Syntactic and Semantic Extensions of Malicious Activity Diagrams to Support ISSRM

Othmar Othmar Mwambe
Lecturer,Department of Library and Information studies
Tumaini University Makumira Dar es salaam college,Dar es salaam,Tanzania

ABSTRACT

Information security has played a great role in supporting security of organizational assets.Computes softwares / information systems developers have taken information security into great consideration particularly during systems/software development.There are several modelling languages that can be used to architect security features of information systems with respect to information system security management domain model(ISSRM).Malicious Activity Diagrams have been widely used by developers to model security features of various information systems as an extension of Unified Modeling Language(UML)[[2]].However Malicious Activity Diagrams can not cover all the features of ISSRM[[11]]. Due to the limitations of Malicious Activity Diagrams,this study has proposed new additional featers that will enable Malicious Activity Diagrams to cover the remaining security concepts of ISSRM(such as security constraint of the static information/security criterion-figure 6).

Keywords

Information security,Activity diagrams, Security requirements , ISSRM, Mal-Activity diagrams, Software development lifecycle management.

1. INTRODUCTION

Usually the study of information security provides a comprehensive framework for ensuring the effectiveness information security controls over information resources that support organizational opperations and assets.The construction and implementation of security-critical systems can only be complete if the main objectives of infromation security are maintained (Integrity, Confidentiality and Availability)[[8]].The risk management defines some factors that can lead to failure of main objectives of information security[[11]].Even though it is hard for many organisations to considers security of information due to the high cost implementation but it is vital important to take it into account due to fact that all information systems are exposed to threats.

There are several security risk management methods Such as Operationally Critical Threat Asset and Vulnerability Evaluation(OCTAVE[[12]]), The Security Quality Requirements Engineering (SQUARE), National Institute of standards and technology (NIST [[16]]) and frameworks such as Information System Security Risk (ISSRM) which can be used to investigate, analyze and risk treatment for security risk management but our main area of concern will include only Information System Security Risk framework and Malicious Activity Diagrams as modelling tool of demonstration.

2. Background study, related work, literature review and state of the Art

As I stated before (Abstract) that the main goal of my research is to improve Malicious Activity diagrams to support ISSRM by overcoming the existing limitations of Malicious Activity diagrams.The approach used for this part ofresearch work undergoes three main stages:

I. Observing the existing situation of Malicious Activity diagrams(*SituationAS IS*) and ISSRM

This has been precisely illustrated using examples which cover one of the main objectives of security(*Confidentiality*) using example *online Banking System*(Based on [[4]])

II. Exposing the limitations of Mal-Activity Diagrams to support ISSRM.

III. Extending Mal-Activity Diagrams regarding ISSRM coverage. (*SituationTO BE*).

2.1 Information System Security Risk (ISSRM) domain model

ISSRM domain model[[13]] is well structered in such away that it can present different concepts and their mutual relationships.The concepts are divided into three major categories:asset related-concepts, risk-related concepts and security-treatment concepts.

Asset-related concepts tell us about important assets of organization that deserve high priority of protection.*Asset* is anything valuable to organization and it supports organization to achieve its goal.*Business asset* represents information,processes and skill which add value to business of the organization while IS asset is an essential component of information system which supports business assets.*Security criterion* is the property of business asset which defines security needs(such as security objectives eg. *Availability*, *Confidentaility* and *Integrity*).

Risk-related concepts describes how we can define risk and its components.A *risk* is the combination of a threat with one or more vulnerabilities leading to a negatiive impact harming one or more of the assets.*Impact* describes the potential negative consequence of a risk incase of successfull excercise of the threat.*Event* is the combination of threat with one or more vulnerabilities.*Vulnerability* defines IS asset characteristic that exposes the weakness of either IS asset or group of IS assets.Attack that targets IS assets which can result into the harm of the assets is called *threat* while an agent responsible for launching an attack to harm IS assets is called *threat agent*.*Attack method* is describes the means used by threat agent to launch the attack.

Risk treatment-related concepts tell us about the means(such as *decisions*, *security requirements* and *controls*) which can be used either to mitigate or treat the risks.Risk treatment is the decision (e.g. avoidance, reduction,retention or transfer) to manage the risk.Security requirement is improvement of risk treatment decision to mitigate the risk.Control is a security measure implemented in respect to the identified security requirements.

