iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** X **Month of publication:** October 2017

DOI: http://doi.org/10.22214/ijraset.2017.10293

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

A Security-Oriented Enhancement to the Tropos Methodology

K. Suresh Babu[1], Ch. Rambabu [2]
[1]*Sr. Assistant Professor, Department of CN&IS, School of Information Technology (JNTUH), Village KPHB, Mandal Kukatpally, Dist Medchal, Telangana, India*
[2]*M.Tech Student, Department of CN&IS, School of Information Technology (JNTUH), Village KPHB, Mandal Kukatpally, Dist Medchal, Telangana, India*

Abstract: ***Now-a-days the usage of social networks by people is increasing gradually, also the social networks increasingly becoming the primary channel for dispersal of information. The social networks, from the last few years, in addition to dispersal of information they are also used by banks and payment industries. These industries are actively developing mechanisms to facilitate transfer of money over social media. So in this work we try to evaluate the information security aspects over social networks using some open source tools. In this we use Secure Tropos, a security oriented extension to the tropos methodology, to model various possible interactions on the popular social networking website Facebook. Tropos methodology uses the concepts like actors, goals and the possible interactions among them. In this work we use secure tropos to analyze the confidentiality, integrity and availability requirements of information security. In the process we evaluate the tools ability to capture known flaws in the security model of Facebook.***

I. INTRODUCTION

Information security is defined as defending information from unauthorized activities. The unauthorized activities in-clude unauthorized access, use, disclosure, modification, pe-rusal, inspection, recording or destruction. Unlike web2.0 wherein the webmaster was the only person who could edit the content on the website, todays WWW is based on Web3.0 where in multiple participants can create and edit content on the web. Examples for web 3.0 are the social networking websites like Facebook, linkedin, twitter etc. Today social networking websites are being increasingly used as payment platforms by banks. Almost all social networking websites provide multiple means and mechanisms for the users to interact with one another. Essentially, today's social networking websites are complex socio-technical systems in which the users who otherwise can be labeled as actors interact with one another and with technical components also known as wall, pages, pictures, videos, applications, to fulfill their goals. Ensuring the three attributes of information security in a distributed systems of actors is a challenge and requires a well organized representation of the actors, their roles and study of possible social interactions between the actors. Each participant is au-tonomous, and the system is defined in terms of the interactions among actors, which may be: social reliance, actors rely on others to achieve their goals, and information exchange, actors exchange relevant information. In such systems, many security issues arise from the interaction between actors, and on how the exchanged information is manipulated. Therefore, social aspects are a main concern when analysing security. Social networks are more popular today and have increas-ingly become primary platforms for information dissemination. Many companies today rely on social networks as a means to promote their products and associated services. Similarly, organizations both private and public rely on social networks to stay connected with their members. In addition to use of social networking websites for non-financial services, banks today are in the process of leveraging on social networks to enable peer to peer financial transactions [9]. Given this background, the current project aims to systematically structure information security rules binding the integrity of information shared and analyse the rules to detect gaps if any in the information se-curity rules based on the well understood Information security triad of confidentiality, Integrity and Availability. To model Information security in social networks, we use the concept of secure tropos [6]. Secure tropos is a security oriented extension of tropos methodology. Tropos uses the i* modeling framework. It includes the concepts like actors, goals and social dependencies among them.

II. BACKGROUND

In the last year a few banks have started using social network platforms for their customers to do peer-to-peer trans-actions. ICICI bank allows users to do banking conveniently in social networking site Facebook through an application called Pockets [11]. Pockets is an application developed based on API provided by facebook social networking platform. The customers can use this app by installing it into their Facebook account after logging in. The application allows customers to transfer money to friends, top up

prepaid mobile talk time, purchase movie tickets, check account balance, keep track of the last 10 transactions, view credit card statements, apply for a cheque book etc. Axis bank is another bank that is facilitating banking oper-ations over Twitter [12] social networking platform. Customers can use this feature by linking their twitter handle with their Axis bank account. The customers will be able to recharge their mobile phones, data card, DTH and also view their last 3 transactions. For example, to view the balance in the account a customer can format the message "#balance followed by last 6 digits of the account number" to @AxisBankSupport twitter handle. In response the bank will send a message contain-ing the account balance. Similarly various banks in several other countries are increasingly exploiting social networking platforms to facilitate banking operations. Given the wide range of mechanisms that social networking platforms provide for people to share, exchange and edit content, it becomes necessary to model the and evaluate the security aspects of the underlying complex social interaction model.

