American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-02, Issue-12, pp-360-366
www.ajer.org

Research Paper Open Access

A Survey on Security Requirements Elicitation and Presentation in Requirements Engineering Phase

Md. Alamgir Kabir, Md. Mijanur Rahman
[1, 2] *(Department of Software Engineering, Daffodil International University, Bangladesh)*

Abstract: - Secure software development is the new attention of current world in recent days. Security is the key issue for assuring the quality full software. Since, security is one the non-functional requirement most of the times it is ignored in the requirements phase. But, it is possible to reduce software development cost and time to identify user security requirement in the early stage of the software development process. IT security must apply to ensure the reliable system and protect assets of the business organization. In this scene, the main deal is to present the user security requirements combining with user functional requirements which are collected form requirement phase in Software Development Life Cycle (SDLC). Secure Software Development Life Cycle (SSDLC) start from security requirements. If we can elicit user security requirements and present these requirements in requirements phase then secure software develop will be ensure from the very beginning. In industry and academic, there are several methods to elicit and analyze the user security requirements, but few methods are efficient for identifying and presenting the user security requirements. This paper reflects the current research on software user security requirements elicitation techniques in requirements engineering phase. We try to identify the research trend, based on related published work.

Keywords: - *Requirements Phase, Security Requirements Engineering, Secure Software Development Life Cycle, Security Requirements Model, Security Requirements*

I. INTRODUCTION

In the competitive economic market, the demand of secured and reliable system is increasing day by day. A successful software development is possible by considering equally both functional and nonfunctional requirements. For this issue, nonfunctional requirements are much important like functional requirements. There are few generic nonfunctional requirements for a system like auditability, extensibility, maintainability, performance, portability, reliability, security, testability, usability and etc. among them security is very vital issue for system development. If we want to develop a reliable and secure system, we have to more concern about security before developing the system that means as early stage in software development life cycle. And this will be requirements stage. In requirements stage, generally we collect user functional requirements. But if we collect user security requirements with user functional requirements then secure software development will be possible with less effort and less cost. Because if user security requirements is arranged after some development from users or stakeholders then it is more difficult, costly and matter of time to combine with user functional requirements with the product or module.

In real sense, user security requirements means the security requirements for a specific requirements or function. That means for a login system, user name or password is necessary for a successful login. But if the users or stakeholders enter wrong user name or password simultaneously and continuously then some effect will be occurred for security purpose. But the users or stakeholders can enter user name and password two or three times which is specified in requirement stage for specific requirement or function then this type of security purpose is achieved from early stage with less effort, time and cost.

Beyond this introduction on the background details, rest of the paper is organized as follows: In Section II, Security Requirements (SR) in Software Development Process is briefly reported, In Section III, Security Requirements Engineering is briefly reported, whereas in Section IV, we present Security Requirements Elicitation and Presentation Model is briefly reported. Finally, Conclusion is drawn in Section V.

II. SR IN SOFTWARE DEVELOPMENT PROCESS

Adding security requirements to a system that has already functionally developed is very difficult. The security requirements should be integrated at the requirement stage so that it can be identified with the first parts of development phase. Salim Chehida and Mustapha Kamel Rahmouni think that the development of a security policy must be done at the same time, than the functional design stage, and the final model must integrate at the same time, the functional and security specifications [26]. The security of the critical systems must start with the early stage and should follow an approach which would present: what are the threads? What do we have to protect? Why? [26]. P. Devanbu said in the book named "Software Engineering for Security: A Roadmap" that security concern must inform every phase of software development, from requirements engineering to design, implementation, testing and development [27].

Microsoft says that defining and integrating user security requirements helps make it easier to identify minimize disruptions to plans and schedules for establishing security requirements in early stage [3].
Microsoft's security development life cycle in requirement phase has three phase. These are; (a) establish security requirements, (b) create quality gates/bug bars and perform security and (c) privacy risk assessments.

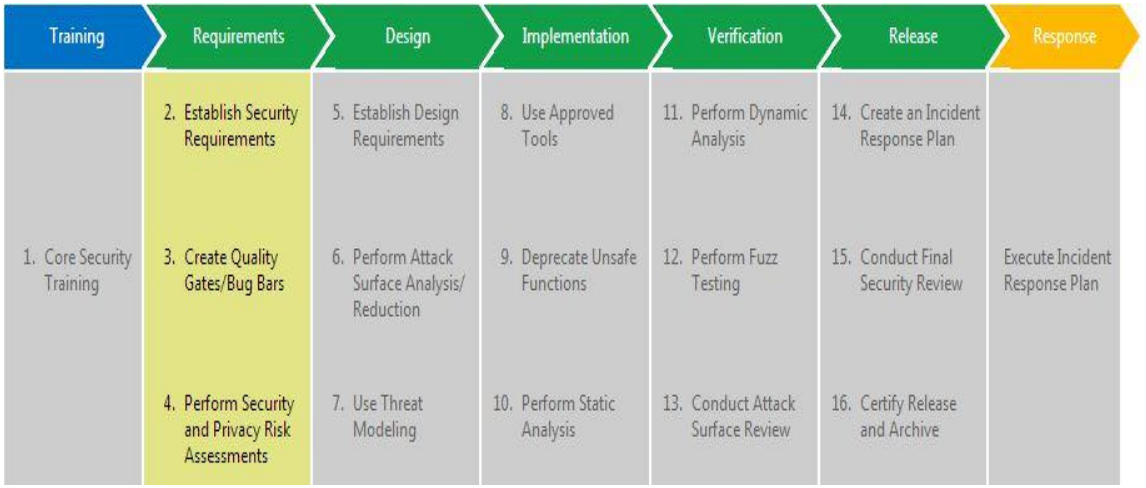

Fig 1. security development lifecycle: requirements phase

In fig 1 security requirements gets more importance in requirements phase in SDL which is developed by Microsoft. Following Microsoft description, the project inception phase is the best time for a development team to consider foundational security and privacy issues and to analyze how to align quality and regulatory requirements with costs and business needs [4].

Viega J presented in the CLASP application security process in volume 1.1 that CLASP, a plug-in to RUP, is another well-defined and structured method to consider security in the very first step of software lifecycle. CLASP fully supports UML 2.0 in the entire software development lifecycle [5].
Hence, secure software development if we want to integrate user security requirements with in user functional requirements especially in requirement analysis phase is considered as one the today's research challenges [2].

III. SECURITY REQUIREMENTS ENGINEERING

Requirements engineering is the first major stage of software development. Security requirements of requirements engineering aren't the initial interested area of most application developers. And they aren't knowledgeable about security requirements engineering. For decades, the focus has been on implementing as much functionality as possible before the deadline, and patching the inevitable bugs when it's time for the next release or hot fix [16], [17]. However, the software engineering community is slowly beginning to realize about requirements engineering that security requirements is also important for application [18].

Table 1: security requirements approaches

Serial No	Approach Name
1	Knowledge Agent-oriented System (KAOS)
2	Risk Analysis
3	Security Patterns
4	Security Design Analysis (SeDaN)
5	Abuse Cases
6	Software Cost Reduction
7	Threat Trees
8	Fault Trees
9	Problem Frames
10	Security Use Cases
11	Simple Reuse of Software Requirements (SIREN)
12	Threat Modeling for Security Requirements
13	Agile Security Requirements Engineering
14	Security Models
15	Security Development Lifecycle Tool (SDL)
16	Controlled Requirements Expression (CORE)
17	Joint Application Development (JAD)
18	Issue-based information systems (IBIS)
19	Critical discourse analysis (CDA)
20	Accelerated Requirements Method (ARM)
21	Quality Function Deployment (QFD)
22	Misuse Cases
23	Abuser Stories
24	Secure TROPOS
25	Security Problem Frames
26	Anti-models
27	i* Security Requirements
28	Common Criteria
29	System Quality Requirements Engineering (SQUARE)
30	Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
31	Attack Trees
32	Usage-centric Security Requirements Engineering (USeR)
33	Comprehensive Lightweight Application Security Process (CLASP)

Various researchers are underway on the different aspects of security requirements in requirements phase. However, a rapid growth about security requirements engineering has been visualized recently. Some significant contributions bear weight and appear valuable among all. A selection from the trend setting research contributions are briefly described one by one for analysis on the advances, as follows:

Open web application security project (OWASP) developed a cheat sheet which build requirements security into multiple parts or module of software development processes including requirement phase. It describes various policies and rule for security requirements in SDLC [7].

For identifying and measuring the requirement security and related verification method in requirements engineering (RE), Souhaib Besrour and Imran Ghani presented a paper and proposed a new set of tools. And they proposed an effective security check list of security requirements questions that should be considered for identifying and measuring security in RE phase [8].

About security requirements engineering, P. Salini and S. Kanmani published a review paper. They reviewed various methods on security requirements engineering and analyzed and compared different methods of requirements engineering [9].

Sultan Aljahdali, Jameela Bano and Nisar Hundewale published a review paper on requirement engineering which is goal oriented. This paper helps in identifying security requirements of Goal oriented requirements engineering [10]. Smriti Jain and Maya Ingle developed a model namely Software Requirement Gathering Instrument that helps to gather security requirements from the various stakeholders. The proposed model helps the developers to gather security functional requirements and incorporate security requirements with functional requirements during the requirements phases of software development [11].

The most comprehensive model for security requirements is currently the SQUARE method presented by the SEI of Carnegie Mellon University [12].

M. A. Hadavi, V. S. Hamishagi and H. M. Sangchi presented a paper about security requirements engineering. This paper focuses on the current research situation by reviewing and classifying the efforts into four main categories: security requirements in the standard software development processes, security

requirements engineering consist of eliciting and modeling security requirements and threat modeling as a basis for security requirements engineering [13].

P.salini and S.kanmani presented a paper about survey on Security Requirement Engineering (SRE). In this paper they present a view on Security Requirements, Security Requirements issues, and types, Security Requirements Engineering and methods. Comparison on different methods and trends of Security Requirements Engineering is given. With this short view information security requirements for banks and the approach that can be adopted for security requirements engineering can be easily identified by the developers [14].

Daniel Mellado, Eduardo Fern´andez-Medina, and Mario Piattini presented a paper about applying security requirements engineering process. In this paper they presented a case study of SREP (Security Requirements Engineering Process), which is a standard-centered process and a reuse based approach which deals with the security requirements at the earlier stages of software development in a systematic and intuitive way by providing a security resources repository and by integrating the Common Criteria into the software development lifecycle [15].

IV. SECURITY REQUIREMENTS ELICITATION AND PRESENTATION MODEL

Security Requirements Elicitation is the initial activity for most of the requirements engineering approaches in requirement phase that we analyzed. This phase is mainly concerned with gathering as much information as possible from a variety of stakeholders including past documentation [19].

User security requirements elicitation and presentation is the branch of software security requirements engineering concerned with the real-world goals for, security functions of user functions, and constraints on software or module. It is also associated with the user functional requirements to precise specifications of software behavior [6].

For the purposes of this review, we focus only on those approaches that proactively address the issue of security. We addressed variety of approaches that could be adapted to engineer security requirements. But we did not consider other approaches because they make no mention of security as they currently stand. Over 30 SRE approaches were originally considered [19] in Table 1.

These models are in table 1 is about security requirements model. In general, we can address and evaluate security requirements before and after development. But our main target is that we want to address security requirements before development in requirement analysis phase. In table 1, all models aren't these type of model which address security before development in requirement phase in SDLC.

M. A. Hadavi, V. S. Hamishagi, H. M. Sangchi presented a paper in Proceedings of the International Multi Conference of Engineers and Computer Scientists 2008 Vol I, IMECS 2008, 19-21 March, 2008, Hong Kong named Security Requirements Engineering: State of the Art and Research Challenges. In this paper, they described about Current research activities and methods in SR engineering [1].

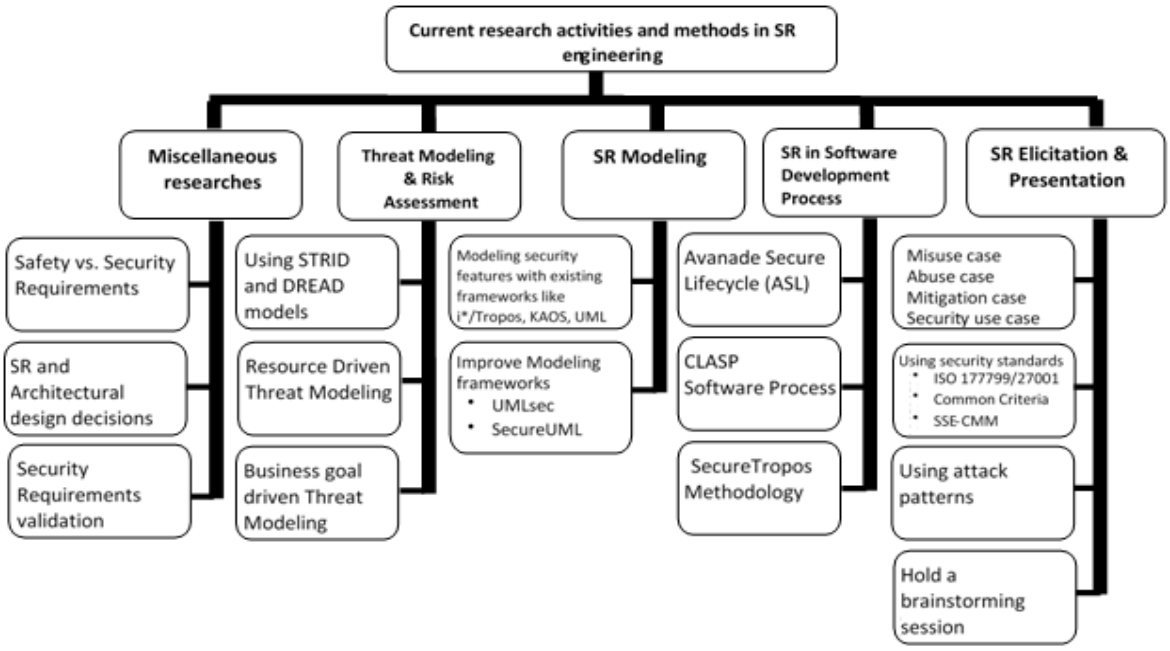

Fig.2 Categorization of research activities and current method in SR engineering

In fig. 2, security requirement approaches are divided in categories. Some approaches are for threat modelling & risk assessment, some are for software development process and some are for security requirement elicitation and presentation. We focused security elicitation and presentation approaches which are misuse case, abuse case, mitigation case, security use case, security standards, using attack patterns and hold a brainstorming session.

Researchers are undergoing on the different aspects of security requirements elicitation and presentation model in requirements phase. A selection from research contributions which are published recently and are briefly described one by one for analysis as follows and arranged in table 2:

Guttorm Sindre, Donald G. Firesmith and Andreas L. Opdahl presented a paper named a Reuse-Based Approach to Determining Security Requirements. They propose a reuse-based approach to determining security requirements. Development with reuse involves identifying security assets, setting security goals for each asset, identifying threats to each goal, analyzing risks and determining security requirements, based on reuse of generic threats and requirements from the repository [20].

Use cases are widely used for functional requirements elicitation. However, security non-functional requirements are often neglected in this requirements analysis process. Form this issue, Thitima Srivatanakul, John A. Clark, and Fiona Polack presented a paper named Effective Security Requirements Analysis: HAZOP and Use Cases. This paper takes one such technique, HAZOP, and applies it to one widely used functional requirement elicitation component, UML use cases, in order to provide systematic analysis of potential security issues at the start of system development [21].

Table 2: research contributors list

Serial No.	Writer's Names	Paper Title	Proposed Model
1	Guttorm Sindre, Donald G. Firesmith and Andreas L. Opdahl	Reuse-Based Approach to Determining Security Requirements	A reuse-based approach to determining security requirements [20].
2	Thitima Srivatanakul, John A. Clark, and Fiona Polack	Effective Security Requirements Analysis: HAZOP and Use Cases	HAZOP, and applies it to one widely used functional requirement elicitation component, UML use cases, in order to provide systematic analysis of potential security issues at the start of system development [21].
3	Guttorm Sindre and Andreas L. Opdahl	Eliciting Security Requirements with Misuse Cases	A systematic approach to eliciting security requirements based on use cases, with emphasis on description a method guidelines [22].
4	Ala A. Abdulrazeg, Norita Md Norwawi and Nurlida Basir	Security Measurement Based on GQM to Improve Application Security during Requirements Stage	A security metrics model based on the Goal Question Metric (GQM) approach, focusing on the design of the misuse case model [23].
5	Michael S. Ware, John B. Bowles and Caroline M. Eastman	Using the Common Criteria to Elicit Security Requirements with Use Cases	An approach to eliciting security requirements for IT systems with use cases using Common Criteria methodologies [24].
6	Smriti Jain and Maya Ingle	Software Security Requirements Gathering Instrument	Software Security Requirements Gathering Instrument (SSRGI) that helps gather security requirements from the various stakeholders [25].
7	Pauli, J. and Dianxiang Xu	Integrating functional and security requirements with use case decomposition	An approach to decomposing use cases, misuse cases, and mitigation use cases [28].
8	Donald Firesmith	Security Use Cases	Provides examples and guidelines for properly specifying essential (i.e., requirements-level) security use cases [29].

Guttorm Sindre and Andreas L. Opdahl presented a paper named eliciting security requirements with misuse cases. This paper, they presents a systematic approach to eliciting security requirements based on use cases, with emphasis on description an method guidelines. The approach extends traditional use cases to also cover misuse, and is potentially useful for several other types of extra-functional requirements beyond security [22].

Ala A. Abdulrazeg, Norita Md Norwawi and Nurlida Basir published a paper named Security Measurement Based on GQM to Improve Application Security during Requirements Stage. In this paper, they present a security metrics model based on the Goal Question Metric (GQM) approach, focusing on the design of the misuse case model. Misuse case is a technique to identify threats and integrate security requirements during the requirement analysis stage. The security metrics model helps in discovering and evaluating the misuse case models by ensuring a defect-free model. Here, the security metrics are based on the OWASP top 10-2010, in addition to misuse case modeling antipattern [23].

The Common Criteria is often too confusing and technical for non-security specialists to understand and therefore properly use. At the same time, it is essential that security critical IT products under development be validated according to such standards not after but rather during the software engineering process. To help address these issues, Michael S. Ware, John B. Bowles and Caroline M. Eastman published a paper named using the Common Criteria to Elicit Security Requirements with Use Cases. This paper, they presents an approach to eliciting security requirements for IT systems with use cases using Common Criteria methodologies. They focus is to ensure that security issues are considered early during requirements engineering while making the Common Criteria more readily available to end-users in an understandable context [24].

Smriti Jain and Maya Ingle published a paper named software security requirements gathering instrument in (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 7, 2011. This paper describes Software Security Requirements Gathering Instrument (SSRGI) that helps gather security requirements from the various stakeholders. This will guide the developers to gather security requirements along with the functional requirements and further incorporate security during other phases of software development. They presented case studies that described the integration of the SSRGI instrument with Software Requirements Specification (SRS) document as specified in standard IEEE 830-1998. Proposed SSRGI will support the software developers in gathering security requirements in detail during requirements gathering phase [25].

Pauli, J. and Dianxiang Xu presented a paper named Integrating functional and security requirements with use case decomposition in Engineering of Complex Computer Systems, 2006. ICECCS 2006. 11th IEEE International Conference in Stanford, CA. In this paper they proposed an approach to decomposing use cases, misuse cases, and mitigation use cases [28].

Donald Firesmith presented a paper in Journal of Object Technology, vol. 2, no. 3, May-June 2003, pp. 53-64 named Security Use Cases. This paper provides examples and guidelines for properly specifying essential (i.e., requirements-level) security use cases [29].

V. CONCLUSION

In this paper, we have discussed about security requirements engineering, security requirements in software development process and security requirements elicitation and presentation model. And here, we listed security requirements approaches of security requirements engineering. We also specified model for security requirements elicitation and presentation. This research work provides the knowledge of security requirements elicitation and presentation approaches for requirements phase in software development life cycle. These model are associated with security requirements with user functional requirements. One of the future work may be developed an elicitation and presentation method for security requirements in requirements phase. Security requirements combining techniques with functional requirements can be developed as a future work. Future task may be done to develop a security requirements testing tool that have to be more efficient to preserve security requirements for the requirements phase. A mathematical model can also be developed for evaluating security requirements in requirements analysis phase. We have also planned a model for identifying user security requirements for specific functional requirements in requirements analysis phase for secure software development.

REFERENCES

[1] M. A. Hadavi, V. S. Hamishagi, H. M. Sangchi, "*Security Requirements Engineering; State of the Art and Research Challenges*", Proceedings of the International Multi Conference of Engineers and Computer Scientists 2008 Vol I, IMECS 2008, 19-21 March, 2008, Hong Kong

[2] Paolo Giorgini, Fabio Massacci, Nicola Zannone, "*Security and Trust Requirements engineering*", Foundations for Security Analysis and Design, Lecture Notes in Computer Science, Volume 3655, Berlin: Springer, 2005.

[3] Security Development Life Cycle, Retrieved on December 6, 2013. Available at http://www.microsoft.com/security/sdl/default.aspx

[4] Security Development Life Cycle, Retrieved on December 7, 2013. Available at http://www.microsoft.com/security/sdl/process/requirements.aspx

[5] Viega J. "*The CLASP Application Security Process*". Volume 1.1. Training Manual. Secure Software Inc. 2005.

[6] D. Gollmann, J. Meier, and A. Sabelfeld, "*Applying a Security Requirements Engineering Process*" (Eds.): ESORICS 2006, LNCS 4189, pp. 192–206, 2006. Springer-Verlag Berlin Heidelberg 2006

[7] The Open Web Application Security Project (OWASP) cheat sheet in 2013. Retrieved on December, 7, 2013. https://www.owasp.org/index.php/Secure_SDLC_Cheat_ Sheet#Purpose

[8] Besrour Souhaib and Ghani Imran 2012," *Measuring Security in Requirement engineering"*International Journal of Informatics and Communication Technology (IJ-ICT) Vol.1, No.2, pp 72-81.

[9] Salini P. and Kanmani S. 2012 *"Survey and analysis on Security Requirements Engineering"*, Journal Computers and Electrical Engineering, Volume 3, Issue 6, pp 1785-1797.

[10] Aljahdali Sultan, Bano Jameela and Hundewale Nisar 2011 *"Goal Oriented Requirements Engineering - A Review"*, -1-880843-83-3/ISCA CAINE.

[11] Jain Smriti, Ingle Maya 2011 "*Software Security Requirements Gathering Instrument"*, International Journal of Advanced Computer Science and Application Vol. 2, No. 7, pp 116-121.

[12] Christian T. and Mead N. 2010. "*Security Requirements Reusability and the SQUARE Methodology"*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Note CMU/SEI2010-TN-027. Retrieved on March, 7, 2013 http://www.sei.cmu.edu/library/abstracts/reports/10tn027.cfm

[13] Hadavi M. A., Hamishagi V. S. and Sangchi H. M. 2008. *"Security requirements Engineering; State of the Art and Research Challenges"*, International MultiConference of Engineers and Computer Scientists Vol I, pp 19-21.

[14] P.salini and S.kanmani. 2011. *"A survey on security requirements engineering"*, International Journal of Review in Computing. Vol 8, pp 1-10.

[15] Daniel Mellado, Eduardo Fern´andez-Medina, and Mario Piattini. 2006. *"Applying a Security Requirements Engineering Process"*. ESORICS 2006, LNCS 4189, pp 192-206 at Springer- Verlag Berlin Heidelberg.

[16] P. Coffee, "*Security Onus Is on Developers*," *eWeek*, 7 December 2013, www.eweek.com/article2/0,1895,1972593,00.asp

[17] H. Mouratidis, P. Giorgini, and G. Manson, "*When Security Meets Software Engineering: A Case of Modeling Secure Information Systems*," *Information Systems*, vol. 30, no. 8, 2005, pp. 609–629.

[18] J.D. Meier, "*Web Application Security Engineering*," *IEEE Security & Privacy*, vol. 4, no. 4, 2006, pp. 16–24

[19] Jose Romero-Mariona, Hadar Ziv, Debra J. Richardson, *"Security Requirements Engineering: A survey"*, August 2008, ISR Technical Report # UCI-ISR-08-2

[20] Guttorm Sindre, Donald G. Firesmith and Andreas L. Opdahl, "*A Reuse-Based Approach to Determining Security Requirements*".

[21] Thitima Srivatanakul , John A. Clark, and Fiona Polack, *"Effective Security Requirements Analysis: HAZOP and Use Cases"*. K. Zhang and Y. Zheng (Eds.): ISC 2004, LNCS 3225, pp. 416–427, 2004. At Springer-Verlag Berlin Heidelberg 2004

[22] Guttorm Sindre, Andreas L. Opdahl, *"Eliciting security requirements with misuse cases"*. Received: 15 February 2002 / Accepted: 5 March 2004 / Published online: 24 June 2004 at Springer-Verlag London Limited 2004

[23] Ala A. Abdulrazeg, Norita Md Norwawi and Nurlida Basir," *Security Measurement Based on GQM to Improve Application Security during Requirements Stage*", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 211-220, the Society of Digital Information and Wireless Communications (SDIWC) 2012 (ISSN: 2305-0012)

[24] Michael S. Ware, John B. Bowles and Caroline M. Eastman, "*Using the Common Criteria to Elicit Security Requirements with Use Cases*".

[25] Smriti Jain and Maya Ingle, "*Software Security Requirements Gathering Instrument*", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 7, 2011.

[26] Salim Chehida and Mustapha Kamel Rahmouni, "*Security Requirements Analysis of Web Applications using UML*", Proceedings ICWIT 2012.

[27] P. Devenbu, "*Software Engineering for Security: A Roadmap*", 2000.

[28] Pauli, J. and Dianxiang Xu, "*Integrating functional and security requirements with use case decomposition*", Engineering of Complex Computer Systems, 2006. ICECCS 2006. 11th IEEE International Conference in Stanford, CA

[29] Donald Firesmith: "*Security Use Cases*", in *Journal of Object Technology*, vol. 2, no. 3, May-June 2003, pp. 53-64. http://www.jot.fm/issues/issue_2003_05/column6