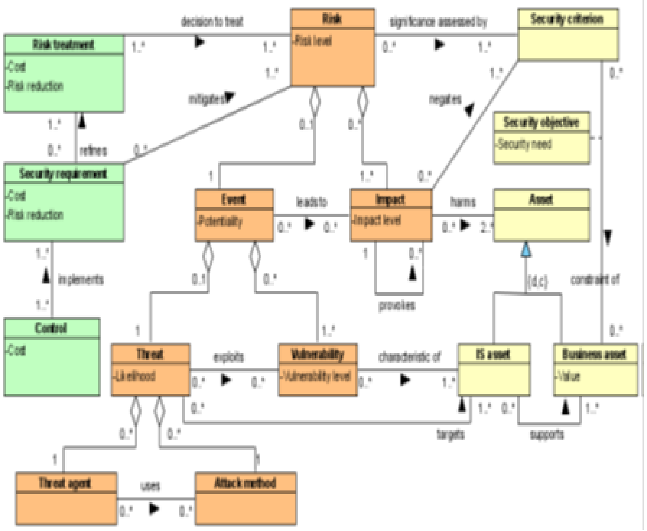

Figure 1: ISSRM Domain Model(Based on [[5]])

2.2 MAL-ACTIVITY DIAGRAMS

The concept of Malicious-Activity Diagrams defines the model process of exposing possible threats that attacker can perform by using same syntax and semantics as for normal UML diagrams but only the inverse of normal activities and actors used as swimlanes.The initial purpose of this concept is not to model the secure business processes but rather to model the process as-is together with the possible threats that attackers could perform towards these processes.Even though this concept is considered to be much better than misuse cases(open ended method) which doesnt give specific technical suggestion in a wide range but it has two major shortcomings;firstly, *not having any defined process on how to use Mal activity diagrams* and secondly,*not having perfect match with respect to ISSRM*.

2.3 Concrete Syntax

Consider *Online banking system example*(Fig 2. Asset model) an *acto*r(**Bank official**) initiates online banking process with an *Activity* (**Send email to Update home address**) by sending an email to **Client** via **Online Banking Server** which registers an email(*activity***Register email**) ready for **client** to open it.A **Client** opens an email(*activity***Open email**) and automatically *activity* (**Display email content**) provoked in the server to display the content of the email.Once a **client** agrees to Update home address(*activity***Agree to Update home address**) then *activity***Load website** is provoked and user gets an option to Enter his/her personal information(*activity***Enter login and password**).After entering his/her personal information then **Online Banking Server** checks client's validilty(*activity***validate the user**) and makes *decision*(**Is it Valid?**).If is valid then **Online Banking Server** redirects the **client**to home page (*activity***Redirect to the home page**) to update home address(*activity***Update home address**) otherwise error message is sent back to **client**(*activity***Send error message**).

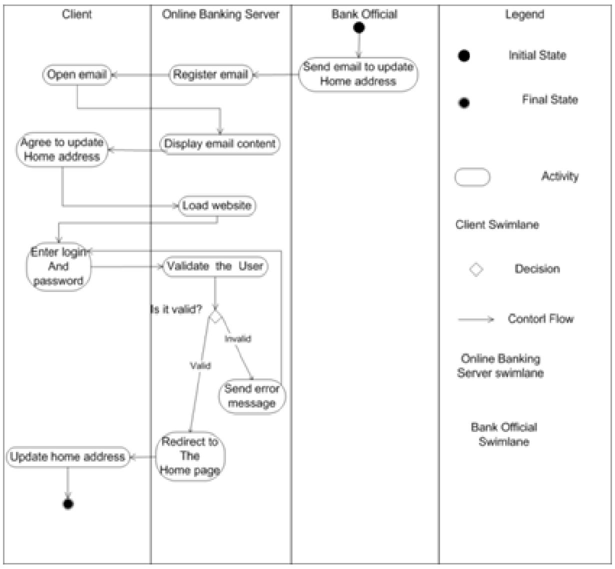

Figure 2: Asset model-Online banking server

Through the process descibed above(Online banking system),Mal Activity can define possible threat and identify security requirements as shown in the security threat model (Fig 3)whereby *Malicious actor* /*Hacker*(**Mal-Swimlane**)launched an attack to the online banking system by sending an email with malware(*Mal-Activity***Send email with malware**)unknowingly **Online Banking Server** registers infected email and when client opens an email,silently the malware is installed into the system and collects client's personal login information(*Mal-Activity***Capture login name and password**) as soon as client enters his/her personal login information.After capturing the login information then *malware*(**Mal-Swimlane**) sends client's login information to the *hacker*(*Mal-Activity***Send login name and password to hacker**) and finally hacker manages to make a successful attack after receiving client's login information(*Mal-Activity***Receive login name and password**).