III. RELATED WORK

Secure Tropos is a simulation tool based on agent oriented software engineering methodology used to model and ana-lyze information security principles. Agent oriented software engineering methodology introduces an alternative approach to analyze and design complex interactions between various stakeholders of a distributed IT system. Secure Tropos is a security extension to the Tropos method-ology. STS is a Security Requirements modelling tool that makes use of Secure Tropos to perform security requirements modeling, automated analysis through Disjunctive Datalog. The tool is a standalone application written in Java. STS-Tool has been widely used to analyze security requirements of large distributed IT projects through modeling [7], [8], [9].An e-Government scenario was analyzed using STS-tool in [1]. The scenario involves land selling with trustworthy buyer and also exchanging several documents with various government bodies. It is represented using STS-tool's 3 views. Travel planning scenario is represented using STS-tool in 3 views in [2]. In this scenario, the travel agency allows its uses to read about various destinations, book flights, hotels cars etc. In [3], a lot selling using DoUP application scenario is represented using STS-tool. A lot owner wants to sell his/her lot for this he/she may contact real-estate agency (REA) and an interested party wants to buy this lot will enquire in this application. Using its 3 views STS presented this scenario.

In [4], the scenario of digitally processing the enrollment process of new students based on their eligibility as per university policy is studied. The evaluation system involves exchange of requisite digital documents between the student and the university. This is a scenario which comes under The University of Trento, which is one of Italian public administra-tion. The scenario was presented using tropos model. In [5],a transition process from paper based voting to electronic voting is studied for possible flaws. It is an e-Voting scenario and is represented using tropos methodology and UML. Finally, in [6], a tropos goal achieving methodology is presented. Goal decompositions are used to achieve a goal. In STS, a goal can be AND decomposed or OR decomposed.

IV. ABOUT TOOL

A tool called STS-tool (Socio Technical Security tool) is used to model the scenario. It uses the STS-ml (STS-Modeling Language).In socio technical systems the participants are au-tonomous. Social reliance and information exchange are the 2 ways of interaction among participants in the system. The participants in the system can express their own requirements, which can be allowed by the STS-ml. It also enables the possibility to represent the interaction between different actors which are interacting to achieve their own goals. There are 3 views in which we have to model the scenario in STS-tool:

A. Social View

The social view shows the involved stakeholders, which are represented as roles and agents. Agents refer to actual par-ticipants (stakeholders) known when modelling the Scenario, whereas roles are a generalisation (abstraction) of agents. To capture the connection between roles and agents, the play relation is used to express the fact that certain agents play certain roles. Stakeholders have goals to achieve and they make use of different information to achieve these goals. They interact with one another mainly by delegating goals and exchanging information. Information is represented by means of documents, which actors manipulate to achieve their goals.

