification or deletion of system components
  - Availability: system will be available when needed.
  - Confidentiality: private or confidential component of system will not be disclosed to unauthorized individuals.

- **Security Subclasses: Security Can be Classified into the Following:**



- **Taxonomy of Security Requirements Described as Following:**



Description of the Taxonomy of Security Requirements

- **Access control** is the degree to which the system limits access to its resources only to its authorized externals (e.g., human users, programs, processes, devices, or other systems).The following are quality sub factors of the access-control quality sub factor:
  - **Identification** is the degree to which the system identifies (i.e., recognizes) its externals before interacting with them.
  - **Authentication** is the degree to which the system verifies the claimed identities of its externals before interacting with them. Thus, authentication verifies that the claimed identity is legitimate and belongs to the claimant.
  - **Authorization** is the degree to which access and usage privileges of authenticated externals are properly granted and enforced.
- **Attack/harm detection** is the degree to which attempted or successful attacks (or their resulting harm) are detected, recorded, and notified.
- **Availability protection** is the degree to which various types of Denial of Service attacks are prevented
- **Integrity** is the degree to which components are protected from intentional and unauthorized corruption. Integrity includes the following:
  - **Data integrity** is the degree to which data components (whether stored, processed, or transmitted) are protected from intentional corruption (e.g., via unauthorized creation, modification, deletion, or replay).
  - **Hardware integrity** is the degree to which hardware components are protected from intentional corruption (e.g., via unauthorized addition, modification, or theft).

- **Personnel integrity** is the degree to which human components are protected from intentional corruption (e.g., via bribery or extortion).
- **Software integrity** is the degree to which software components are protected from intentional corruption (e.g., via unauthorized addition, modification, deletion, or theft).
  - **Immunity** is the degree to which the system protects its software components from infection by unauthorized malicious programs (i.e., malware such as computer viruses

- **Nonrepudiation** is the degree to which a party to an interaction (e.g., message, transaction) is prevented from successfully repudiating (i.e., denying) any aspect of the interaction.
- **Physical protection** is the degree to which the system protects itself and its components from physical attack.
- **Privacy** is the degree to which unauthorized parties are prevented from obtaining sensitive information.
  - Anonymity is the degree to which the users' identities are prevented from unauthorized storage or disclosure.
    - **Confidentiality** is the degree to which sensitive information is not disclosed to Unauthorized
- **Prosecution** is the degree to which the system supports the prosecution of attackers.
- **Recovery** is the degree to which the system recovers after a successful attack.

- **Security auditing** is the degree to which security personnel are enabled to audit the status and use of security mechanisms by analyzing security-related events.
- **System adaptation** is the degree to which the system learns from attacks in order to adapt its security countermeasures to protect itself from similar attacks in the future.

■ **Context of Security Requirement Elicitation**

- Security analysis of system requires :
  - Consider security attributes
  - Keen understanding of system characterization (functional requirements of system, users of system, data & information, system interfaces, flow of information, network topology, system architecture)
  - Sensitive and critical system assets: Asset is something of value (e.g. data, network, software, hardware).
  - Possible threats to system assets (A threat is the potential for abuse of an asset that will cause harm.
  - Analysis of system vulnerabilities (weak point of system that can be exploited)

Appendix B: Description of Situation Based Scenario No 1

Online Shopping Mall (Situation of Low Level of Detail)

Content of the situational scenarios are taken from documentation of Online Shopping Mall reported at http://osmlite.googlecode.com skynet 2008, 2009. Original contents are rearranged & reorganized to make the situational scenario more detailed and logical.

■ Outline of Document

1. Problem statement
2. Position statement
3. Project goals
4. Scope
5. Use case description

1. Problem Statement

The problem of:	Founded in 1992 in China, "KING Business" is a well reputed Shopping Mall. It has 38 stores with 1500 employees. Each store is tailored to address the needs of valuable customers. They offer a range of products in their stores … Food (Dairy, fruits & vegetables, Groceries, Bakery),…. Non Food office equipment, clothing wear/ Men's wear/children wear/Shoes, sports etc. Today the internet and its boom have created a new economic scenario. Unlike the prevailing "brick and mortar" shops which have physical existence people operate solely from cyberspace. There is a competitive race – physical shopping mall vs online shopping mall.
The impact of which is	In this era of information technology, owners of "KING Business" shopping mall are really concerned to meet the new business challenges. They have identified 3 new challenges in this regard: 1. Barriers of time: with physical shopping mall they have limited working timings… e.g. 9 to 5 2. Barriers of distance: only a limited community can visit the shop. It is very difficult to take order from other city or other country 3. Higher means of doing business: traditional means of sale are more expensive because they have cost of place, salesman, and energy bills etc. By maintaining multiple store fronts, itself being an expensive proposition, store prices are forced to rise.
A successful solution would be:	A system "online shopping mall" is going to be developed. It is an e- Commerce package that is fully featured, user friendly online shopping mall. It would enables vendors to set up online shops, customers to browse through the shops, and a system administrator to approve and reject requests for new shops and maintain lists of shop categories. it will increase their sales by: 1. Allowing them to maximize their working timing by providing opportunity of 24/7 2. Expanding the size of the market from regional to national or national to international,. 3. enabling them to get cheaper means of doing business because E retailers don't have expensive rates and rentals associated with high streets and mall shops

2. Position Statement

The Online Shopping Mall (OSM) application enables vendors to set up online shops, customers to browse through the shops, and a system administrator to approve and reject requests for new shops and maintain lists of shop categories.

Also on the agenda is designing an online shopping site to manage the items in the shop and also help customers purchase them online without having to visit the shop physically.

Our online shopping mall will use the internet as the sole method for selling goods to its consumers. The consumer will be in complete control of his/her shopping experience by using the "unique storefront" concept. Shopping will be highly personalized and the mall will provide lower prices than most competitors. This, in brief, is a description of our product which will showcase a complete shopping experience in a small package.

3. Project Goals

3.1. Definition

The "Online Shopping Mall" (OSM) system will be a global Web-based marketplace bringing together private individuals and small companies to buy and sell all manner of items.

3.2. Business Goal

The business goal of the Online Shopping Mall is to take advantage of the Internet and World Wide Web to radically improve the way private individuals and small companies buy and sell items.

3.4. Business Objectives

The business objectives of the OSM are to provide the following business benefits to its buyer, sellers, and owners.

3.5. Buyers' Business Benefits: The OSM will:

- Provide its buyers with a huge selection of items (and sellers).
- Enable its buyers to easily search for, find, and buy the items they want.
- Enable buyers to buy items that they could not ordinarily find or afford.
- Make buying more convenient by allowing buyers to buy items:
  - Anytime (i.e., 24 hours a day and 7 days a week).
  - Anywhere the buyers have access to the Internet (e.g., at home, at work, and while traveling).

3.6. Sellers' Business Benefits: The OSM will:

- Provide its sellers with a huge customer base of potential buyers.
- Enable its sellers to easily target and personalize their marketing to appropriate potential buyers

- Enable its sellers to sell items that they could not otherwise afford to sell (e.g., by minimizing the overhead and transaction costs).
- Make selling more convenient by allowing sellers to sell items:
  - Anytime (i.e., 24 hours a day and 7 days a week).
  - Anywhere the sellers have access to the Internet (e.g., at home, at work, while traveling).

3.7. Marketplace Owner Business Benefits: The OSM will:

- Minimize the costs of providing a marketplace (e.g., capital costs, labor costs) compared to a physical marketplace (e.g., a shopping mall) by maximizing automation and thus minimizing labor and facilities costs.
- Maximize income by maximizing the number of sellers (i.e., merchants) paying marketplace fees.

4. Scope: Initial functional requirements will be: -

- Secure registration and profile management facilities for Customers
- Browsing through the e-Mall to see the items that are there in each category of products like Apparel, Kitchen accessories, Bath accessories, Food items etc.
- Adequate searching mechanisms for easy and quick access to particular products and services.
- Creating a Shopping cart so that customers can shop no. of items and checkout finally with the entire shopping carts.
- Regular updates to registered customers of the OSM about new arrivals.
- Uploading 'Most Purchased' Items in each category of products in the Shop like Apparel, Kitchen accessories, Bath accessories, Food items etc.
- Strategic data and graphs for Administrators and Shop owners about the items that are popular in each category and age group.
- Maintaining database of regular customers of different needs.
- Shop employees are responsible for internal affairs like processing orders, assure home delivery, getting customer's delivery-time feedback, updating order's status and answering client's queries online.
- Feedback mechanism, so that customers can give feedback for the product or service which they have purchased. Also facility rating of individual products by relevant customers. Also feedback can be given on the performance of particular vendors and the entire mall as well.
- Adequate payment mechanism and gateway for all popular credit cards, cheques and other relevant payment options, as available from time to time

5. Case Description for Online Shopping Mall

The online shopping mall is going to be developed for products of different categories like clothing, kitchen accessories, bath accessories, food items etc. it will enable vendors to setup online shop and customers to browse through the shop and purchase product without having to visit the shop physically. The Mall should be used through internet.

Following use cases are essential:

Manage administration module of online shopping mall: The mall administrator is the super user and has complete control over all the activities that can be performed. He is responsible to approve and reject request for new shop, maintain various lists of shop categories, secure registration and management of user's accounts (customers, shop owner and employees: sales managers, account managers, purchase managers,), create and manage shopping carts, maintain payment records and update guest book entries.

Open E – shop in Online shopping mall: Any user can submit a shop creation request through the application. When the request is approved by the Mall Administrator, the requester is notified, and from there on is given the role of Shop Owner. The Shop Owner is responsible for setting up the shop and maintaining it. The job involves managing the sub-categories of the items in the shop. Also, the shop owner can add or remove items from his shop. The Shop Owner can view different reports that give details of the sales and orders specific to his shop. The Shop Owner can also decide to close shop and remove it from the mall.

Visit online shopping mall: Gusts/visitors can visit the site without registration. They are allowed to visit the site and browse the catalog to search different products.

Establish customer account. As visitor select product for purchase, he gets the offer to establish a customer account. He is assigned a unique id to login and password is set to access the account. A customer profile is established that includes personal information (name,

address, contact num, credit card num), payment details (credit card details) for which security is particularly important. By the time history of purchased items and previous transactions is also included in the customer profile.

Purchase product: A Mall Customer can browse through the shops and choose products to place in a virtual shopping cart. The shopping cart details can be viewed and items can be removed from the cart. To proceed with the purchase, the customer is prompted to login. Also, the customer can modify personal profile information (such as phone number and shipping address) stored by the application. The customer can also view the status of any previous orders, and cancel any order that has not been shipped yet.

Manage sales department: A sales manager mange sales to customers by allocating to the selected product according to the customers choice, view and verify personal details of the customer, alert account manager for assuring of credit card details and financial transaction, and delivering right product to the right customer. He also deals with shipping of the product. He also keeps track of each product items for selling purpose and responsible for informing administrator when any product's stock goes under the minimum level.