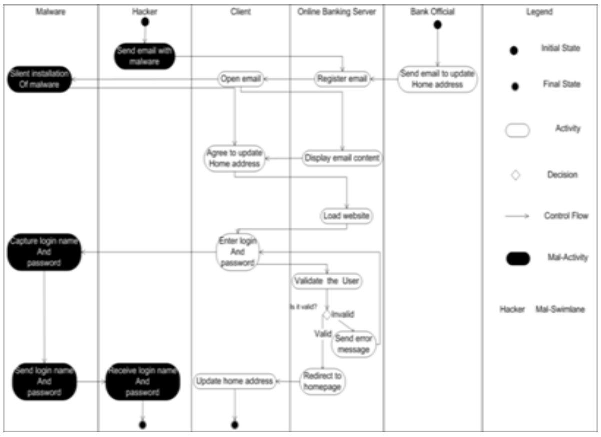

Figure 3: Threat Model-Online banking server

The security was introduced(fig 4 Security model) to mitigate risks where by mitigation activities such as Enable email **filtering**,**Setup anti-malware,** and **Enable traffic scanner** were introduced to mitigate security risk.

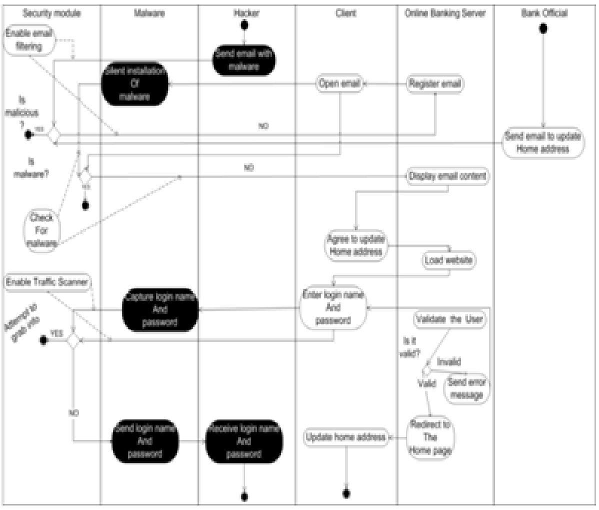

Figure 4: Security model-Online banking server

2.4 Abstract syntax

The abstract syntax is well descibed by metal model for Mal activity diagrams(figure 5) which is based on exististing metal model from previous research work(Sindre,2007 [1]).Currently Mal activity diagrams are composed of main three types of activities which are Activity, Mal-Activity and MitigationActivity.Anactivity is the specification of a parameterized sequence of behavior.A MitigationActivity shows the improvement of the process to avoid Malcious Activity.AMal-Activity is inverse of Activity which exposses the threat.AnySwimlane holds all the constructs of the Mal activity diagrams,it consists of Swimlane and Mal-swimlane whereby Swimlane consists of SwimlaneElement which is holding Activity,MitigationActivity and Decision.Mal-swimlane holds Mal-swimlaneElement which consists of Malactivity and Mal-decision.

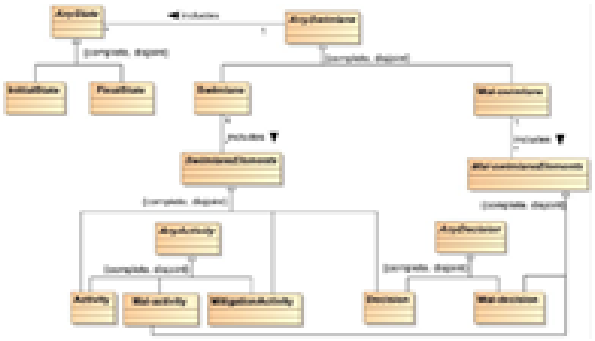

Figure 5: Meta Model of Mal Activity Diagrams(Based on [[1]])

3. Contribution

In this section i have briefly presented my achievement.

3.1 Syntax and semantic extension of Mal-Activity diagrams to support ISSRM

Limitations of Mal-Activity diagrams

As shown in table 1(Alligment of Mal-Activity with ISSRM),the coverage was not complete(blue highlited) due to fact that:

- Mal-Activity diagrams do not support security constraint of the static information(e.g. security criterion).
- Mal-Activity diagrams do not have enough constructs to cover essential concepts of ISSRM(e.g. security criterion,risk, impact, vulnerability, risk treatment).
- Mal-Activity diagrams do not provide guide on how to use its constucts.
- Mal-Activity diagrams do not have proper metal model.

3.2 Constructs

In order to cover the remaining essential ISSRM features(concepts), I have introduced several new constructs,Availability, Security criterion,mitigation link,leads to, Negates, Harms, Constraint of security,decision to treatto cover the missing parts in ISSRM domain model(Figure 6).

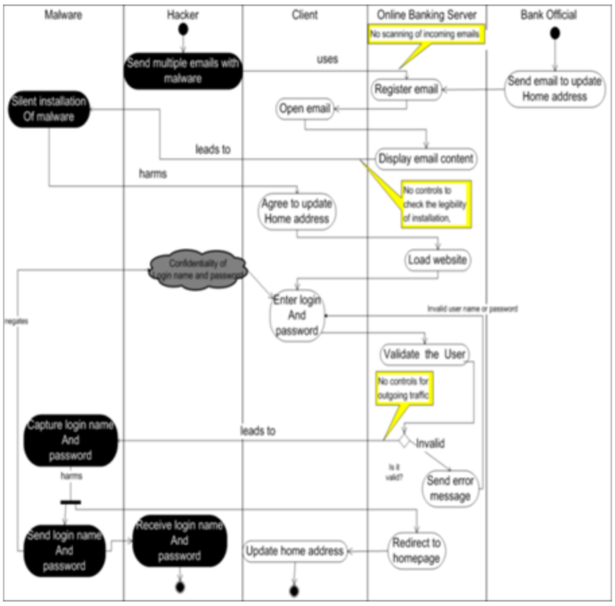
Malware
Hacker
Client
Online Banking Server
Bank Official
No scanning of incoming emails
uses
Send multiple emails with malware
Register email
Send email to update Home address
Silent installation Of malware
Open email
leads to
Display email content
harms
No controls to check the legibility of installation.
Agree to update Home address
Load website
Confidentiality of Login name and password
Enter login And password
Invalid user name or password
negates
Validate the User
No controls for outgoing traffic
Capture login name And password
leads to
Invalid
Is it valid?
harms
Send error message
Send login name And password
Receive login name And password
Update home address
Redirect to homepage

Figure 6: Improved Threat model-Online banking server

3.3 Extension of Mal-Activity diagrams regarding ISSRM coverage

Concrete Syntax

I have divided the concrete syntax of Mal-Activity diagrams into three parts, Asset related concepts, Risk related concept and Risk related treatment.With the help of additional constructs, we can now be able to express ISSRM relationships(e.g. supports, constraint of, exploits, targets, mitigates, negates, leads to,harms, decision to treat and uses).

a. **Asset related concepts**

ISSRM assets are represented by ***Activity, Decision, swimlane, ContolFlow***and ***Security criterion***.Business and IS assets are well connected using *supports*.ISSRM Support is represented by ***Control flow*** while ISSRM security criterion is represented by new*mal construct**Security criterion***and ISSRM relationship *constraint of* is represented by new *mal construct* ***constraint of security***.

b. Risk-related concepts

ISSRM Vulnerability is reprented by new *mal construct**Vulnerability***,threat agent is represented by ***Mal-swimlane*** while attack method represented by using ***Mal-swimlane***,***mal-activities,mal-decision***and***control flow***.Impact is represented by ***Mal-activities*** while combination of threat agent and attack method results into threat whereby *hacker* is using ISSRM relationship uses to hold attack methods which is represented by new *mal construct* ***uses***.Event is represented by combination of constructs which stand for threat and vulnerability which are connected by ISSRM relationship exploits which is represented by new mal construct ***exploits***.An event leed into impact under through ISSRM relationship leeds to which is represented by new *mal construct**leeds to***while the combination of event and impact results into Risk.

c. Risk treatment concepts

Finally, after the improvement of Mal-activity diagrams risk can be treated and the protection of *confidentiality* is made manageable(Table 1 .Alignment between improved Mal-Activity diagrams and ISSRM).ISSRM Security requirements is represented by *mal construct**Mitigation Activity*** which mitigates risk through ISSRM relationship mitigates which is also represented by new mal construct ***mitigation link***.Control is represented by ***swimlane*** while Risk treatment is represented by combination of construct that represent security requirements,mitigates,decision to treat,implement and control,it treats risk through ISSRM relationship decision to treat which is represented by new construct ***decision to treat***.

3.4 Alignment between Mal-Activity diagrams and ISSRM(Comparison)

In this section you can find the comparison between the existing Mal-Activity diagrams(Table 1) and Improved(/ proposed) Mal-Activity diagrams(Table 2) with regarding ISSRM coverage.If you observe the fulfilment of the the two tables,you may figure out that there are several ISSRM security concepts that couldnt be covered by Mal-Activity diagrams(Table 1) due to the existing limitations of the language but we can finally see them covered by the improved Mal-Activity diagrams(Table 2).

4. Conclusion and future work

Conclusively,the study has exposed the limitations of Malicious Activity Diagrams and proposed the solutions to those limitations as follows:

i. In support of security constraints,the study has introduced several new constructs that will enable Malicious Activity Diagrams to catch even static information such as security criterion.

ii. In support of essential risk related concepts,the study has proposed several other constructs that will represent risk, impact,vulnerability as well as risky treatment.

iii. In support of the usage of constructs and their relationship the study has clearly elaborated the proper use of constructs and derived relationships that can bring about semantic sense to Malicious Activity Diagrams.

iv. The study has also proposed some procedures to be followed by software/systems developers in order to construct and implement security critical systems[8]

Therefore the output of this study will be very helpuf not only to Systems/software developers but it will also set free from limitations whoever wishes to make a proper use of Malicious Activity Diagrams.I am looking forward to design a new meta model of improved Mal-Activity diagrams.

Acknowledgment.

I thank God for this achievement.I would also like to acknowledge my friends Mr. and Mrs. Michael O'Bryan (USA), Dr. Raimundas Matulevicius (Estonia), Mr. and Mrs. Alec Watts (UK), Prof. Marlon Dumas (Estonia), Dr.Ulrich Norbisrath (Germany), all members of LIS department at Tumaini University-Dar es salaam,Godwin Gondwe(Tanzania) and last but not the least my family for their support, guidance and encouragement.

Table 1:Alligment of Mal-Activity diagrams with ISSRM-Online banking server

ISSRM Domain Model		**Mal Activity**	**Example**
Asset Related	**Aset**		
	Business	--Activity, Decision, ContolFlow constructs	Send email to update the home address,Receive email,Open email,Load the website ,Put the username and password,Push login button,Update the home address,LogoutIs filter working?Is anti-malware working?Is traffic scanner working?Online banking server

	IS aset	-Swimlane -Activity, decision (connected using Control flow constructs)	Bank official, Online banking server,Validate the user,Redirect to the home page, Send error message,Is it valid?
	Security criterion	-	Confidentiality of login name and password.
Risk Related	**Risk**	-	-
	Impact	Mal-Activities	Silent installation of malware, Capture login name and password, Send Login name and password to hacker
	Event	-	-
	Vulnerability	-	No scanning of incoming email,No controls to check the legibility of installation,No controls for outgoing traffic
	Threat	-	-
	Threat Agent	Mal-swimlane	Hacker
	Attack Method	- Mal-Activities, -Mal-Decision -Control flow -Mal-swimlane	Send an email with malware, Receive login name and password, Malware
Risk Treatment	**Risk Treatment**	-	-
	Security reqirements	MitigationActivity	Enable email filtering, Setup anti-malware, Enable traffic scanner
	control	Swimlane	Security module

Table 2:Alligment of Improved Mal-Activity diagrams with ISSRM-Online banking server

ISSRM Domain Model		**Mal Activity**	**Example**
Asset Related	**Aset**		
	Business	-Activity, Decision, ContolFlow constructs -Objects used to perform activities(implicit)	Send email to update the home address, Receive email,Open email, Load the website , Put the username and password, Push login button, Update the home address, LogoutIs filter working?Is anti-malware working?Is traffic scanner working? Online banking server
	IS aset	-Swimlane -Activity,decision(connected using Control flow constructs)	Bank official, Online banking server, Validate the user, Redirect to the home page, Send error message, Is it valid?
	Security criterion	*-Security criterion*	Confidentiality of login name and password.

Risk Related	**Risk**	*-combination of event and impact*	*Send email with malware, Silent installation of malware, Send the login name and password, Receive login name and password,Hacker, No scanning of incoming email, No controls to check the legibility of installation, No controls for outgoing traffic*
	Impact	Mal-Activities	Silent installation of malware, Capture login name and password, Send Login name and password to hacker
	Event	*-combination of threat and vulnerability*	Send email with malware, Silent installation of malware, Send the login name and password, Receive login name and password, Hacker, No scanning of incoming email,No controls to check the legibility of installation, No controls for outgoing traffic
	Vulnerability	*- vulnerability*	No scanning of incoming email, No controls to check the legibility of installation, No controls for outgoing traffic
	Threat	*-combination threat agent and Attack method*	*Send email with malware, Silent installation of malware, Send the login name and password, Receive login name and password,Hacker*
	Threat Agent	Mal-swimlane	Hacker
	Attack Method	-Mal-Activities, Mal-Decision and Control flow -Mal-swimlane	Send an email with malware, Receive login name and password, Malware
Risk Treatment	**Risk Treatment**	*- Described by combination of control ,mitigation activity ,decision to treat,implements and security requirements supported by control flow constructs*	*Enable email filtering,Setup anti-malware, Enable traffic scanner*
	Security reqirements	-MitigationActivity	Enable email filtering, Setup anti-malware, Enable traffic scanner
	control	-Swimlane	Security module

5. REFERENCES

[1] Sindre G., “Mal-Activity Diagrams for Capturing Attacks on Business Processes”. Inproceedings of the Working Conference on Requirements Engineering: Foundation forSoftware Quality, 2007.

[2] Andrey Naumenko and Alain Wegmann , “A Metamodel for the Unified Modeling Language”,EPFL-IC-LAMS, CH-1015 Lausanne, Switzerland,2002.

[3] Raimundas Matulevi_cius, “ Improving the Syntax and Semantics of Goal Modelling Languages”, University of Namur, Belgium,2008.

[4] Mohammad Jabed Morshed Chowdhury,Dr. Raimundas Matulevičius,Prof. Guttorm Sindre,Dr. Peter Karpati,“Modeling Security Risks at the System Design Stage”,Master’s thesis,June, 2011.

[5] Nicolas Mayer,Eric Dubois,Raimundas Matulevicius,PatrickHeymans,“Towards a Measurement Framework for Security Risk Management ”,CRP-Henri Tudor – CITI,PReCISE, University of Namur,rue Grandgagnage 21, B-5000 Namur, Belgium,2008.

[6] K. Hinkelmann, D. Karagiannis, R. Klein, N. Stojanovic (eds.): “Semantic Business Processand Product Lifecycle Management”. Proceedings of the Workshop SBPM 2007, CEUR Workshop Proceedings, ISSN 1613-0073, online CEUR-WS.org/Vol-251/, Innsbruck, April 7, 2007.

[7] Bresciani P., Perini A., Giorgini P., Fausto G. and Mylopoulos J., “TROPOS: an Agentoriented Software Development Methodology”. Journal of Autonomous Agents and Multi-Agent Systems, Volume 25, pages 203–236, 2004.

[8] Lee S. W., Gandhi R., Muthurajan D., Yavagal D. and Ahn G. J., “Building problem domain ontology from security requirements in regulatory documents”. In proceeding of the International Workshop on Software Engineering for Secure Systems, 2006.

[9] Mitnick Kevin. “The Art of Deception: Controlling the Human Element of Security”. WileyPublishing, Inc., Indianapolis, 2002.

[10] Axel van Lamsweerde,“Elaborating Security Requirements by Construction of Intentional Antimodels”.In the proceedings of the 26th International Conference on Software Engineering, 2004.

[11] Dubois E., Heymans P., Mayer N. and Matulevičius R., “A Systematic Approach to Define the Domain of Information System Security Risk Management”. Book published fromSpringer-Verlag, ISBN: 978-3-642-12543-0,2010.

[12] Christopher Alberts,Audree Dorofee,James Stevens,Carol Woody , “Introduction to the OCTAVE® Approach”,Hanscom AFB, MA 01731-2116,August 2003.

[13] Haley C. B., Moffett J. D., Laney R. and Nuseibeh B., “A Framework for Security.Requirements Engineering”. In Proceedings of the 28th International Conference on Software Engineering, pages 35-42. ACM Press, 2006.

[14] Nicolas Mayer, Patrick Heymans, Member,IEEE and Raimundas Matulevicius,“Design of a Modelling Language for Information System Security Risk Management”,2007.

[15] SANS Institute , “An Introduction to Information System Risk Management”,2007.

[16] Gary Stoneburner, Alice Goguen, and Alexis Feringa,“Risk Management Guide forInformation Technology Systems”,NIST Special Publication 800-30,Natl. Inst. Stand. Technol. Spec. Publ. 800-30, 54 pages,July 2002.

[17] Steve Elky,“An Introduction to Information System RiskManagement”,SANS Institute 2007,May 31, 2006.