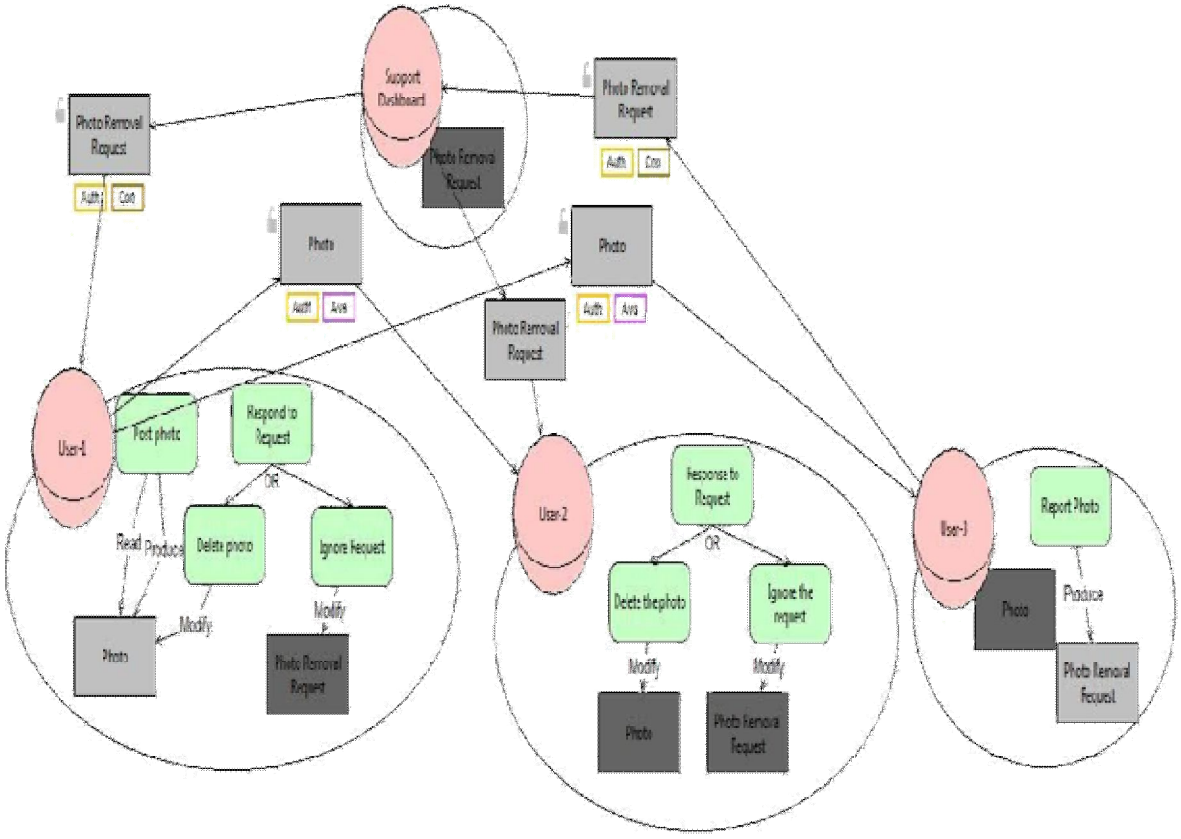


Fig.1.Social View

B. Information View

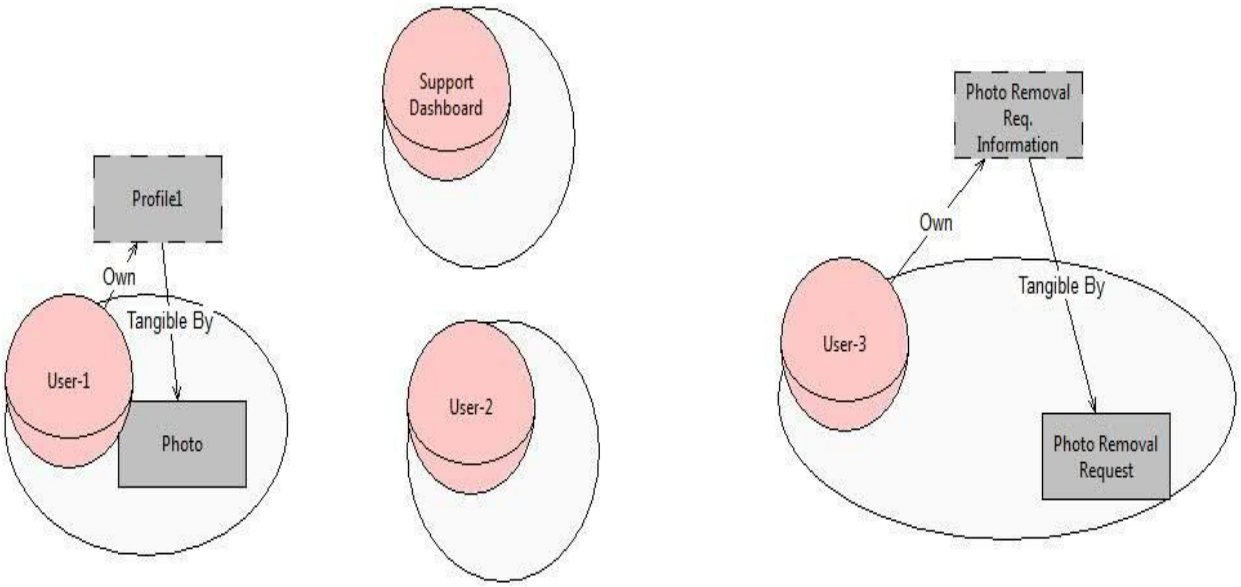


Fig.2.Information View.

The information view gives a structured representation of the information and documents in the Scenario. It shows what is the informational content of the documents represented in the social view. Information is represented by one or more documents (tangible by), and the same document can make tan-gible multiple information entities. Moreover, the information view considers composite documents (information) capturing these by means of part of relations.

C. Authorization View

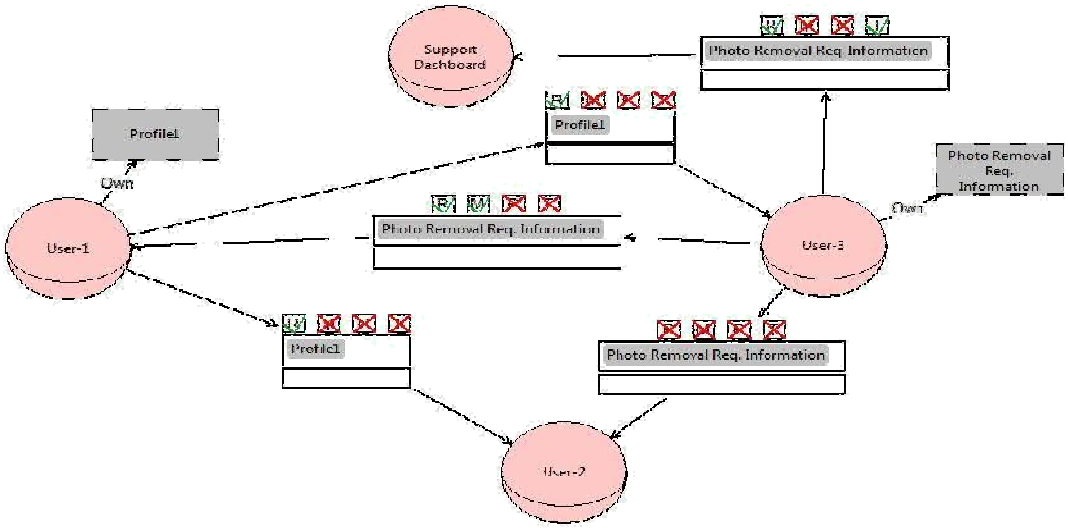


Fig.3. Autherization View.

The authorization view shows the permissions or prohibi-tions flow from a stakeholder to another, that is, the authoriza-tions stakeholders grant or deny to others about information, specifying the operations the others can and must perform over the information. Apart from granting authority on performing operations, a higher authority can be granted, that of further authorising other actors (i.e. authorization transferability) Au-thorizations start from the information owner. Therefore, in the authorization view, ownership is preserved and inherited from the information view.

V. IMPLEMENTATION

As mentioned before the scenario can be designed in 3 views: Social, Information and Authorization view.

A. Stakeholders

This section describes the stakeholders identified in the PhotoRemoval Flaw project. Stakeholders are represented as roles or agents.In particular, identified roles are: User-1, User-2, User-3 and Support Dash-board (Figure 1). In the PhotoRemoval Flaw project there are no plays relationships taking place for the given agents/roles.