Manage account departments: Account manager deals with financial department of the Online shopping mall. he regulate payments by keeping track of all the payment transactions made by the customer and update payment information.

Login to the customer account: every user must provide user name and password for this. New users can sign up by creating new id.

Log out from customer account: customer must logout before leaving the online shop. If the customer is idle for 5 min, logout will occur automatically due to a time out function

Appendix C: Description of Situation Based Scenario No 2

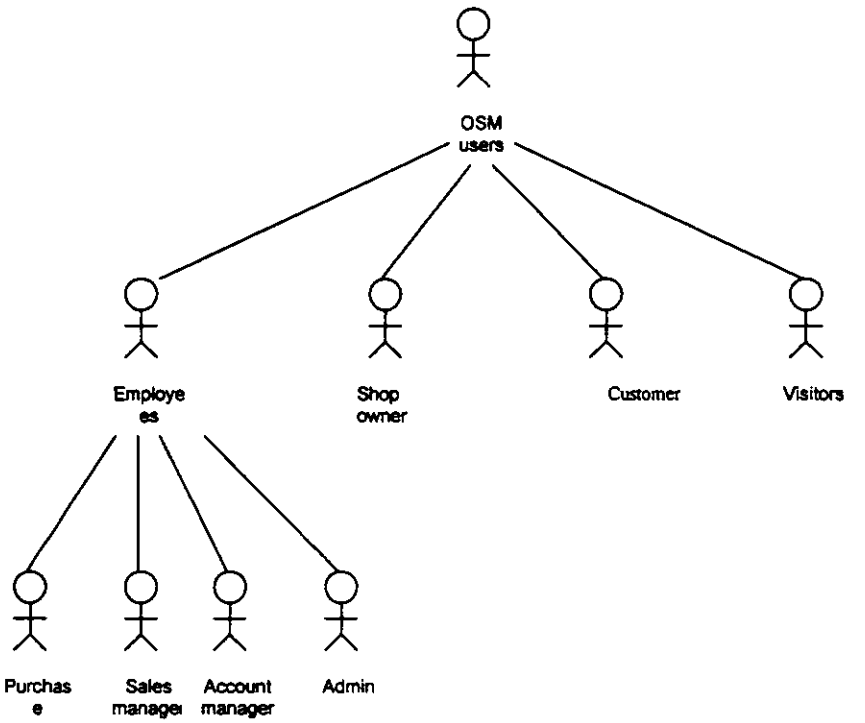
Online Shopping Mall (Situation of Medium Level of Detail)

■ **Outline of Document**

1. Problem statement
2. Position statement
3. Project goals
4. Scope
5. Use case description
6. User hierarchy
7. Use case diagram
8. overall description of the responsibilities of users' Online Shopping Mall

Problem statement, position statement, project goal, scope and use case description are same as described in appendix B for situation of low level of detail, so in appendix C, we just describe additional artifacts (user hierarchy, use case diagrams, overall description of responsibilities of users' Online Shopping Mall) for situation of medium level of detail.

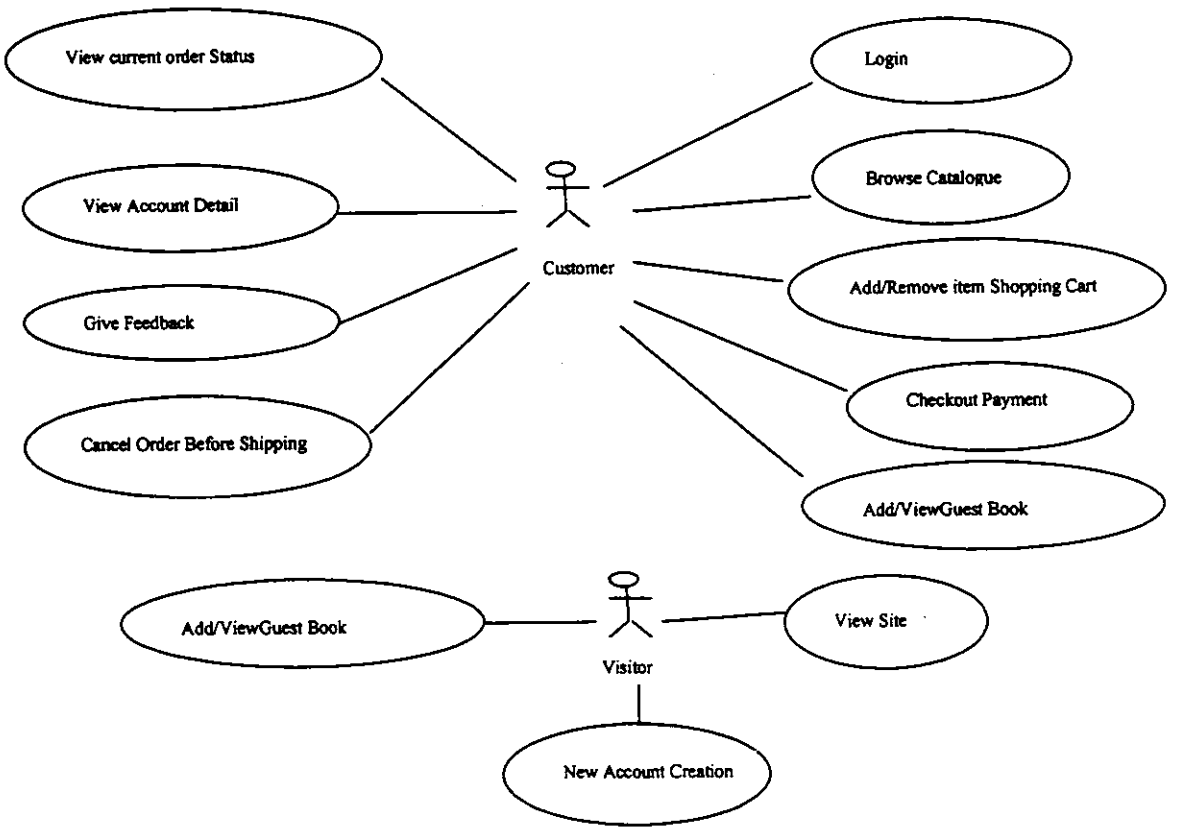
6. User Hierarchy: Hierarchy of Target Users:



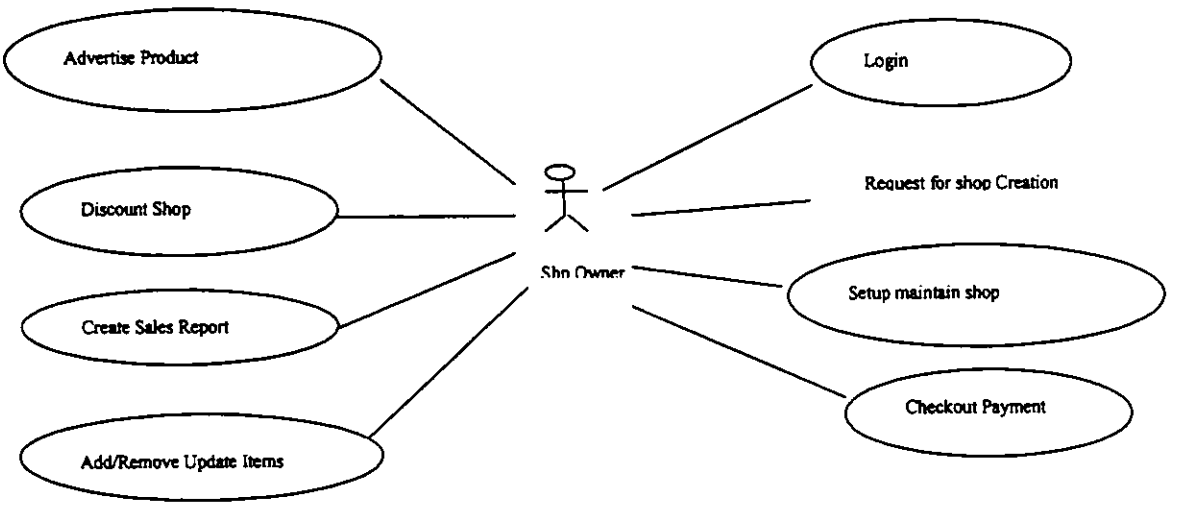
Visitors	Visit the shops	Browse through the shops & view products
Customers	Buy products from the shops	Browse through the shops, maintain user profile, place order
Shop owner	Owner of the shop	Setting up the shop and maintaining it
Employee 1.**Purchase manager**	Maintain purchasing activities	Manage stocks of each product, take perMUSsion from admin for the products to be purchased on Online Shops.
Employee 2.**Sales manager**	Look after the sales of products	allocating right products to right customer, verify personal details of customer to confirm the order and regulate shipping procedures
Employee 3.**Account manager**	Look after accounting activities	Regulate payments, keep track of financial transaction
Employee 4.**Administrator**	Super user of the system	Has complete control over all the activities that can be performed, approve/ reject shop creation requests, manage list of product categories, maintain user accounts and guest book entries

