Comparison between Secure Tropos and VOSREP

Chandana das, Pardeep kumar Sharma, Kritika Chaudhry

Abstract - Security is the main concern now days for any software system. In the past security was often treated as an add-on on other requirements, which make the system expensive on both the developer and user sides. Computer system security attacks are one of the most urgent problems facing IT professionals today. Security engineering should be integrated with the Software development life cycle to handle all the issue related to the software security. There are various techniques for addressing security requirements during the early phases of Software Development Life Cycle (SDLC).In this paper we are comparing two existing technique Secure Tropos and VOSREP with the help of example medical information system.

Keywords - Secure Tropos, VOSREP, Functional and non-functional Requirement, Security Requirement, Threats.

INTRODUCTION

In the development of system such as e-commerce, military system, online business component engineering Security has been a great concern for software engineering community in the last decade[1].Security is usually defined in terms of the existence of properties such as confidentiality, authentication, integrity, access control, non-repudiation and availability and the ability to overcome possible threats. System is attacked by virus, malicious crackers and various other threats of cyber terrorism[1] .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 rework and reduce potential security vulnerabilities. Research experience shows that to overcome from the system failure the engineer should captured and maintained security requirements along with the functional and non functional requirements [2]. For integrating Security engineering with SDLC the Requirement engineers are clear about the requirements for the securities. The engineers are also concerns about the architectural and behavioral constraints. Now there are many methodologies like common criteria, misuse cases, attack trees, Secure Tropos, VOSREP for this purpose. So in this paper we are comparing latest two methodologies i.e. Secure Tropos and VOSREP. Both the methodologies concerns about the non functional requirements as well as functional requirements and is better than misuse cases and attack trees. In this paper we have described medical information system using Secure Tropos and VOSREP.

.EXISTING CONCEPT

Secure Tropos: Tropos was an agent oriented software engineering methodology and was not conceived with security. Secure Tropos is the security–oriented extension of the Tropos methodology where the developers can consider security issues during the software development process. Security requirements are identified by employing the modelling activities of secure Tropos [9], such as security reference diagram construction, security constraints and secure entities modelling.

Secure Tropos, includes the following concepts.

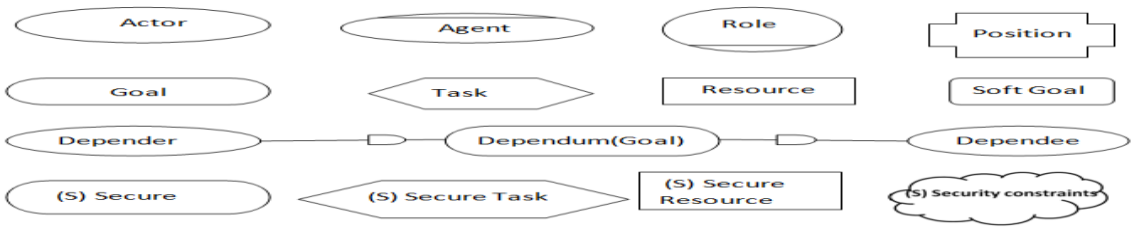

Fig. 1. Secure Tropos notation[8]

Actors are the entities that have strategic goals and intentionality.

Goals can be define as an actor's strategic interests.

Soft-goals are those goals which have no clear criteria whether they are satisfied or not[9].

Tasks represent in an abstract level a way of doing something.

Resources represent a physical or informational entity.

Intentional dependencies indicate that actors are interdependent to perform some specific goals and delivery of resources[9].

Security constraint is defined some constraints like as integrity, privacy, availability of the information system which is under development [9].

Secure dependency introduces security constraint(s) that must be applied for the dependency satisfaction. There will be the agreement between both the depender and the dependee in security constraints for the validity of the security dependency. The depender expects from the dependee for satisfaction of the security constraints [9].

S**ecure goal** involves the strategic interest of security with the actor. It mainly introduced to achieve every possible security constraints that are imposed to the actor. These are mainly introduces for security constraints [9].

S**ecure task** is defined as a task that represents a particular way for achieving a secure goal.

The secure Tropos process allows for two types of validation. A model validation and design validation. The model validation involves the validation of the developed models like the goal diagram or the actor diagram with the aid of a set of validation rules [9]. The design validation aims to validate the developed solution against the security policy of the system.

VOSREP-- View Point Oriented Requirement elicitation process
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 [3].This is very important activity of the security engineering.

REQUIREMENTS ENGINEERING

Requirement engineering is the software engineering process that includes the discovering; maintain a set of requirements for the software.