B. Stakeholders' documents

Stakeholders have documents they possess or ex-change with others to achieve their goals. Documents are represented within the rationale of the role/agent (Figure 1). In our scenario (Figure 1) we have:
User-1 has document Photo. Moreover it has document Photo Removal Request provided by Support Dashboard.
User-2 has document Photo Removal Request provided by Support Dashboard and docu-ment Photo provided by User-1.
User-3 has document Photo Removal Request. Moreover it has document Photo provided by User- 1.
Support Dashboard has document PhotoRequest provided by User-3.

C. Stakeholders' documents and goals

Stakeholders documents are linked to their goals: they read (make) documents to achieve their goals, they modify documents while achieving their goals, and they may produce documents from achieving their goals. In the scenario (Figure 1) stakeholders documents and goals are related as follows:
User-1 modifies document Photo to achieve goal Delete photo, modifies document Photo Removal Request to achieve goal Ignore Re-quest and readsand produce document Photo to achieve goal Post photo.
User-2 modifies document Photo Removal Request to achieve goal Ignore the request and modifies document Photo to achieve goal Delete the photo.
User-3 produces document Photo Removal Request to achieve goal Report Photo.

D. Goal Refinement

Stakeholders have goals to achieve. Goals are rep-resented within the rationale (round compartment attached to the role/agent, see Figure 1) of the role/agent representing the stakeholder. They achieve their goals by further refining them into finer-grained goals (subgoals) by means of AND/OR decomposi-tions. AND-decompositions structurally refine a goal into multiple subgoals (all AND subgoals need to be achieved for the goal to be achieved), while OR-decompositions represent alternative ways for achiev-ing a goal (at least one of the subgoals in the OR-decomposition needs to be achieved for the goal to be achieved). In the scenario (Figure 1) we have:

User-1 has to achieve goal Post photo and goal Respond to Request. To achieve Respond to Request, User-1 should achieve either goal Delete photo or goal Ignore Request

User-2 has to achieve goal Response to Re-quest. To achieve Response to Request, User-2 should achieve either goal Delete the photo or goal Ignore the request

User-3 has to achieve goal Report Photo.

E. Goal Contributions

Goals can contribute one to another. A contribution identifies the impact the fulfilment of one goal has on the fulfilment of another goal. This impact can be either positive or negative, and is represented with ++ and – respectively. Positive contribution means that the achievement of a goal also achieves the other goal. Negative contribution means that the achievement of a goal inhibits the achievement of another goal. In the scenario there are no contribution relations taking place for the given agents/roles.

F. Stakeholders Interactions

This section describes stakeholders interactions, pro-viding insights on whom they interact with to fulfil their desired objectives, as well as which are the stakeholders that rely on them to fulfil their respective goals. This kind of interaction is carried out by means of goal delegations. To achieve their goals stakeholders might need specific information. If they

do not possess this information, they may ask other stakeholders to provide them documents. Document transmission is used to capture this interaction.

G. Goal Delegations

Stakeholders interact with others to achieve some of their goals by means of goal delegations. Goal delegations are graphically represented as a relation that starts from a delegator actor to a delegate actor (following the direction of the arrow), having a rounded corner rectangle representing the goal being delegated. Security needs are graphically specified as labels that appear below the delegated goal (Figure 1). In the scenario there are no goal delegations taking place for the given agents/roles.

H. Document Transmission

Stakeholders exchange information by means of documents with other stakeholders. The following description enlists all the transmission from one role/agent representing the stakeholder, to other roles/agents. Document transmission is represented as an arrow from the transmitter to the receiver, with a rectangle representing the document. The security needs expressed over the transmission are described, if applicable. Security needs are specified with the help of labels that appear below the document being transmitted. In the scenario (Figure 1), we have the following document transmissions:

User-1 trasmit ducument Photo to User2. The following security needs apply to this transmission.Authentication:sender and Availability:100.User-3 transmit document Photo Removal Re-quest to Support Dashboard. The following security needs apply to this transmission: Au-thentication: sender and Confidentiality: re-ceiver. Support Dashboard transmit document Photo Removal Request to User-1. The following security needs apply to this transmission: Au-thentication: sender and Confidentiality: re-ceiver. Support Dashboard transmit document Photo Removal Request to User-2.