Summary of Target User

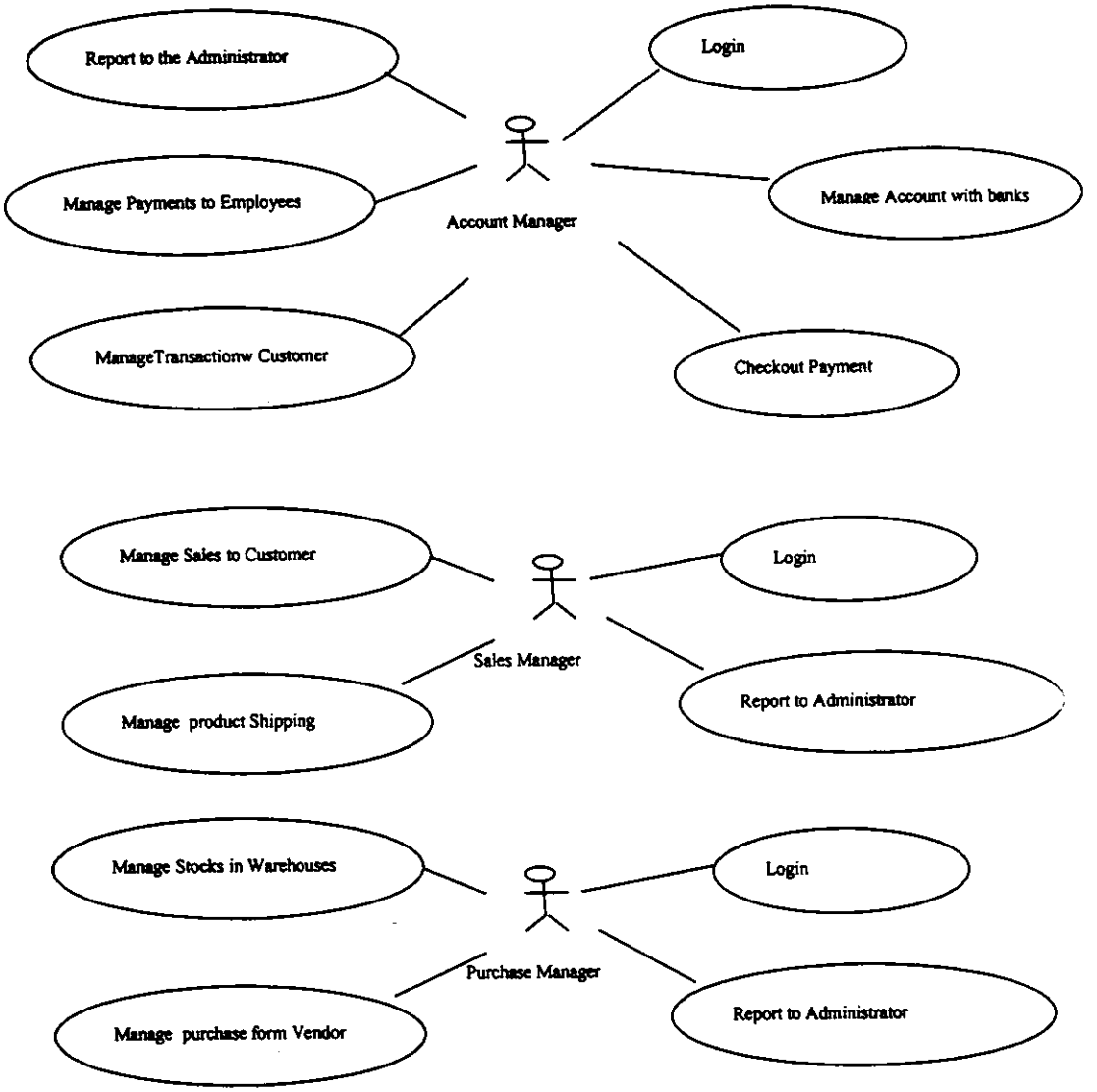
7. Use Case Diagrams



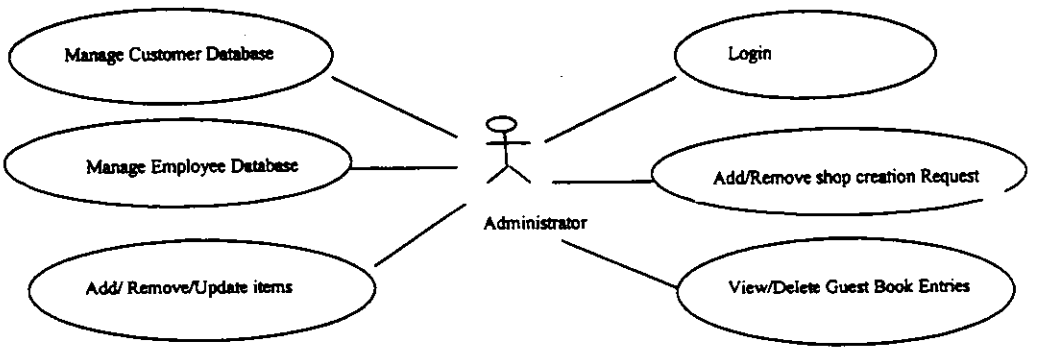
Use Case Diagram for Customer & Visitor



Use Case Diagram for Shop Owner



Use Case Diagrams for Employees



Use Case Diagram for Administrator

8. Responsibilities of User

Given below is an **overall picture of the responsibilities of OSM users** as depicted in the above use-case diagrams:

Administrator:

- **Database Management:** Control the database and keep track of all records of customers and employee details.
- **Contact and Giving Permission to Vendors:** Contact with the vendors and give permission to sell their product under the site after testing the product's quality.
- **View all details:** View the details of all employees and control the whole site.
- **Advertising the Site:** Responsible for making advertisements for the site.

Customers:

- **Login:** Customers must have a valid login id to enter into the site.
- **Registration:** New users can sign up by creating new ID.
- **View and edit Own Details:** Can view/edit his personal details, payment details, and details about services provided.
- **Choosing and comparing products:** Can view all available products and can compare them and make a choice for purchasing products.
- **Purchasing:** Can purchase any product through valid credit card.
- **Giving Feedback to Customer Care:** Can give feedback to the 24X7 Customer Care Service center about their impression for the site and services.

Visitors:

- **Visiting the Site:** Can only visit the site without registration.
- **Register :** register themselves as customer to buy products

Shop Owner:

- **Taking Permission from Administrator:** Vendors must take permission from the Administrator for selling their products under the site. Administrator will test product's quality according to its market price to permit vendor for selling purpose.
- **Consulting with Administrator:** Can consult with the Administrator regarding product's quality and advertisements.
- **Advertising Vendor's Own Products:** Responsible for making advertisements of his products, but the site will not be responsible for any kind of advertisements about product

Sales Manager:

- **View customer details:** View the personal details of the customer.
- **Managing Sales to Customers:** Responsible for properly allocating the selected product according to the customer's choice and delivering product to the customer.
- **View Product Stocks:** Keep track of each product item's stocks for selling purpose.
- **Contacting with Administrator:** Responsible for informing administrator when any product item's stock goes under the minimum level.

Purchase Manager:

- **Consulting with Administrator:** Taking permission from the Administrator for the product to be purchased from vendor.
- **Product Stock Management:** Responsible for managing stocks of each product items.

Accounts Manager:

- **Regulating Payments:** Keep track of all the payment transactions made by the customers and update the payment information.

- **Consulting with Banks:** Responsible for contacting the banks for the validation of the a/c number provided by the customer while purchasing and make the transaction from the given a/c.
- **Consulting with Administrator:** Consult with the Administrator about the payment details of the customers for the updating of the database.

Appendix D: Description of Situation Based Scenario No 3

Online Shopping Mall (Situation of High Level of Detail)

■ **Outline of Document**

1. Problem statement
2. Position statement
3. Project goals
4. Scope
5. Use case description
6. User hierarchy
7. Use case diagram
8. Overall description of the responsibilities of users' Online Shopping Mall
9. Action sequence (flow chart)
10. Deployment diagram

Problem statement, position statement, project goal, scope and use case description are same as described in appendix B for situation of low level of detail and user hierarchy, use case diagrams, overall description of responsibilities of users' Online Shopping Mall are same as described in appendix C for situation of medium level of detail, so only additional artifacts for situation 3 (Action sequence, Deployment Diagram) are included in appendix D

9. Action Sequence

This section describes in detail the sequence of steps that are needed to be done by the users of the system to utilize the functionalities being provided by this web application. Grouping the actions by users, we start from the following user of the system:

- **The Customer:**

The customer is the main user of the shopping mall website and is the main reason why this web application exists in the first place. The customer can browse through the shops and choose products to place in a virtual shopping cart. The shopping cart details can be viewed and items can be removed from the cart. To proceed with the purchase, the customer is prompted to login. Also, the customer can modify personal profile information (such as phone number and shipping address) stored by the application. The customer can also view the status of any previous orders, and cancel any order that has not been shipped yet.

Since the customer is the main user of the system, we will follow the customer as he or she goes about with the various activities in the shopping mall. This way we will have explored all the ways this shopping mall functions as well as obtained an "algorithm" of the steps of functioning of the entire shopping mall application.

The Algorithm is:

Step 1: A potential customer X visits the website of OSM.

Step 2: X either knows the product he or she is searching for or is unaware of his expectations from the shopping mall.

Step 3a: If X knows the product he is searching for he enters the name of the brand of that product in the search box on the home page itself. He is then whisked right to the separate page for that brand, where he can choose the product according to his liking.

Step 3b: If X wants to browse the products before deciding what to buy, then he can choose the categories of the products in the home page itself. From there he will be taken to the product categories page from where he can choose the brand that appeal to him.

Step 4: After selecting the brand of the product, X can click on a particular product which will take him to the product page for that particular product. This page contains all the detailed information about the product.

Step 5: Now that the product has been selected, X might want to actually buy the product. He will then have to log in to the website to actually affect the buying process.

Step 5a: If X is a new user, he will have to first register in the website's new user registration page. Then he will be able to login to the website and complete he transaction.

Step 5b: X may also wish to view his account detail in the account details page. There he can check and change his contact information. He can also view his shopping cart including any incomplete shopping carts which have not matured to the buying status.

Step 6: When X selects to buy the product he may follow two paths.

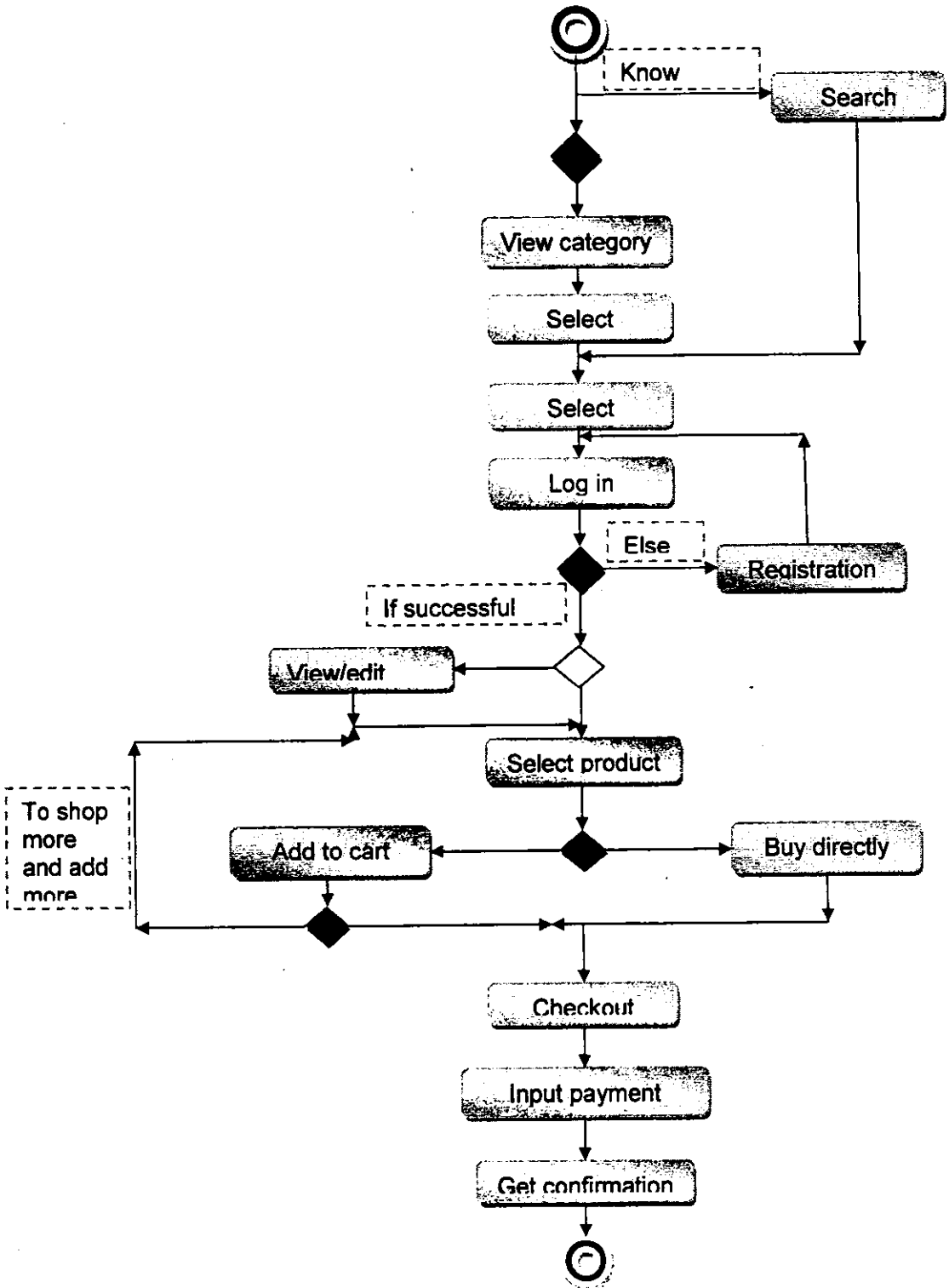
Step 6a: X may add one item to his shopping cart and then keep on browsing the store for more good things. When he has filled his cart to the brim, he can rush to checkout the shopping cart on the shopping cart page.