The different types of requirement are as follows:-.

i. Functional Requirements
A functional requirement specifies set of functions that a system or component must be able to perform. Functional requirements may vary depending on the type of software, types of users and the type of system requirements where the software is used [1].

ii. Non Functional Requirements
A non-functional requirement is a statement that defines how a system must behave, it is a constraint upon the systems behavior. Non-functional requirements specify all the residual requirements that are not covered by the functional requirements [1].

iii. Domain Requirements
Domain requirements are those that are derived from the application domain and also describe the requirements on which the system works[1]. It describe the characteristics and feature related to the domain.

SECURITY REQUIREMENTS ENGINEERING

Security Requirements can be defined as the requirement that gives detail specification of any online system.

Different types of security requirements [3] 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[3].

Authentication Requirement: - It is for the security purpose 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[3].

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 [3].

Immunity Requirement: - This is required for the infection and unauthorized and undesirable program such as viruses, malwares, worms, Trojans[3].

Integrity Requirement: - This security requirement is meant to ensure that system data does not get corrupted intentionally via unauthorized creation, deletion, modification[3].

Intrusion detection Requirement: - This security requirement is meant to ensure that system data does not get corrupted intentionally via unauthorized creation, deletion, modification[3].

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[3].

Privacy Requirements: - This security requirement specifies the different types of privacy to be maintained by the system so that the application must able to keep its information (data) and communications private from unauthorized individuals and programs. Also its objective is to minimize user's confidence and bad press comments[3].

Security Auditing Requirements: - A security auditing requirement specifies that a system shall enable security manager to audit the status of user and use of its security mechanisms. This helps security team to analyze information about various security mechanisms it has implemented and review them[3].

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[3].

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[3].

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[3].

COMPARING SECURE TROPOS AND VOSREP

Secure Tropos

If secure Tropos is applied on Medical information System [8] which we can consider as a part of hospital Management System then the first step in the early requirements analysis is the construction of the security reference diagram. The main security features of the security reference diagram are privacy, integrity and availability, and a part of it is shown in the figure2.
The next step of the process involves the modelling of the stakeholders of the system together with their goals, dependencies and security constraints. For this purpose, Tropos employs the actor diagram. In the paper[8] five actors considered.
The **Professional** actor, who represents a health and social care professional;
The **Older Person,** who represents a patient over 65.
The **DoH** actor, which represents the English of

Heath of Department of Health, Department

The **R&D Agency** actor, which represents a research and development agency interested in obtaining medical information for research purposes;

The **Benefits Agency**, which represents an agency that financially helps the older person.

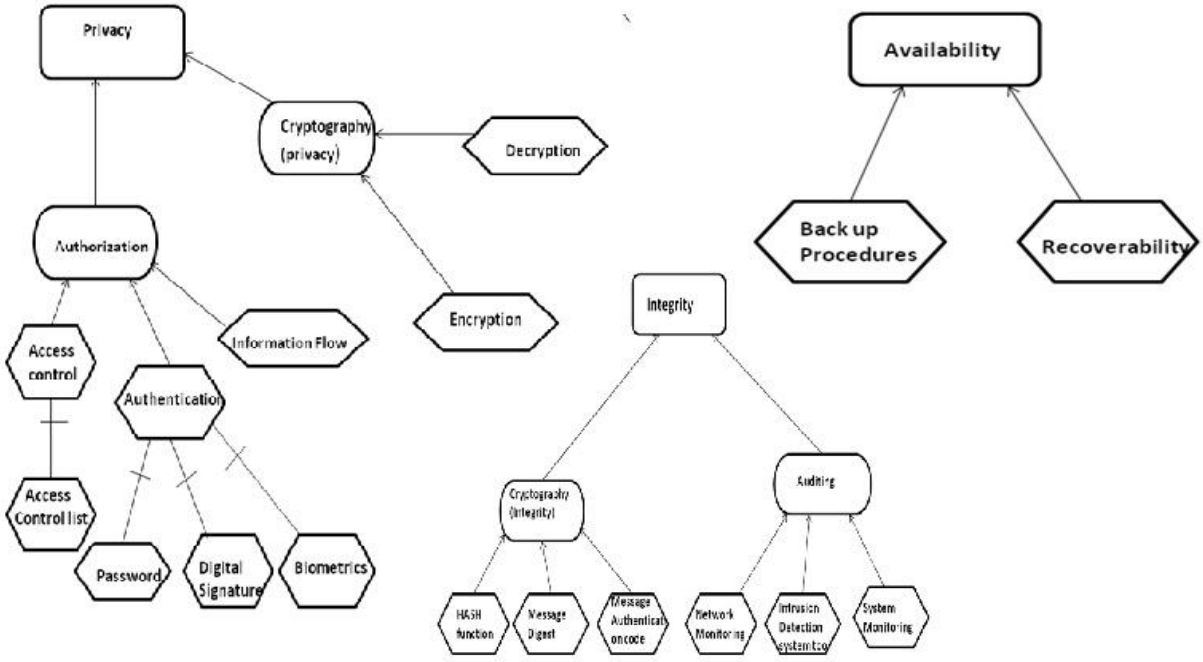

Fig. 2. Security reference diagram[8]

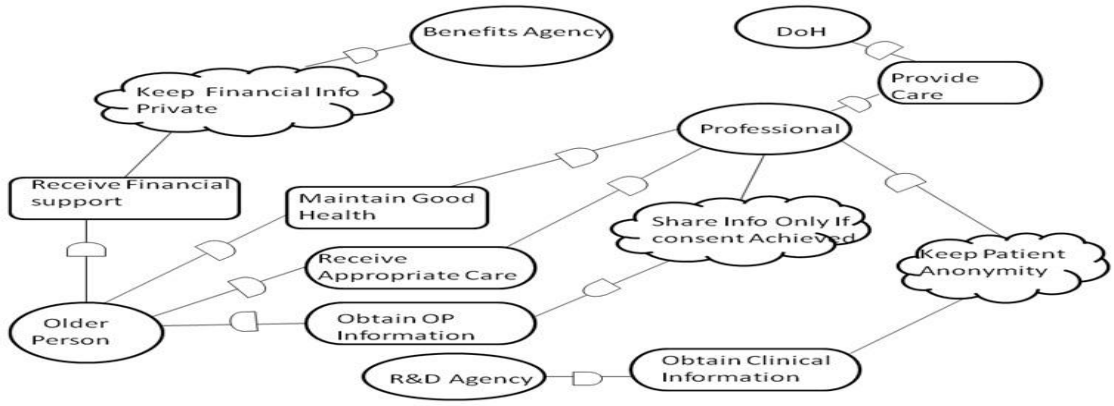

Fig. 3. Partial actor diagram[8]

In the actor diagram the Professional relays upon the Older Person to Obtain (Older Person). Older Person needs the privacy of their personal medical information and not wants to share it to anyone. Thus, most of the times, the Professional is imposed a constraint to share this information only if the older person's consent has been obtained[9].

Similarly, for the Financial Support the Older Person depends upon Benefits Agency. Older Person also suspicious about his financial privacy. R&D Agency obtains Clinical information for research and testing. R&D Agency depends on the Professional to access this information. However, the Professional is imposed a constraint (by the Department of Health) to Keep Patient Anonymity[9].

The security analysis starts by assigning the security constraints of the actor, to the goals of the actor they (the security constraints) restrict.

Now Considering the Professional actor. By analyzing the Professional actor's goals and tasks, the Share Medical Info goals are identified[9]. The main goal to share the information, only it is provided by the older person. The constraints are satisfied by the Professionals. This goal is achieved by many different ways for example the Professional obtain it personally or only with his reliable nurse. Therefore, a sub-constraint is introduced, Only Obtain Consent Personally. To achieve this sub-constraint the secure goal Personally Obtain Consent is introduced to the actor, which is divided into two sub-tasks: Obtain agreement by Mail or Obtain agreement by Phone.

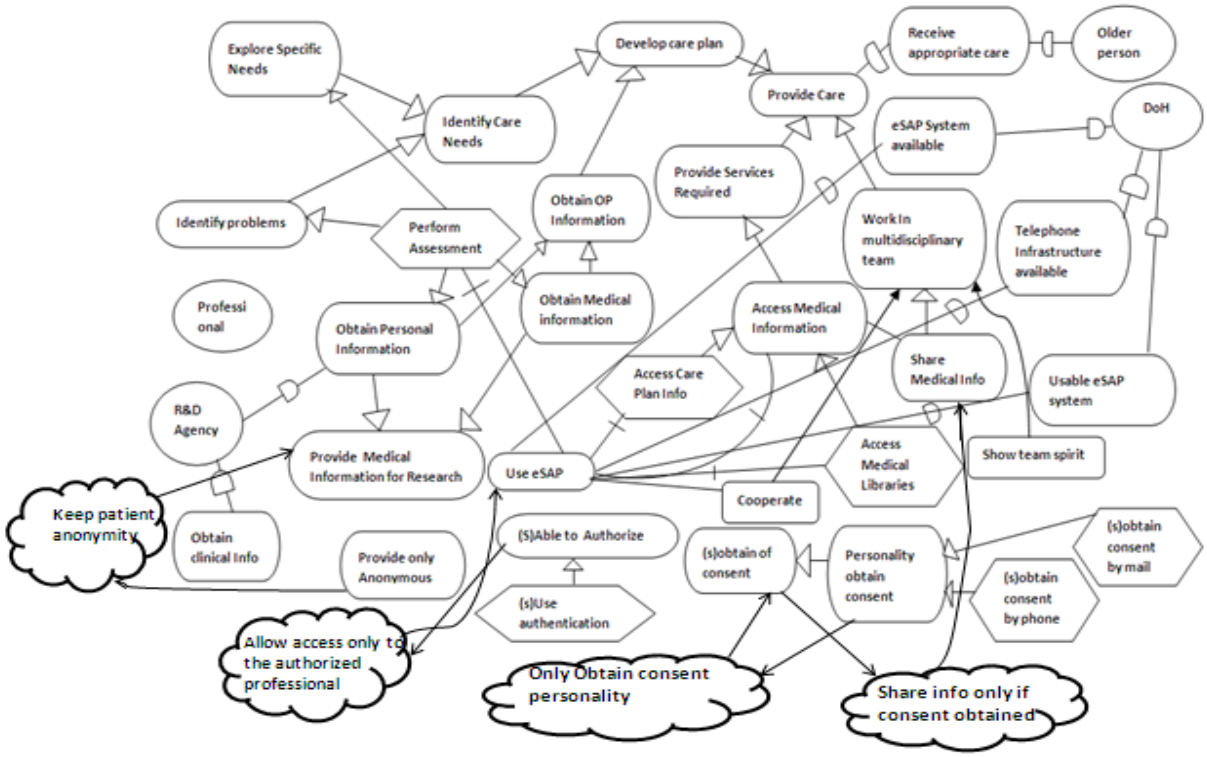

Fig. 4. Professional actor partial analysis[8]

VOSREP:-

If **VOSREP** is applied on Hospital Management System then the first step is the early requirements analysis is as follows.

View point	Services	Non functional requirements	Threats	Security requirements
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
Pharmaceutical Department	1.Maintain the list of medicine. 2.Check the expiring date of medicine.	1.Availability	1.Integrity. 2.Privacy_Voilated 3.Change_Data	1.Integrity Requirement 2.Identification Requirement.
Financial Department	1.Keep the account Number of patient. 2.Keep record all the financial transaction. 3.Deal with the employee's salary.	1.Correctness 2.Maintain Database 3.Recoverability	1. Integrity 2. Privacy-Violated 3. Security breaches 4. Social_Engineer 5. .Insider	1.Integrity Requirements. 2.Authorization Requirements
Administrator	1.Maintain the record of financial department. 2.Maintain the record of doctor availability. 3.Maintain the record of patient list. 4.Maintain the record of pharmaceutical department.	1.Recoverability 2.Manageability 3.Faster processing	1. .Insider. 2. .Impersonate	1.Authorization requirements. 2.Authentication Requirement.

Database	1.Maintain the financial transaction. 2.Maintain the all other transaction.	1.Availability. 2.Cost and Delivery.	1.Integrity. 2.Privacy_Voilates 3.Change_Data 4.Disclose_Data	1.Security Auditing Requirement 2.Intrusion Detection Requirement.

Fig 5:- An example "Hospital Management System" explaining VOSREP

COMPARISON RESULT

1. As we have seen using VOSREP is less complex then the Secure Tropos and it is easy to understand .
2. VOSREP is in the tabulated form providing all the security, functional and non-functional requirements in detail.
3. VOSREP conclude all the actor in one table with each details of each actor but in Secure Tropos each time we have to consider one actor and all the details about the actor which is very time consuming .

4. In Secure Tropos there are many terms like Security Constraints, dependee, dependum, depender which are not easily understandable to a new user .

Conclusion

Our main emphasis is on to discovering the security requirement as early as possible so that the system under development is efficient and less vulnerable which is the need of the day in current scenario 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 not on the design and implementation phase. In this paper I have gone through the two methodologies Secure Tropos and VOSREP. By applying both methodologies on the Hospital Management system we have seen that VOSREP tool is more user friendly than the Secure Tropos methodology. It provides more information in tabulated form.

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] Haralambos Mouratidis, Paolo Giorgini, Gordon Manson, Ian Philp,"A Natural Extension of Tropos Methodology for Modelling Security", 2002.

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

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

[8]Haralambosn Mouratidis ," Secure Tropos: A Security-Oriented Extesion of the Tropos Methodology", International Journal of Software Engineering and Knowledge Engineering World Scientific Publishing Company.2007

[9] "Secure Tropos: dealing effectively with security requirements in the development of multiagent systems", H. Mouratidis, P. Giorgini,School of Computing and Technology, University of East London, England, Department of Information and Communication Technology, University of Trento, Italy..2006

[10] Sindre G, Opdahl AL, "Eliciting security requirements by misuse cases". In proceeding of IEEE conference, 2000.

[13] Dan Wu, "Security Functional Requirements Analysis For Developing Secure Software", 2007.

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.

Kritika Choudhry received her M-Tech in Software Engineering degree in the year 2011, from Delhi College of Engineering Affiliated by Delhi Technology University, Delhi. She is currently working as an Assistant Professor in Lovely Professional University, Punjab. Her area of interest includes Software Engineering.