I. Organizational Constraints

Apart from the security needs actors specify over their interactions, there are others, which are dic-tated either by the organization, business rules and regulations, or law. In this section we enlist these constraints, together with the security requirements derived from them. Currently, the language supports these organizational constraints: Separation of Duties (SoD) and Binding of Duties (BoD). Graphically we represent these constraints using a similar notation to that used in workflows, as a circle with the unequal sign within and as a circle with the equals sign within, respectively. The relations are symmetric, and as such they do not have any

arrows pointed to the concepts they relate (being these roles or goals). In the scenario there are no organizational constraints specified.

J. Events

No events have been modelled in the scenario.
Information View:

K. Modeling Ownership

The information view represents also who are the owners of the information that is being manipulated through the documents that represent them in the social view. The owners for the different information in the scenario are User-1 owns the information Profile1 and the information Photo Removal Req. Information belongs to User-3.

L. Representation of Information

Information is represented (made tangible by) by documents, which stakeholders have and ex-change. The documents stakeholders in the sce-nario (Figure 2) have and exchange with one an-other contain the information as summarized below: The information Profile1 is tangible by document Photo and Photo Removal Req. Information is made tangible by Photo Removal Request.

1) *Authorization View:* N. Authorization FlowIn this section are described for each role/agent, the authorizations it passes to others and what authoriza-tions it receives from other roles/agents.In the sce-nario (Figure 3) the authorizations for each role/agent are:Role User-authorizes User-2 to read and prohibits tomodify, produce and transmit information Profile1, passing the right to further authorizing other actors, and authorizes User-3 to read and prohibits to modify, produce and transmit informa-tion Profile1, passing the right to further authorizing other actors. User-1 is authorized by User-1 to read and modify and prohibited to produce and transmit information Photo Removal Req. Information, having the right to further authorising other actors. Role User-2: User-2 is authorized by User-2 to read and prohibited to modify, produce and transmit information Profile1, having the right to further authorizing other actors, and is prohibited by User-2 to read, modify, produce and transmit informa-tion Photo Removal Req. Information, having the right to further authorizing other actors.
2) *Role User-3:* User-3 authorizes Support Dashboard to read and transmit and prohibits to modify and produce information Photo Removal Req. Information, passing the right to further authorizing other actors, and au-thorizes User-1 to read and modify and prohibits to produce and transmit infor-mation Photo Removal Req. Information, passing the right to further authorizing other actors, and prohibits User-2 to read, modify, produce and transmit informa-tion Photo Removal Req. Information, passing the right to further authorizing other actors.
3) *User-3* is authorized by User-3 to read and prohibited to modify, produce and transmit information Profile1, having the right to further authorizing other actors. Role Support Dashboard: Support Dashboard is authorized by Sup-port Dashboard to read and transmit and prohibited to modify and produce infor-mation Photo Removal Req. Information, having the right to further authorizing other actors.

VI. RESULTS

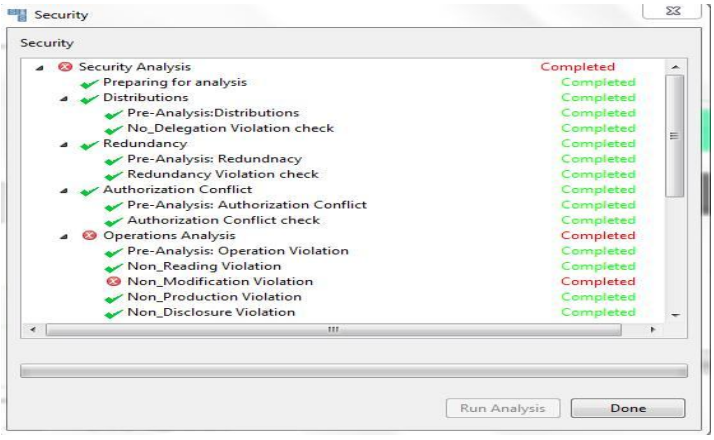
A. Well-formedness Analysis

The purpose of well-formedness analysis is to verify whether the diagram for the scenario is consistent and valid. A diagram is considered to be consistent if its constituent elements (concepts and relationships) are drawn and intercon-nected following the semantics of modeling language (STS-ml in our case). Thus, well-formedness analysis performs post checks to verify compliance with STS-ml semantics for all checks that cannot be performed live over the models. The Well-formedness Analysis analysis for scenario didn't find any errors.