Step 6b: Or X may decide to buy just one product and rush to checkout the product. He can then in the checkout page put in his credit card information and submit the information. That will complete the transaction process.

Step 6c: Or after browsing for some products, X can come back to his incomplete cart and complete the payout process.

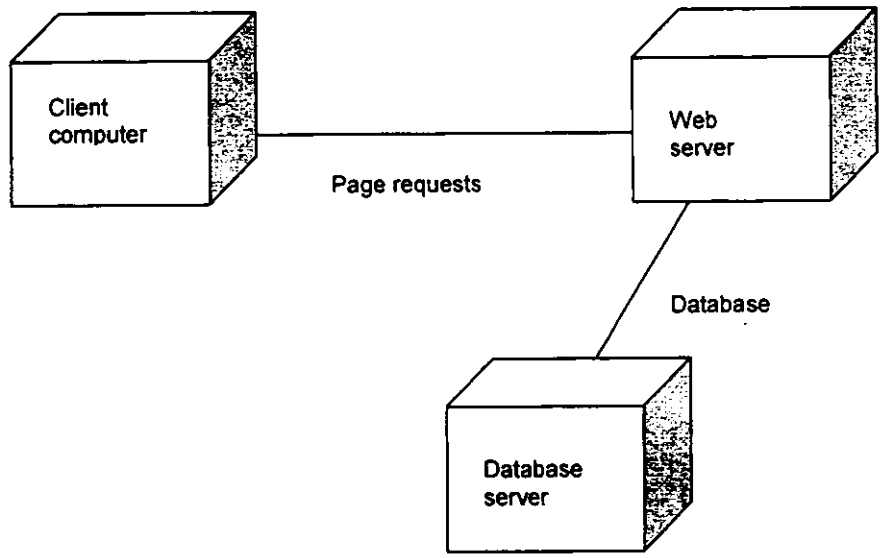
Step 7: X will have to provide his credit card details and then proceed to check out. Then he will be given a confirmation that his credit card has been validated and that he will receive the product within a stipulated time frame.

The Flowchart For the Aforementioned Steps:



10. Deployment Diagram

The following deployment diagram describes how the "Online Shopping Mall (OSM)" system is deployed across an infrastructure. The intention is not to describe an infrastructure but rather the way in which specific components belonging to OSM system are deployed.



Deployment Diagram

Three major components:

- Client computer
- Web server
- Database server

Client Computer

A customer uses computer, equipped with web browser (e.g. internet explorer) to request the resources from web server. Through browsing he can select product items they would like to order online.

Web Server

Web server works as a routing point between all client browsers and the data base. Its task is to provide requested resources to client browser by calling on Database server. As the

online transaction involves the web server communicate with the database server to update the status of the data base.

Database Server

The data server, which provide the application server with the data it requires. It stores data of customer's profile, product stock, shopping cart etc.

Appendix E: Tutorial about Task for Learning Activity

Online Education

Introduction

If you want to earn a degree but you work full time and have children at home, you may feel that going back to school is not an option. One way to get that important diploma is to consider earning a degree online. Our online "education system" allows you to quickly search for available Online postgraduate courses / research opportunities

Main features:

Search for available courses: Applicant interested in Online Education can visit our website "www. Online Education" Site maintain list of courses – undergraduate/postgraduate/ research categories. There are also list of majors in each category along with degree duration, semester schedule and fee requirements.

Student registration: To apply for online degree system asks applicant to register himself as student. Applicant's student account is set and user id and password is assigned. After creating a login, applicant selects the degree from "Undergraduate", "postgraduate", "research" catalogue. System shows list of majors and applicant click on one major e.g. MBA. This will take the applicant to admission form screen. Applicant will complete the admission form by entering personal details (name, age, address, ID number) the degree details (MBA) and credit card details (pin number, amount of tuition fee per course) are included.

Student online learning After completing the admission process, applicant is recognized as student. He is able to maintain user profile, access and download faculty resources (lectures, quizzes, assignment, exam sheet and result transcript). He is also able to contact with faculty members and other degree fellows by an "online discussion room.

Faculty online education System maintains user account for Faculty members too. They also have user profile (name, address, faculty status etc) and financial icon (statements of their

credit hour and course package, bank account number, and the way pay check transferred to their account). They are eligible to upload lectures, assignments, and result transcript, conduct exam and quizzes participate in online discussion room, view students submissions (assignment, quizzes and exams and develop result transcript)

Student/faculty login: Student/faculty must have to enter a valid login ID and password to access their account

Student/faculty logoff: Student/faculty must have to logoff before leaving the site

Appendix F: Tutorial about Misuse Cases

Contents of Appendix F are based on literature (Guttorm & Andreas, 2000; Guttorm & Andreas, 2004; Ian 2002a; Ian, 2002b; Ian, 2002c; Meledath, 2006; Lillian, 2005).Original contents are rearranged & reorganized to make the tutorial in a logical flow.

1. Introduction:

Misuse cases have been introduced in literature as extension of use cases – negative use cases. The major contribution of Misuse case is presentation of threats and hostile intentions of attackers to break the system. The following definitions from literature are referred to make tutorial more precise:

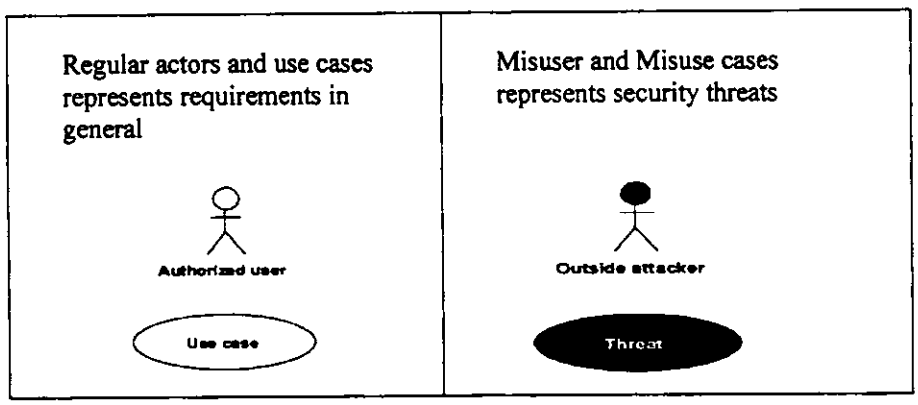
2. Structural Elements:

(1) Misuse Case:

"A Misuse case is a special kind of use case, describing behavior that the system/entity owner does not want to occur". Moreover Misuse case are defined as "A sequence of actions, including variants, that a system or other entity can perform, interacting with Misusers of the entity and causing harms to some stakeholder if the sequence is allowed to complete".

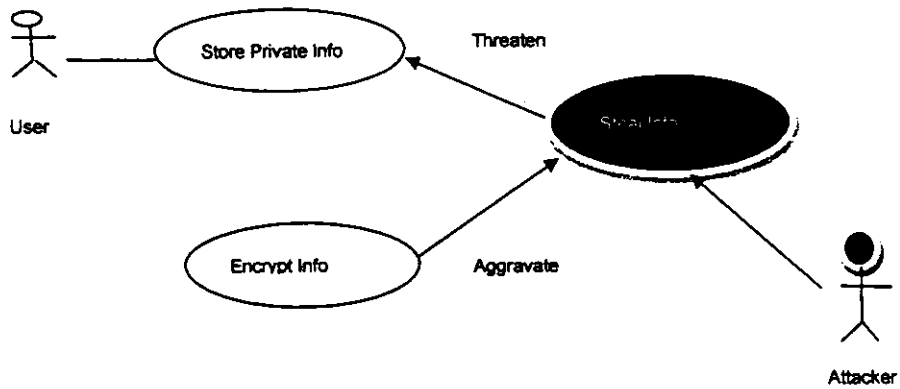
(2) Misuser:

"Misuser An actor that initiates Misuse cases, either intentionally or inadvertently"

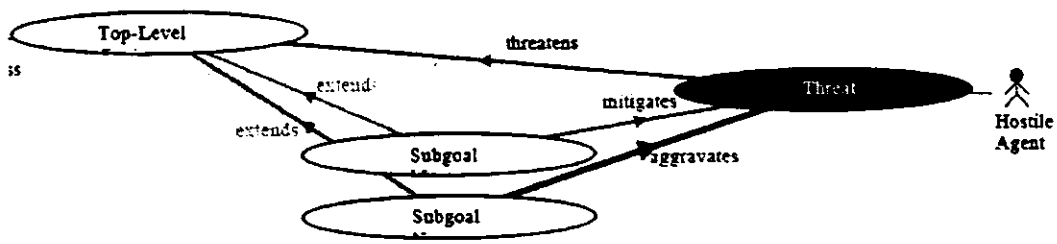


3. Grammar:

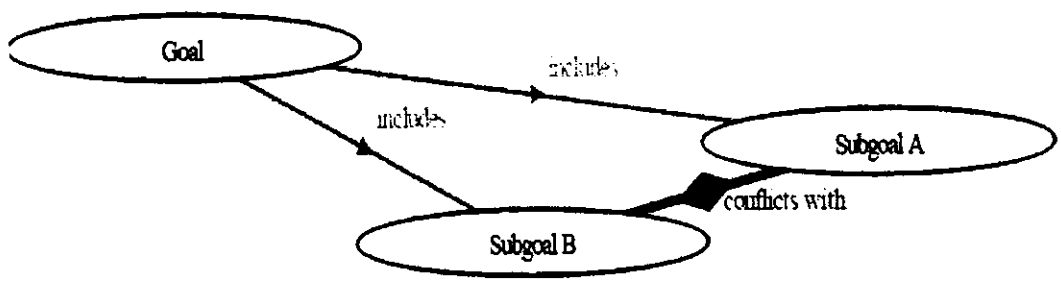
- **Include**: may or may not be used/ its optional
- **Extend**: must be used in order to complete the functionality
- **Threaten:** Misuse case threatens use case: The use case is exploited or hindered by a Misuse case. For example, the "register customer" use case is threatened by a denial-of-service attack, "flood system", that prevents legitimate users from accessing internet services, including customer registration.
- **Mitigate**: Security Use case mitigates Misuse case: The security use case is a countermeasure against a Misuse case, i.e., the use case reduces the Misuse case's chance of succeeding. An example is "protect info", which mitigates "steal credit card info", as shown in the following figure.



- **Aggravate:** Use or Misuse Case A 'aggravates' Misuse Case B if it increases either the probability of success or the seriousness of the damage that B threatens. The target of 'aggravates' is always a Misuse Case, as the relationship inherently implies that something negative is being reinforced. Where the source of 'aggravates' is a Use Case, the meaning is that a desired goal unintentionally causes an undesired side-effect.



- **Conflict With:** Use Case A 'conflicts with' Use Case B if achieving A's goal makes achieving B's goal more difficult (or impossible), and vice versa for B's effect on A. Both ends of a 'conflicts with' relationship are always Use Cases, as the relationship inherently implies that something desirable is being contradicted. In fact, 'conflicts with' is a mutual, bi-directional relationship.



Steps to be Followed:

1. First identify actors (representing user classes) and build a comprehensive set of use cases as usual.

2. For each use case, brainstorm and identify how 'negative' agents would attempt to defeat its purpose or thwart some of the steps in the use case description; this leads to the major Misuse cases. During the brainstorm sessions the focus should be to identify as many ways an attacker could cause harm in the service provided by the use case in focus; details of such attacks may be determined later. Each of these modes of attacks becomes a candidate Misuse case.

The goal is to identify security threats against each of the functions, areas, processes, data, and transactions involved in the use case from different potential risks such as unauthorized access from within and without, denial of service attacks, privacy violations, confidentiality and integrity violations, and malicious hacking attacks.

In addition to modes of attacks, the process should also try to uncover possible user Mistakes and the system responses to them. Often these Mistakes could cause serious issues in the functioning or security of the system. By identifying all inappropriate actions that could be taken, we would capture all actions of abnormal system use—by genuine users in terms of accidental or careless Mistakes and by attackers trying to break or harm the system function.

3. Show the relationships between each use case and the corresponding Misuse cases in a diagram.

4. After the Misuse cases have been constructed, identify security use cases to counter or thwart the intended purpose of each Misuse case.

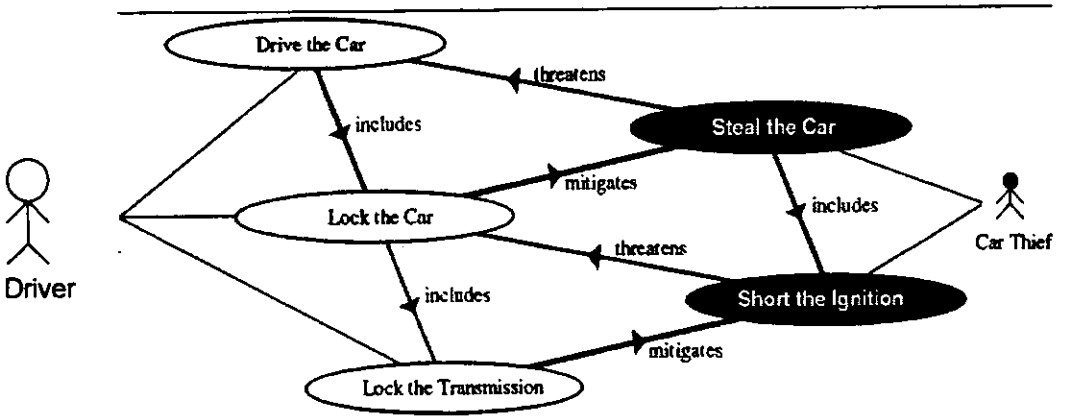
5. Continue steps (2) through (4) for each major use case until one is satisfied that

(a) All reasonable threats to the basic functionality and services of the system (as represented by the use case model) are identified and represented as Misuse cases

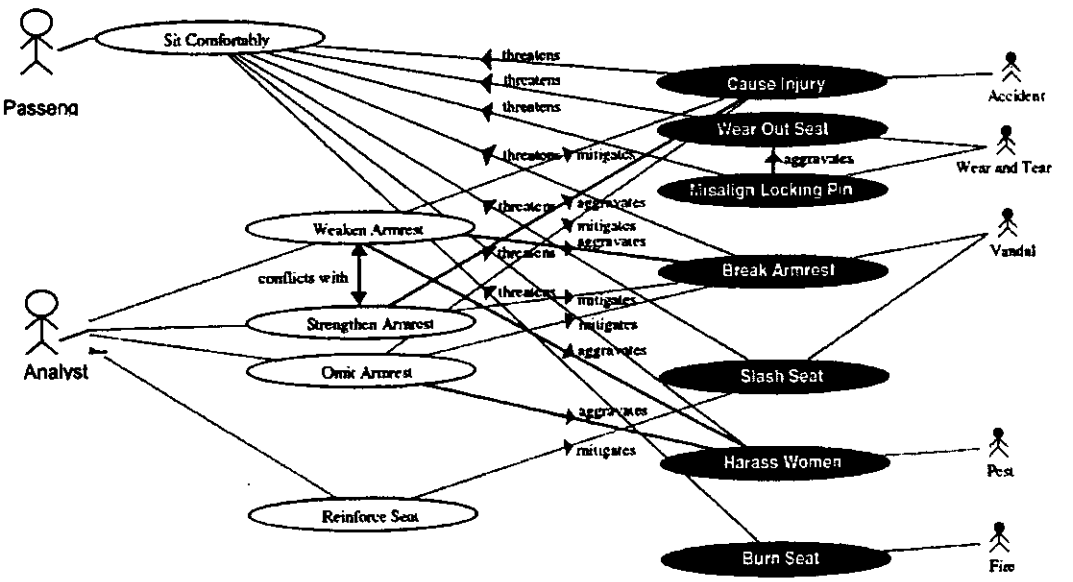
and

(b) Each of these threats has been thwarted by one or more newly introduced "security use cases."

Example 1



Example 2



Appendix G: Tutorial about IBIS

Contents of IBIS are based on (Nancy, 2006a; Jeff, 2008; Jeff, 2003; Kailash, 2009b; Kailash, 2009c; Kailash 2009a) Original contents are rearranged & reorganized to make the tutorial in a logical flow.

1. Introduction

Issue based information system (IBIS) introduced in 1970, is a requirement elicitation technique use visual notation and well defined grammar rules. It is believed to be a useful way to address issues that arise on complex projects, particularly those involving stakeholders with diverse point of view.

Basically, IBIS is "Questioning and Arguing" based approach. It presents a graphical network that integrates many problems, solutions and point of views and shows the big picture of the problem.

2. Structural Elements

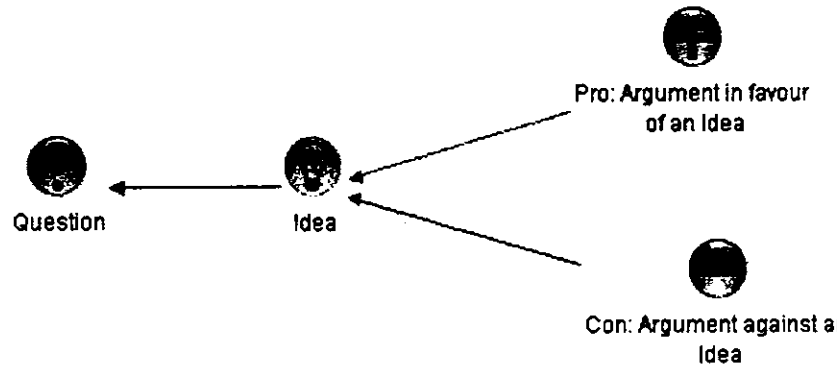
"IBIS is based on the idea that "wicked problems" – or any controversial issue – can be understood by discussing them in terms of three essential elements: *issues* (or questions), *ideas* (or answers) and *arguments* (for or against ideas)."

The Elements are:

Question: an *issue* that's being discussed or analyzed. Note that the term "question" is synonymous with "issue". Different types of questions may be asked e.g. what is the problem?, What is the problem background?, What should we do to solve the problems?, How should we achieve our aim?, What do you mean by X? Meaning or conceptual questions – Who are the stakeholders on this project?, Basically WH questions – what, why, how, who, when.

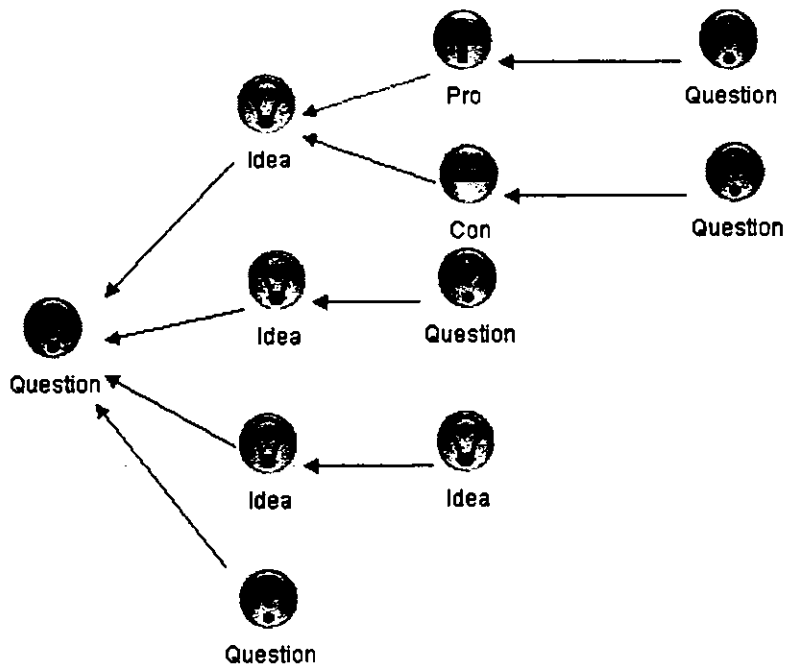
Idea: a response to a question. An idea responds to a question in the sense that it offers a potential resolution or clarification of the question.

