ISSN:0975-9646

Enhancing Security in Software Development Life Cycle

Chandana Das, Pardeep Kumar Sharma

CSE, Lovely Professional University,Punjab.

Abstract:-Computer system facing security attack. To handle proper security in a software we must consider the security requirements early in the software development life cycle. In this decade there are various techniques exist for proper security requirements during the early phases of Software Development Life Cycle (SDLC) there are .In this paper we are introducing a new methodology which is extend form of VOSREP methodology. In the propose methodology we are measuring the quality of security which is provided by VOSREP by using Security Quality Requirements Engineering (SQUARE) methodology. According to the result of the quality of security we enhancing more security in this propose methodology.

INTRODUCTION

In the recent years security incidents have broken all barriers. System is attacked by virus, malicious crackers and various other threats of cyber terrorism .So every system should have safety, reliability and other quality features otherwise the systems may not be acceptable as one cannot depend on them. Security needs to be considered from the beginning of software development life cycle to avoid expensive[1]. This has awakened venders and researchers to think
seriously about its countermeasures. Integrating security within the development life cycle has been proven to be the most effective way to develop secure software. Now a day Security requirements engineering is used more frequently in software development. Security requirements engineering provides a structured approach to defining a set of supportable security requirements in the early stages of software development.

EXISTING CONCEPT

VOSREP-- View Point Oriented Requirement Definition
The VOSREP process defined is well embedded in VORD process making security engineering a unified approach with requirement engineering. VOSREP deal with security requirements as we deal with other functional and non – functional requirements [3]. The VOSREP process is to elicit, analyze, prioritize and manage security requirements.

Activity of VOSREP

The different activities in the VOSREP are as follows: -

i. Security Requirements Discovery and Definition
   In is the first activity of the VOSREP process the security requirements along with functional and non functional requirements are discovered and defined for the system to be developed. In VOSREP we extend the conventional VORD process for requirement engineering so that we can elicit the corresponding security requirements [3].
ii. Analysis and Prioritization of Security Requirement
   In the second activity the various security requirements are analyze which are discovered in the first activity for their completeness, Consistency, Unambiguousness, Feasibility etc. Once the security requirements are analyzed the corresponding security requirements are prioritized based on the measure of risk of threat on an asset [3].
iii. Management of Security Requirements
   Once the security requirements are discovered, analyzed, prioritized the next activity is to manage them. This is very important activity of the security engineering[3].

REQUIREMENTS ENGINEERING

Requirement engineering is the process of establishing the functional requirements that the customer requires from a system and the constraints under which is developed it operates and[2].
The different types of requirement are as follows:-.

i. Functional Requirements
   A functional requirement specifies a function that a system or component must be able to perform. Functional requirements may vary depending on the type of software[3].
ii. Non Functional Requirements
   A non-functional requirement is a statement of how a system must behave, it is a constraint upon the systems behavior. Non-functional requirements specify all the remaining requirements not covered by the functional requirements[3].
iii. Domain Requirements
   Domain requirements are those that are derived from the application domain. Domain requirements be new functional requirements, constraints on existing requirements[3].

Security Requirements Engineering

Security Requirements can be defined as the requirement that gives detail specification of any online system.
Different types of security requirements[1] are as follows.

Identification Requirement: -

Identification requirement specifies the extent to which the system shall identify its users and other applications that actually uses the system[1].

Authentication Requirement: -

It is the security requirement that specifies the extent to system should verify the identity of its users which can be

human user, system stakeholders or other applications integrated with it. They are not independent of Identification requirements, and many applications will group them together[2].

Authorization Requirement:

This requirement specifies the extent to which authenticated externals can access specific application, capabilities or information. This requires that System administrator will pre decide the privileges, functionalities permitted to external and he shall be allowed to access for which they are explicitly specified[2].

Immunity Requirement: -

An immunity requirement is a security requirement. This security requirement specifies that an application shall protect itself from infection by unauthorized and undesirable programs such as computer viruses, worms, and Trojans[2].

Integrity Requirement: -

This security requirement is meant to ensure that system data does not get corrupted intentionally via unauthorized creation, deletion, modification[2].

Intrusion detection Requirement: -

This security requirement is meant to ensure that system data does not get corrupted intentionally via unauthorized creation, deletion, modification[2].

Non repudiation Requirements: -

This security requirement specifies the extent to which system shall maintain tamper proof record of all accesses made to it by different users. This may be required to avoid future legal and liability problems that a party should not deny after interacting with all or part of the interaction[2].

Privacy Requirements: -

This security requirement specifies the different types of privacy to be maintained by the system so that the application is able to keep its resources and communications private from unauthorized programs and individuals . Also its objective is to minimize user's confidence and bad press comments[2].

Security Auditing Requirements: -

A security auditing requirement specifies that a system shall manage the security to audit the status and for that use its security mechanisms. This helps security team to analyze information about various security mechanisms it has implemented and review them[2].

Survivability Requirements: -

The security requirement specifies the range to which an application should work possibly in degraded mode even if some intentional destruction loss of data has been there in the application. They are different from robustness requirements which prevent the system from hardware or human error[2].

System Maintenance requirements: -

This requirement specifies system maintenance against accidentally modifications of security mechanism deployed by it. It means during usage of the system all security mechanism deployed by the system should be maintained and reviewed[2].

Physical Maintenance requirements:

This security requirement specifies the extent to which system shall protect itself from physical damages such as destruction, theft of computer or replacement of its hardware or software due to sabotage or terrorism[2].

SQUARE:

Security Quality Requirements Engineering (SQUARE) is the methodology which provides a means for eliciting, categorizing, and prioritizing security requirements for information systems and applications. SQUARE guides the interaction of the requirements engineering team and stakeholders at a client organization during the early stage of a development project. Its output is a set of verifiable security requirements [9]. SQUARE consists of nine steps[9]:

1. Agree on Definitions
2. Identify Assets and Security Goals
3. Develop Artifacts
4. Perform Risk Assessment
5. Select Elicitation Technique
6. Elicit Security Requirements
7. Categorize Requirements
8. Prioritize Requirements
9. Inspect Requirements

COMMON CRITERIA

Common Criteria become the international security evaluation criteria. The CC consists of three parts: Part 1: Introduction and general model. This part defines the basic concepts and provides the general models for evaluation[14]. Also the Protect Profile (PP) and Security Target (ST) are described in this part. Part 2: Security functional components. This part establishes a set of functional components providing a standard way of expressing the functional requirements for target systems [13]. Part 3: Security assurance components. This part establishes a set of assurance components for expressing the assurance requirements for target systems [13]. This paper mainly focuses on selecting functional components.

In CC, there are 11 functional classes, 65 functional families, 134 functional components and 251 functional elements [11]. They are classified according function and objectives. Some components have dependent relationship. Table 1 shows the 11 functional classes .

Id	**Abbreviation**	**Functional Class**
1	FAU	Security Audit
2	FCO	Communication
3	FCS	Cryptographic support
4	FDP	User Data Protection
5	FIA	Identification and Authentication
6	FMT	Security Management
7	FPR	Privacy
8	FPT	Protection of the TSF
9	FRU	Resource Utilization
10	FTA	TOE Access
11	FTP	Trusted Path/Channels

Table 1 . Security functional classes[14]

Key concepts are as follows: Target of Evaluation (TOE) is set of software, firmware and/or hardware possibly accompanied by guidance [10]. Protect Profile (PP) is implementation independent statement of security needs for a TOE type [14]. It can meet specific user needs and cares about the requirements of user without how to implement it. Security Target (ST) is implementation-dependent statement of security needs for a specific identified TOE [14]. So it needs to tell users what will be provided and how to implement. Asset is entities that the owner of the TOE presumably places value upon [14]. In the process of developing systems, asset can be recognized as the valuable resource or information for organizations or individuals. Security Objective is statement of intent to counter identified threats and/or satisfies identified organization security policies and/or assumptions [14]. Security Functional Requirement (SFR) provides security functional components and defines the desired security behavior of the system. And it proposed security requirements by the structure of "class-family-component".

PROPOSED IDEA

If we apply proposed idea for the Hospital management system the it will be as bellow. By applying VOSREP on the Hospital management system the functional, non-functional and security requirement are defined for each view point(actor) and then Review security by applying the SQUARE method. We can enhance this framework, by adding more viewpoints according to the project requirement. The SQUARE is basically a questioner technique. We have to asked five question to each view point. In the example of hospital management system we are asking same question to each view point for our concern. The quality of the security is range in between 0-5 according to the questioner. If the range of security break is more than 3 the system is not secure and we need to apply more security on the system and less than 3 is considered to be safe. For enhancing security we are taking the functional security component of the common criteria as mentioned above. Table 4 showing the questioner for each view point and what security requirements need for each question.

Table 2:- Proposed Idea

View point	Services	Non functional requirements	Threats	Security requirements	Review Security (SQUARE i.e by Questioner)	Enhance Security (based on common criteria)

Table 3:- Propose Idea applying on Hospital management system

View point	Services	Non functional requirements	Threats	Security requirements	Review Security (SQUARE)	Enhance Security
Doctor	1.Check patient list. 2.Provide Treatment. 3.Take salary	1.Minimize response time. 2.Correctness.	1.Disclose_data 2.Change_data 3.Privacy_violates	1.Identification Requirement. 2.Authorization Requirement 3.Privacy Requirement. 4.Non Repudiation Requirement.		
Patient Relative	1.Registration of the patient. 2.Enquiring Doctor. 3.Enquiring available bed. 4.Booking the seat. 5.Pay Bill.	1.Reliability. 2.Response time should be minimum. 3.Execution of check for the doctor must be correct.	1.Flooding. 2.Disclose_data 3.privacy_violates. 4.Change_data 5.Repudiate_Recieve 6.Repudiate_Send	1.Authorization Requirement 2.Privacy Requirement. 3.Non Repudiation Requirement.		
Receptionist	1.Check patient registration. 2.Check patient detail. 3.Fix appointment of patient with doctor. 4.Set the date and time of the appointment.	1.Availability 2.Idleness 3.Maintain Database	1. Data_Theft 2.Redundency 3.Errorness.	1.Identification Requirement. 2.Authorization Requirements		

Classes(Enhance Security) / Questioner (Review Security)	FAU	FCO	FCS	FDP	FIA	FMT	FPR	FPT	FRU	FTA	FTP
Qns 1. If your information is leakage				Yes	Yes	Yes		Yes	Yes	Yes	
Qns 2. If your data is not accessible by every time						Yes					
Qns 3. If you faced any kind of unauthorized data changes	Yes		Yes	Yes	Yes	Yes		Yes		Yes	Yes
Qns 4. If you facing any recording failure	Yes				Yes	Yes		Yes	Yes		
Qns 5. If you Are not satisfied by the available security											

Table 4:- Security needed for each Questioner

CONCLUSION

Our main emphasis is on making the VOSREP more secure by enhancing more security based on the functional security requirements of common criteria since the system in today's world are the target of hackers, malicious crackers which is not an option since the society relies heavily on them and not on the design and implementation phase. In this paper we have enhanced more security in the existing tool VOSREP. By applying SQUARE method we have measured the quality of security in VOSREP and then considering the functional security requirements based on common criteria methodology we have enhanced the existing tool of VOSREP.

REFERENCE

[1] Gupta D., Agarwal A., "Security Requirement Elicitation using view points for online system", International Conference on Emerging Trends in Engineering and Technology, Nagpur, July 2008.

[2] Gupta D., Agarwal A., "Guidelines and case study for eliciting Security Requirements", Proceedings of the 2nd National Conference on Computing for Nation Development, Delhi , pages - 445 – 448.

[3] Ashish Agarwal A., "View Point Approach For Engineering Security Requirements" Department of Computer Engineering, Delhi College of Engineering, University of Delhi, 2008.

[4].Shruti Jaiswal," Security Requirement Prioritization" Department of Computer Engineering ,Delhi College of Engineering ,University of Delhi,2009.

[5] Seiya Miyazaki, Nancy Mead, Justin Zhan, "Computer-Aided Privacy Requirements Elicitation Technique" IEEE Asia-Pacific Services Computing Conference, 2008.

[6] M. Ware, J. Bowles, C. Eastman, "Using the common criteria to Elicit security Requirements with use cases", 2006 IEEE.

[7] Michael S. Ware, John B. Bowles, Caroline M. Eastman, "Using the Common Criteria to Elicit Security Requirements with Use Cases". In proceeding of IEEE conference, 2006.

[8] Donald G. Firesmith, "Engineering Security Requirements", Journal of object technology, 2003, vol 2, no.1, pages 53-68.

[9] M. Ware, J. Bowles, C. Eastman, "Using the common criteria to Elicit security Requirements with use cases", 2006 IEEE.

[9] Seiya Miyazaki, Nancy Mead, Justin Zhan, "Computer-Aided Privacy Requirements Elicitation Technique" IEEE Asia-Pacific Services Computing Conference, 2008.

[10] Common Criteria for information technology security evaluation. Version 3.1, Part1: Introduction and General Model, 2009.

[11] Common Criteria for information technology security evaluation. Version 3.1, Part2: Security Functional Components, 2009.

[12] Common Criteria for information technology security evaluation. Version 3.1, Part3: Security Assurance Components, 2009.

[13] Shoichi Morimoto, Shinjiro Shigematsu, Yuichi Goto, and Jingde Cheng, "Formal Verification of Security Specifications with Common Criteria", Proc.22nd Annual ACM Symposium on Applied Computing, ACM Press, pp.1506-1512, 2007.

[14] Zhuobing HAN, Xiaohong LI, Yizhen LIU, Zhiyong FENG, "Auto-Selection of Security Functional Components Based on Common Criteria" 2012.

Chandana Das received her B-Tech(IT) degree in the year 2010, from Shillong Engineering and Management college Affiliated by NEHU. Currently she is pursuing M-Tech(CSE) in LPU, Punjab. Her area of interest includes Software Engineering.

Pardeep Kumar Sharma received his M.Sc(IT) degree in the year 2010, from Graphic Era University, Dehradun. Currently he is pursuing M-Tech(CSE) in Lovely Professional University, Punjab. His area of interest includes Software Engineering, Cryptography, Cloud Computing.