B. Security Analysis

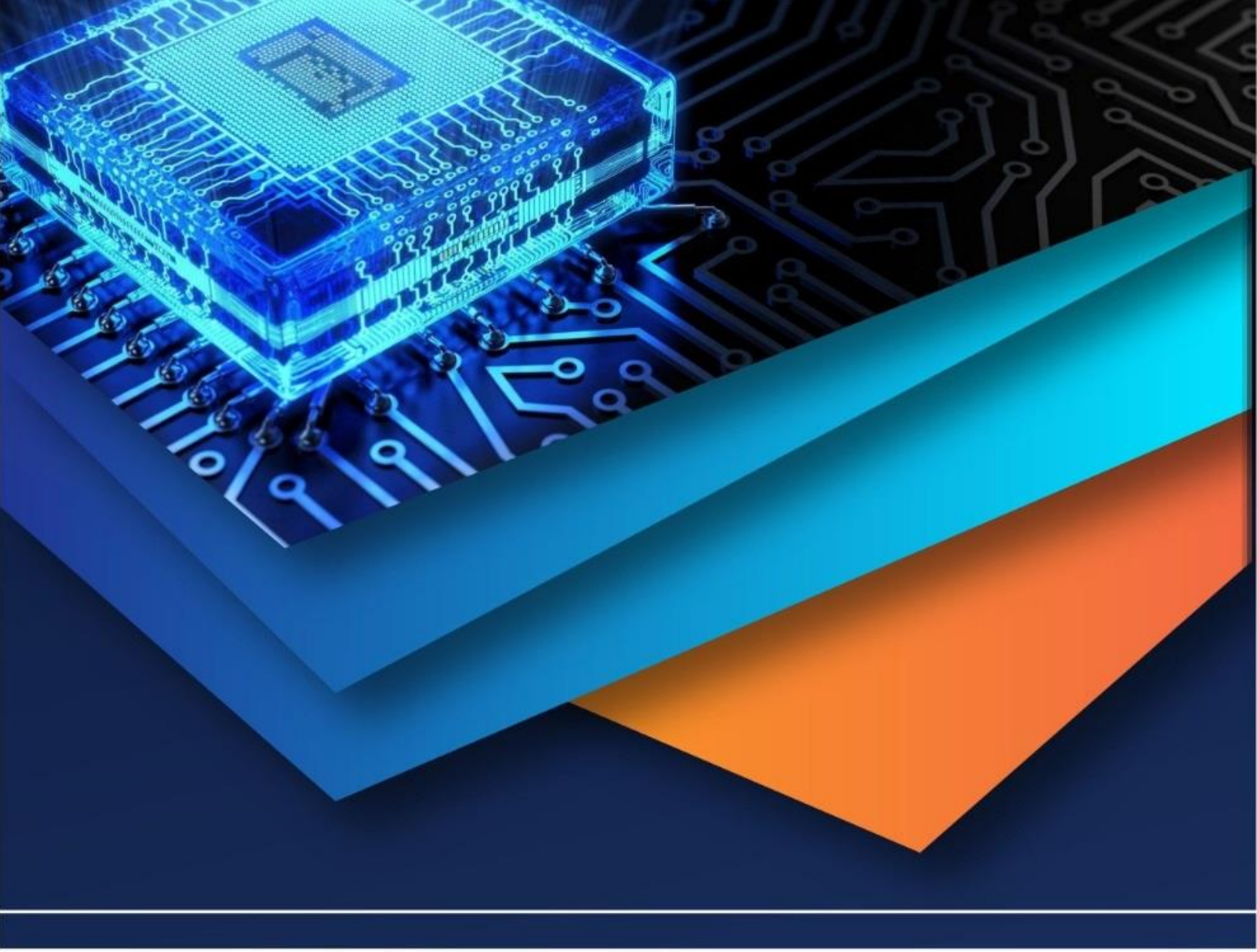
The purpose of security analysis is to verify whether the diagram for the scenario allows the satisfaction of the specified security needs or not. As a result, for all security needs expressed by stakeholders, it checks in the model whether there is any possibility for the security need to be violated. This analysis takes into account the semantics of STS-ml, defining the behaviour of the different elements represented in the models. The elements behaviour is defined by propagation rules that consider what concepts and what relationships the specification of a given security need affects. Datalog is used to define the semantics of STS-ml to express facts (things always. violation. "User-3" has required "User-2" non-modification of information "Photo Removal Req.