Argument: an argument in favor of or against an idea (a pro or a con)



4. Grammar

The IBIS grammar specifies the legal ways in which elements can be linked. The arrows show links or relationships between elements. The rules are nicely summarized in the following diagram:



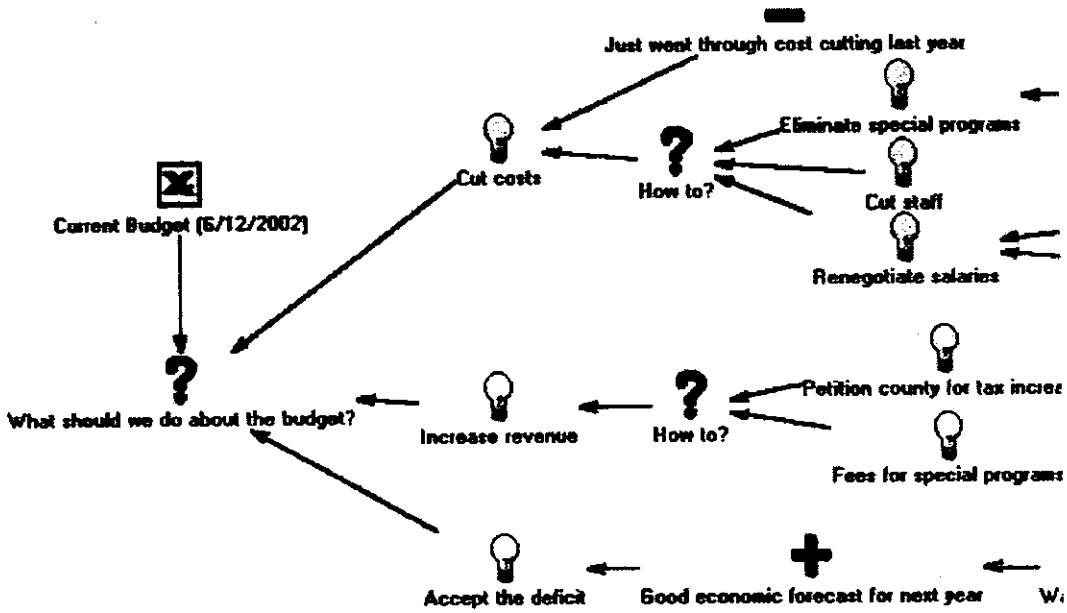
In a nutshell rules are:

- Any element (question, idea or argument) can be questioned.
- Ideas respond to questions.
- Arguments make the case for and against ideas.
- Ideas can be derived from other ideas

Natural steps along the way include:

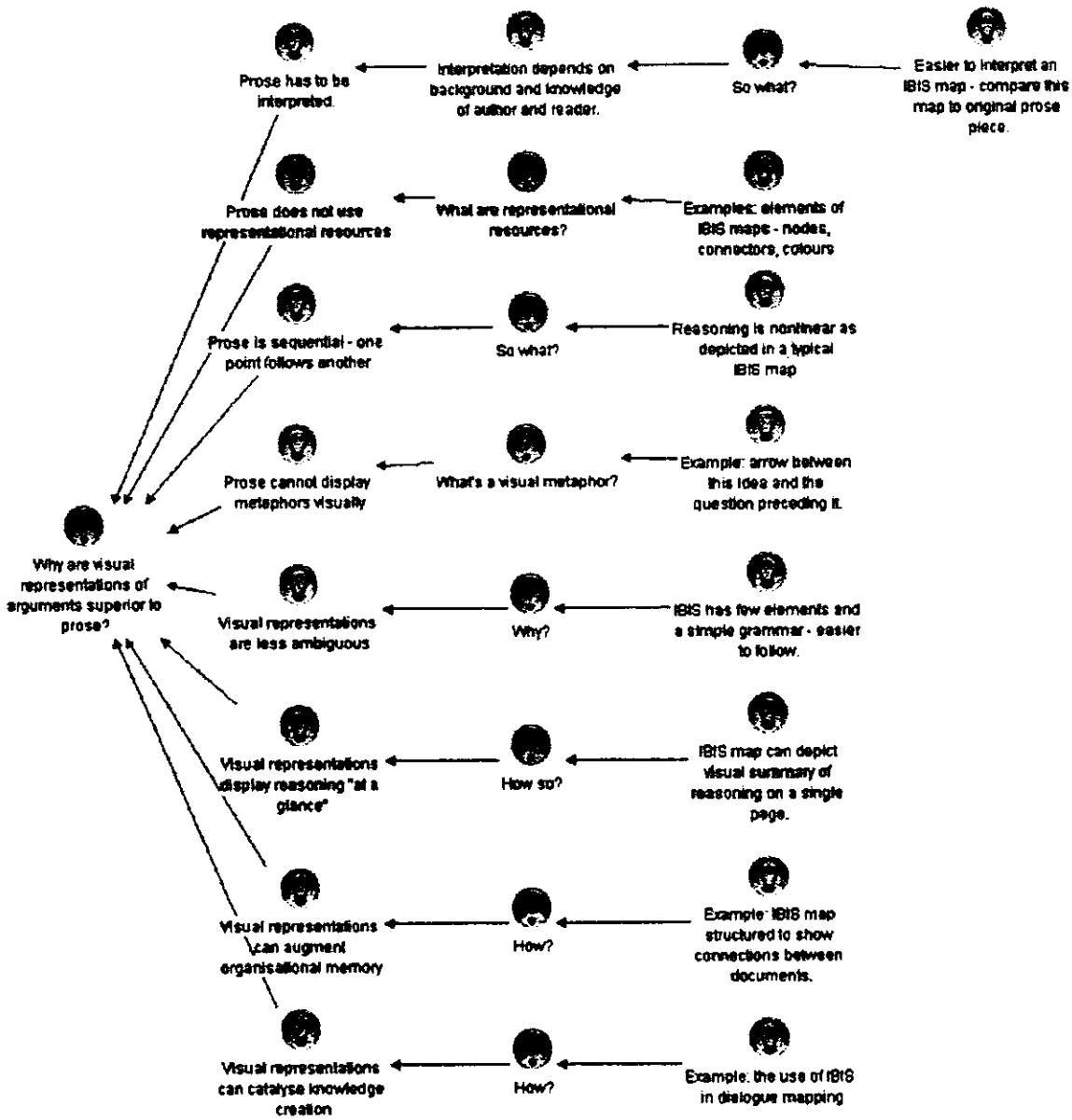
1. Consider "system security: as a problem
2. Understand presented artifacts.
3. Try to interpret presented artifacts in IBIS context – issues (Questions), ideas (or answers) and arguments (for or against ideas).
   a) Formulated a set of questions that would likely cover every aspect of security that could affect the system. Try to come up with any and all questions that would cover confidentiality, availability, and integrity aspects of the system.
      a. Develop list of questions to cover vulnerabilities and threats to system. Also raise questions about essential assets (data, function) of the system that need security e.g. what data need confidentiality?, which functions must have ability to be recovered after attacks.
      b. Identify ideas / answers of these questions & arguments in favor of or against the ideas from the presented artifacts.
   4. Develop IBIS diagram by mapping these reference material.
   5. Critically analyze the issue map and its structural elements, visualize all view points, absorb the whole scenarios and then identify security goals.
   6. Write down security goals on a paper

Example .1:



A school board faced a budget shortfall

Example 2



Prose = writing, written documentation, text base technique

Appendix H. Hypothesis

Hypothesis for comparing MUS and IBIS in three different situations, in terms of no of goals, no of types, technique learning time, execution time, result interpretation time.

Hypothesis Statements for Situation of Low Level of Detail:

H0 = there is no significance difference in number of goals identified using MUC and IBIS, in situation of low level of detail

H1= there is a significance difference in number of goals identified using MUC and IBIS, in situation of low level of detail

H2= MUC is greater than IBIS, in terms of number of goals identified in situation of low level of detail

H3= IBIS is greater than MUC, in terms of number of goals identified in situation of low level of detail

(List 1): Hypothesis for comparing MUC and IBIS regarding no of goals in situation of low level of detail

H0 = there is no significance difference in number of goal types identified using MUC and IBIS, in situation of low level of detail

H1= there is a significance difference in number of goal types identified using MUC and IBIS, in situation of low level of detail

H2= MUC is greater than IBIS, in terms of number of goal types identified in situation of low level of detail

H3= IBIS is greater than MUC, in terms of number of goal types identified in situation of low level of detail

(List2) Hypothesis for comparing MUC and IBIS regarding no of goal types in situation of low level of detail

H0 = there is no significance difference in learning time using MUC and IBIS, in situation of low level of detail

H1= there is a significance difference in learning time using MUC and IBIS, in situation of low level of detail

H2= MUC is greater than IBIS, in terms of taking less learning time in situation of low level of detail

H3= IBIS is greater than MUC, in terms taking less learning time in situation of low level of detail

(List 3): Hypothesis for comparing MUC and IBIS regarding learning time utilization, in situation of low level of detail

H0 = there is no significance difference in technique execution time using MUC and IBIS, in situation of low level of detail

H1= there is a significance difference in technique execution time using MUC and IBIS, in situation of low level of detail

H2= MUC is greater than IBIS, in terms of taking less execution time in situation of low level of detail

H3= IBIS is greater than MUC, in terms taking less execution time in situation of low level of detail

(List 4): Hypothesis for comparing MUC and IBIS regarding execution time utilization, in situation of low level of detail

H0 = there is no significance difference in technique result interpretation time using MUC and IBIS, in situation of low level of detail

H1= there is a significance difference in technique result interpretation time using MUC and IBIS, in situation of low level of detail

H2= MUC is greater than IBIS, in terms of taking less result interpretation time in situation of low level of detail

H3= IBIS is greater than MUC, in terms taking less result interpretation on time in situation of low level of detail

(List 5): Hypothesis for comparing MUC and IBIS regarding result interpretation time utilization, in situation of low level of detail

Hypothesis Statements for Situation of Medium Level of Detail:

H0 = there is no significance difference in number of goals identified using MUC and IBIS, in situation of medium level of detail

H1= there is a significance difference in number of goals identified using MUC and IBIS, in situation of medium level of detail

H2= MUC is greater than IBIS, in terms of number of goals identified in situation of medium level of detail

H3= IBIS is greater than MUC, in terms of number of goals identified in situation of medium level of detail

(List 6): Hypothesis for comparing MUC and IBIS regarding no of goals in situation of medium level of detail

H0 = there is no significance difference in number of goal types identified using MUC and IBIS, in situation of medium level of detail

H1= there is a significance difference in number of goal types identified using MUC and IBIS, in situation of medium level of detail

H2= MUC is greater than IBIS, in terms of number of goal types identified in situation of medium level of detail

H3= IBIS is greater than MUC, in terms of number of goal types identified in situation of medium level of detail

(List 7): Hypothesis for comparing MUC and IBIS regarding no of goal types in situation of medium level of detail

H0 = there is no significance difference in learning time using MUC and IBIS, in situation of medium level of detail

H1= there is a significance difference in learning time using MUC and IBIS, in situation of medium level of detail

H2= MUC is greater than IBIS, in terms of taking less learning time situation of medium level of detail

H3= IBIS is greater than MUC, in terms taking less learning time in situation of medium level of detail

(List 8): Hypothesis for comparing MUC and IBIS regarding learning time utilization in situation of medium level of detail

H0 = there is no significance difference in technique execution time using MUC and IBIS, in situation of medium level of detail

H1= there is a significance difference in technique execution time using MUC and IBIS, in situation of medium level of detail

H2= MUC is greater than IBIS, in terms of taking less execution time situation no2

H3= IBIS is greater than MUC, in terms taking less execution time in situation of medium level of detail

(List 9): Hypothesis for comparing MUC and IBIS regarding execution time utilization in situation of medium level of detail

H0 = there is no significance difference in technique result interpretation time using MUC and IBIS, in situation of medium level of detail

H1= there is a significance difference in technique result interpretation time using MUC and IBIS, in situation of medium level of detail

H2= MUC is greater than IBIS, in terms of taking less result interpretation time situation of medium level of detail

H3= IBIS is greater than MUC, in terms taking less result interpretation on time in situation of medium level of detail

(List 10): Hypothesis for comparing MUC and IBIS regarding result interpretation time utilization ,in situation of medium level of detail

Hypothesis Statements for Situation of High Level of Detail

H0 = there is no significance difference in number of goals identified using MUC and IBIS, in situation of high level of detail

H1= there is a significance difference in number of goals identified using MUC and IBIS, in situation of high level of detail

H2= MUC is greater than IBIS, in terms of number of goals identified in situation of high level of detail

H3= IBIS is greater than MUC, in terms of number of goals identified in situation of high level of detail

(List 11): Hypothesis for comparing MUC and IBIS regarding no of goals in situation of high level of detail

H0 = there is no significance difference in number of goal types identified using MUC and IBIS, in situation of high level of detail

H1= there is a significance difference in number of goal types identified using MUC and IBIS, in situation of high level of detail

H2= MUC is greater than IBIS, in terms of number of goal types identified in situation of high level of detail

H3= IBIS is greater than MUC, in terms of number of goal types identified in situation of high level of detail

(List 12): Hypothesis for comparing MUC and IBIS regarding no of goal types in situation of high level of detail

H0 = there is no significance difference in learning time using MUC and IBIS, in situation of high level of detail

H1= there is a significance difference in learning time using MUC and IBIS, in situation of high level of detail

H2= MUC is greater than IBIS, in terms of taking less learning time situation of high level of detail

H3= IBIS is greater than MUC, in terms taking less learning time in situation of high level of detail

(List 13): Hypothesis for comparing MUC and IBIS regarding learning time utilization in situation of high level of detail

H0 = there is no significance difference in technique execution time using MUC and IBIS, in situation of high level of detail

H1= there is a significance difference in technique execution time using MUC and IBIS, in situation of high level of detail

H2= MUC is greater than IBIS, in terms of taking less execution time situation of high level of detail

H3= IBIS is greater than MUC, in terms taking less execution time in situation of high level of detail

List (14): Hypothesis for comparing MUC and IBIS regarding execution time utilization in situation of high level of detail

H0 = there is no significance difference in technique result interpretation time using MUC and IBIS, in situation of high level of detail

H1= there is a significance difference in technique result interpretation time using MUC and IBIS, in situation of high level of detail

H2= MUC is greater than IBIS, in terms of taking less result interpretation time situation of high level of detail

H3= IBIS is greater than MUC, in terms taking less result interpretation time in situation of high level of detail

(List 15): Hypothesis for comparing MUC and IBIS regarding result interpretation time utilization in situation of high level of detail

Appendix I: Experimental Procedure

Research Procedure

Experiment was performed in 2 consecutive sessions, on 10 Feb 2011 in university lab no 25 the total expected time for each session was around 4 hours. As we are interested to investigate performance based measures in this experiment, where time calculations are important part of performance based measured. So we did time stamps for each activity of this experiment.

First session started at 8:44 AM. 15 subjects participated in this session. They were randomly assigned to 3 groups of 5 subjects each and be seated with reasonable distance so no one can see each others sheet. 2 invigilators were also appointed to make check on participants so they can not be able to cheat. In this session the order of the technique execution was MUC – IBIS but each group was presented from 3 different situations – situation of low level of detail, situation of medium level of detail, situation of high level of detail respectively.

- At, 8:44 all 3 groups were presented an introductory presentation of security requirements as described in appendix A. The notion of this presentation was make participants familiar with the context of security and security requirement elicitation process.
- At 9'o clock, all three groups were given situation based scenarios to read and understand it. For instance Group A was given situation of low level of detail s, Group C was given situation of medium level of detail and Group E was given situation of high level of detail. They had 30 min to read these situation based scenario description. On 9:30 they were asked to get ready for next activity.

1. At 9:37 technique introduction (MUC) was carried out in form of multimedia presentation. Total expected time for this introduction was 20

minute. During presentation Question of participants were also entertained. This presentation took 13 min to be completed.

2. At 9:50 a learning task description was provided to all groups and asked them first to read it for 10 minutes. Then, at 9:56 they were given 15 minutes to make MUC diagram as draft note to assure that they have learned the technique and able to apply it for situation specific task scenario. Time stamps were noted for individual participant on their sheets as they completed this activity. These sheets were collected from all participants. Time spent for technique presentation and development of diagram for learning activity are recorded as learning time of MUC for each individual participant.

3. At 10:16 all 3 groups are asked to consider situation specific scenario and develop MUC diagram in context of scenario given to them. For instance group A – situation no1 scenario, group C situation of medium level of detail scenario, Group E situation of high level of detail scenario. Total expected time for this activity was 30 min and time stamps for each individual participant was recorded by them on their sheet with start time and end time.

4. At 10:51 participants were asked to start next activity that result interpretation form diagram. they were asked to analyze the diagram, indentify security goals and note them in plain language on blank sheet.

Total expected time for this activity was 30 min where this activity ended at 11:10.

.....end first part of first session at 11:15.....

Participants were asked to take 15 min break, but they took only 5 min and all groups were mutually agreed to start 2nd part of the first session.

1. So the 2nd part was started at 11:20 with an introductory presentation of IBIS. The questions regarding IBIS were also entertained during the presentation. Total expected time for this activity was 20 min and it took 15 min to be completed.
2. At 11:37 all 3 group were asked to consider learning task scenario and develop IBIS diagram as draft to make sure that they have learned the IBIS and able to use it. Total expected time for this activity was 15 min, individual time stamps were recorded on participant's sheet as start and end time of activity.
3. At 11:59, all 3 groups were asked to consider situation specific scenario and develop IBIS diagram in context of scenario given to them, for instance group A – situation of low level of detail, group C situation of medium level of detail scenario, Group E situation of high level of detail scenario. Total expected time for this activity was 30 and time stamps for each individual participant was recorded by them on their sheet with start time and end time.
4. At 12:17, all 3 groups were asked to start next activity that is result interpretation form diagram. They were asked to analyze the diagram, indentify security goals and note them in plain language on blank sheet.

Total expected time for this activity was 30 min and time stamps for each individual participant was recorded by them on their sheet with start time and end time.

.....end 2nd part of first session at 12:34.....

Second session started at 1:15. 15 subjects participated in this session. They were randomly assigned to 3 groups of 5 subjects each and be seated with reasonable distance so no one can see each others sheet. 2 invigilators were also appointed to make check on participants so they can not be able to cheat. In this session the order of the technique execution was IBIS - MUC but each group was presented from 3 different situations – situation of low level of detail, situation of medium level of detail, situation of high level of detail respectively.

- At, 1:12 all 3 groups were presented an introductory presentation of security requirements (appendix A). The notion of this presentation was make participants familiar with the context of security and security requirement
- At 1:28, all three groups were given situation based scenarios to read and understand it, for instance Group B was given situation of low level of detail scenario, Group D was given situation of medium level of detail scenario and Group F was given situation of high level of detail scenario. They had 30 min to read these situation based scenario description. At 1:58 they were asked to get ready for next activity.
    1. At 2:00 technique introduction (IBIS) was carried out in form of multimedia presentation. Total expected time for this introduction was 20 minute. During presentation Question of participants were also entertained. This presentation took 18 min to be completed.

2. At 2:20 a learning task description was provided to all groups and asked them first to read it for 10 minutes. Then, at 2:30 they were given 15 minutes to make IBIS diagram as draft note to assure that they have learned the technique and able to apply it for situation specific task scenario. Time stamps were noted for individual participant on their sheets as they completed this activity. These sheets were collected from all participants. Time spent for Step 2 and 3 are recorded as learning time of IBIS for each individual participant.
3. At 2:52 all 3 groups are asked to consider situation specific scenario and develop IBIS diagram in context of scenario given to them. For instance group **B** – situation no1 scenario, group D situation of medium level of detail scenario, Group F situation of high level of detail scenario. Total expected time for this activity was 30 min and time stamps for each individual participant was recorded by them on their sheet with start time and end time.
4. At 3:23 participants were asked to start next activity, that is result interpretation form diagram. They were asked to analyze the diagram, indentify security goals and note them in plain language on blank sheet. Total expected time for this activity was 30 min where this activity ended at 3:37.

.....end first part of second session at 3:42.....

Participants were asked to take 15 min break, but they refused to take break instead they asked to start 2nd part right away

1. So the 2nd part was started at 3:42 with an introductory presentation of MUC. The questions regarding MUC were also entertained during the presentation. Total expected time for this activity was 20 min and it took 13 min to be completed.
2. At 3:58 all 3 group were asked to consider learning task scenario and develop MUC diagram as draft to make sure that they have learned the MUC and able to use it. Total expected time for this activity was 15 min. and individual time stamps were recorded on participant's sheet as start and end time of activity.
3. At 4:24, all 3 groups were asked to consider situation specific scenario and develop MUC diagram in context of scenario given to them For instance group B – situation of low, group D situation of medium level of detail scenario, Group E situation of high level of detail scenario. Total expected time for this activity was 30 and time stamps for each individual participant was recorded by them on their sheet with start time and end time.
4. At 4:51, all 3 groups were asked to start next activity that is result interpretation form diagram. They were asked to analyze the diagram, indentify security goals and note them in plain language on blank sheet. Total expected time for this activity was 30 min and time stamps for each individual participant was recorded by them on their sheet with start time and end time.

.....end 2nd part of second session at 5:14.....

REFERENCES

(Ambrosio et al, 2002) Ambrosio Toval, Joaquin Nicolas, Begona, Moros, Fernando Garcia; "Requirement Reuse for Improving Information System Security: A Practitioner's Approach" CiteSeerx 2002.

(Anders et al, 2007) Anders Herrmann, Daniel Kerkow, Joerg Doerr; "Exploring the Characteristics of NFR Methods – A Dialogue About Two Approaches" Springer 2007.

(Andreas &Guttorm, 2008) Andreas L. Opdahl and Guttorm Sindre; "Experimental Comparison of Attack Trees and Misuse Cases for Security Threat Identification" Science Direct 2008.

(Andy, 2005) Andy Field; "Discovering Statistics Using SPSS (Introducing Statistical Methods S)" Second Edition, Sage Publication Ltd 2005.

(Annie & Julia 2000) Annie I. Antón, Julia B. Earp; "Strategies for Developing Policies and Requirements for Secure Electronic Commerce Systems" ACM 2000.

(Antonio et al, 2006) Antonio de Padua A, Oliveria, Luiz Marcio Cyneiros; "Defining Strategic Dependency Situations in Requirement Elicitation" http://www.math.yorku.ca/~cysneiro/articl... 2006.

(Axel, 2001) Axel Van Lamsweerde; "Goal Oriented Requirement Engineering: A Guided Tour" IEEExplore digital library 2001.

(Axel & Emmanuel, 2000) Axel Van Lamsweerde, Emmanuel Leiter; "Handling Obstascles in Goal Oriented Requirement Engineering" IEEExplore Digital Library 2000.

(Axel, 2007) Axel van Lamsweerde "Engineering Requirements for System Reliability and Security"

(Axel, 2004) Axel Van Lamsweerds; "Elaborating Security Requirements by Construction of Intentional Anti Models" ACM 2004.

(Axelle &Makan, 2005) Axelle Apvrille & Makan Pourzandi; "Secure Software Development by Example" IEEE Security & Privacy 2005.

(Benjamin et al, 2009) Benjamin Fabian, Seda Gurses, Maritta Heisel, Thomas Santen, Holger Schmidt; "A Comparison of Security Requirements Engineering Methods" Springer 2009.

(Betty & Joanne, 2007) Betty H.C. Cheng, Joanne M. Atlee; "Research Directions in Requirements Engineering" IEEExplore Digital Library 2007.

(Charles et al, 2004a) Charles B.Haley, Robin C.Laney, Bashar Nuseibeh; "Deriving Security Requirements from Crosscutting Threat Descriptions" ACM 2004.

(Charles et al, 2004b) Charles B. Haley, Robin C. Lang, Jonathan C. Moffat, Basher Nuseibeh; "The Effect of Trust Assumption on Elaboration of Security Requirements" IEEE Computer Society 2004.

(Charles et al, 2006) Charles B.Haley, Robin C.Laney, Bashar Nuseibeh, Jonathan D. Moffetoul; "A Framework for Security Requirement Engineering" ACM 2006.

(Cynthia, 2002) Cynthia E. Irvine, Timothy Levin, Jeffery D. Wilson, David Shifflett, Babra Pereira; "An approach for Security Requirement Engineering for a High Assurance System" Springer 2002

(Daniel et al, 2006) Daniel Mellado, Eduardo Fernandez Medina, Mario Piattini; "A Comparative Study of Proposals for Establishing Security

Requirements for the Development of Secure Information System" Springer 2006.

(Donald, 2003a) Donald G. Firesmith; "Common Concepts Underlying Safety, Security, and Survivability Engineering" SEI 2003.

(Donald, 2003b) Donald G.Firesmith; "Engineering Security Requirements" Journal of Object Technology http://www.jot.fm/issues/issue_2003_01/column62003.

(Eduardo, 2004) Eduardo B. Fernandez, "A Methodology for Secure Soft-ware Design" CiteSeerx 2004.

(Emmanuel & Axel, 2002) Emmanuel Letier & Axel van Lamsweerde; "Agent-Based Tactics for Goal-Oriented Requirements Elaboration" ACM 2002.

(Gary et al, 2002) Gary Stoneburner, Alice Goguen1, Alexis Feringa; "NIST Special Publication 800-30-Risk Management Guide for Information Technology Systems" National Institute of Standards and Technology 2002.

(Guttorm &Andreas, 2000) Guttorm Sindre and Andreas L, Opdahl; "Eliciting Security Requirements by Misuse Cases" IEEE 2000.

(Gunner, 2004) Gunnar Peterson; "Collaboration in a Secure Development Process Part 1" http://arctecgroup.net/ISB0905GP.pdf. 2004.

(Gustav et al, 2006) Gustav Boström, Jaana Wäyrynen Marine Bodén; "Extending XP Practices to Support Security Requirements Engineering" ACM 2006.

(Ian 2002a) Ian Alexander; "Modelling the Interplay of Conflicting Goals with Use and Misuse Cases" ACM 2002.

(Ian, 2002b) Ian Alexander; "Initial Industrial Experience of Misuse Cases in Trade-Off Analysis" IEEE Computer Society 2002.

(Ian, 2002c) Ian Alexander; "Misuse Cases: Use Cases with Hostile Intent" IEEE Computer Society, 2003.

(Inger et al, 2008) Inger Anne Tøndel, Martin Gilje Jaatun, and Per Håkon Meland; "Security Requirements for the Rest of Us: A Survey" IEEE Computer Society 2008.

(Jeff, 2008) Jeff Conklin; "Growing a Global Issue Base: An Issue-based Approach to Policy Deliberation" cognexus.org/Papers/Growing_a_Global_Issue_Base.pdf. 2008.

(Jeff, 2003) Jeff Conklin; "Dialog Mapping: Reflections on an Industrial Strength Case Study 1" Springer 2003.

(John, 2004) John Viega; "Building Security Requirements with CLASP" ACM, 2004

(Johan et al 2007) Johan Gregoire, Koen Buyens, Bart DE Win, Riccardo Scandariato, Wouter Joosen; "On the Secure Software Development process: CLASP and SDL Compared" IEEE Computer Society 2007.

(Jonathan et al, 2004) Jonathan D. Moffett, Charles B. Haley, Bashar Nuseibeh "Core Security Requirements Artefacts" Technical Report 2004/23. Department of Computing, The Open University 2004.

(Jose et al, 2008) Jose Romero Mariona, Hadar Ziv, Debra J. Richardson; "Security Requirements Engineering: A Survey" ISR Technical Report # UCI-ISR-08-2,Institute for Software Research 2008.

(Kailash 2009a) Kailash Awati; "Dialogue Mapping: a Book Review" http://eight2late.wordpress.com/category/dialogue mapping/page/2/ 2009.

(Kailash, 2009b) Kailash Awati; "The What and Whence of Issue Based InformationSystem" http://eight2late.wordpress.com/2009/07/08/the-what-and-whence-of-issue-based-information-systems/ 2009.

(Kailash, 2009c) Kailash Awati; "Capturing Project Knowledge Using Issue maps" http://eight2late.wordpress.com/2009/04/15/capturing-project-knowledge-using-issue-maps/ 2009.

(Kailash 2009d) Kailash Awaiti; "Issues, Ideas and Arguments: A Communication Centric Approach to Tackling Project Complexity" http://eight2late.wordpress.com/2009/04/07/issues-ideas-and arguments-a-communication-centric-approach-to-tackling-project-complexity/ 2009.

(Kenneth &Gary, 2005) Kenneth van Wyk and Gary McGraw; "Bridging the Gap between Software Development and Information Security" IEEE Security & Privacy 2005

(Lin, Eric & John, 2002) Lin Lui, Eric Yu, John Mylopoulos; "Analyzing Security Requirements as Relationships among Strategic Actors" CiteSeerx 2002.

(Lillian, 2005) Lillian Rosted; "An Extended Misuse Case Notation: Including Vulnerabilities and Insider Threat" CiteSeerx 2006.

(Mamadou et al, 2004) Mamadou H. Diallo, Jose Romero-Mariona, Susan Elliott sim, Debra J. Richardson; "A Comparative Evaluation of Three Approaches to Specifying Security Requirements" CiteSeerx 2006.

(Meledath, 2006) Meledath Damodaran; "Secure Software Development Using Use Cases and Misuse Case" CiteSeerx 2006.

(Michael & Steve, 2006) Michael Howard & Steve Lipner; "The Security Development Lifecycle: SDL A Process for Developing Demonstrably More Secure Software" Microsoft Press 2006.

(Nancy et al, 2005) Nancy R. Mead, Eric D. Hough, Theodore R. Stehney II; "Security Quality Requirement Engineering (SQUARE) Methodology" SEI 2005.

(Nancy, 2006a) Nancy R. Mead; "Requirements Elicitation Case Studies Using IBIS, JAD, and ARM" https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/requirements/532-BSI.html 2006.

(Nancy, 2006b) Nancy R Mead; "Experiences in Eliciting Security Requirement" The Journal of Defense Software Engineering 2006.

(Nancy et al, 2006) Lydia Chung, Frank Hung, Eric Hough, Don Ojoko-Adams Advisor Nancy R. Mead; "Security Quality Requirements Engineering (SQUARE): Case Study Phase III" SEI 2006.

(Nancy et al, 2004) "System Quality Requirement Engineering (SQUARE) Methodology Case Study on Asset Management System" SEI 2004.

(NIST, 1995) National Institute of Standards and Technology Administration U.S. Department of Commerce; "An Introduction to Computer Security: The NIST Handbook", Special Publication 800-12 1995.

(Nigel & Mike, 1989) Nigel Shadbolt & Mike Burton; "The Empirical Study of Knowledge Elicitation Techniques" ACM 1989.

(OWASP, 2006) OWASP; Comprehensive Lightweight Application Security Process. http://www.owasp.org.2006 2006

(Rudolph, 2007) Rudolph Araujo; "Security Requirements Engineering: A Road Map" http://www.softwaremag.com/focus-areas/security/featured-articles/security-requirements-engineering-a-road-map/ 2007.

(Seda et al, 2005) Seda Gurses, Jens H. Jahnke, Cristina Obry, Adeniyi Onabajo, Thomas Santen, Morgan Price; "Eliciting Confidentiality Requirements In Practice" IBM Press 2005.

(Simara et al, 2005) Simara Rocha, Zair Abdelouahab & Eduardo Freire; "Requirement Elicitation Based on Goals with Security and Privacy Policies in Electronic Commerce" CiteSeerx 2005.

(Soo Hoo et al 2001) Soo Hoo, Kevin; Sudbury, Andrew W. & Jaquith, Andrew R.; "Tangible ROI through Secure Software Engineering" Secure Business Quarterly 1, 2 2001

(Tor & Guttorm, 2008) Tor Stalhane and Guttorm Sindre "Safety Hazard Identification by Misuse Cases: Experimental Comparison of Text and Diagrams" Springer 2008.

(Umair & Zulkernine, 2009) Muhammad Umair Ahmed Khan and Mohammed Zulkernine; "On Selecting Appropriate Development Processes and Requirements Engineering Methods for Secure Software" IEEE Computer Society 2009.

(Werner & Horst, 1979) Werner Kunz and Horst W. J. Rittel; "Issues As Element of Information Systems" Working Paper No. 131 (July 1970); Studiengruppe für Systemforschung, Heidelberg, Germany (reprinted, May 1979)

(William, 2006) William M.K. Trochim; "Research Methods Knowledge Base" http://www.socialresearchmethods.net/kb/index.php