Information",but "User-2" can modify "Photo Removal Req. Information" since there is a modify relationship from its goal "Ignore the request" towards document "Photo Removal Request" representing "Photo Re-moval Req. Information"
lso "User-1" has required "User-2" non-modification of in-formation "Profile1", but "User-2" can modify "Profile1" since there is a modify relationship from its goal "Delete the photo" towards document "Photo" representing "Profile1"



REFERENCES

[1] Paja, E., Dalpiaz, F., Poggianella, M., Roberti, P., Giorgini, P.: Modelling Security Requirements in Socio-Technical Systems with STS-Tool, Fo-rum of the Conference on Advanced Information Systems Engineering, 155-162 (2012) .
[2] Paja, E., Dalpiaz, F., Poggianella, M., Roberti, P., Giorgini, P.: STS-Tool: Using Commitments to Specify Socio-Technical Security Requirements, 31st International Conference on Conceptual Modeling, 396-399 (2012)
[3] Elda Paja, Fabiano Dalpiaz, Paolo Giorgin.: Designing Secure Socio-Technical Systems with STS-ml, Proceedings of the Sixth International i* Workshop (2013)
[4] Dalpiaz. F., Paja, E.,Giorgini, P.: Security Requirements Engineering for Sevice-Oriented Appications, Proceedings of the Fith Internal i* Workshop(2011).
[5] Bryl, V., Dalpiaz, F., Ferrario, R., Mattioli, A., Vilafiorita, A.Evaluating Procedural Alternatives: a Case Study in e-Voting., Electronics Govern-ment an International Journal (2009).
[6] Haralambos Mouratidis, Paolo Giorgini: Secure Tropos: A Security-Oriented Extension of the Tropos Methodology,International Journal of Software Engineering and Knowledge Engineering(2006).
[7] tool.eu/download/documentation/documentation v.2.0.0/ManualModelingLanguage v.2.0.0.pdf.
ICICIBank Online, http://www.icicibank.com/Personal-Banking/insta-banking/pockets-on-facebook/index.pageAccessed:2016-12-28
[8] Paja, Elda, Dalpiaz, Fabiano ,Giorgini, Paolo.: STS-Tool: Security Re-quirements Engineering for Socio-Technical Systems, 65-96 (2014)
[9] STS-Tool — Tool for STS-ml modeling language, http://www.sts-tool.eu
[10] Manuals STS-Tool, http://www.sts-tool.eu/download/documentation/documentation v.2.0.0/Manual ModelingLanguage v.2.0.0.
[11] ICICI Bank Online, http://www.icicibank.com/Personal-Banking/insta-banking/pockets-on-facebook/index.page Accessed: 2015-08-13
[12] http://www.axisbank.com/personal/speed-banking/banking-on-twitter/features.aspx Accessed: 2015-08-12
[13] Palestinian Hacker posted vulnerability details on Mark Zuckerbergs Timeline, http://thehackernews.com/2013/08/Mark-Zuckerberg-hacked-facebook-hacking-tool.html Accessed: 2015-09-17



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY