MIS Review 22(1/2), September (2016)/March (2017), 59-71.

Security modeling tool for information systems: Security Oriented Malicious Activity Diagrams Meta Model Validation

Othmar Othmar Mwambe[1], Isao Echizen[2]
[1]Graduate School of Engineering and Science, Shibaura Institute of Technology, Japan
[2]National Institute of Informatics, Chiyoda, Japan

ABSTRACT: *Various information system security risk management approaches and security modeling languages have been used to address information system security threats. However, the dramatic growth of information system security attacks remains a nightmare. As many other security modeling languages, Mal-Activity Diagrams (MAD) have also been used to model system malicious processes and risk mitigation processes but due to their syntactic and semantic drawbacks, Security Oriented Malicious Activity Diagrams (SOMAD) were introduced in our previous study as an extension of MAD. In this study SOMAD Meta model comprehensiveness and applicability have been validated by using industrial survey. The obtained results show that SOMAD Meta Model is a comprehensive tool enough to address information system security issues at large scope.*

KEYWORDS: *Mal-Activity Diagrams, security modeling languages, Information system security, security risks management, requirements engineering, security risk management approaches, management information systems, security oriented malicious activity diagrams*

1. Introduction

The dramatic growth of ransomware attacks (Scaife et al., 2016) reflects not only the transformation of cyber security attacks towards software applications but also indicates the need for information system security measures adjustment (Mailloux et al., 2016) as they might be inconsistent with modern attack methods (Jasiul et al., 2014). For decades various Information system security management approaches have been used to address information systems security issues, commonly used approaches include Operationally Critical Threat, Asset, and Vulnerability Evaluation methodology (OCTAVE), Security Quality Requirements Engineering (SQUARE), National Institute of Standards and Technology (NIST), CCTA Risk Analysis and Management Methodology (CRAMM), Method for Harmonized Analysis of Risk (MEHARI), Expression of Needs and Identification of Security Objectives methodology (EBIOS) and Information System Security Risk Management Domain Model (ISSRM). In support of such approaches, various security modeling languages have been used to address information system security issues during the designing stage of information systems, Misuse cases Diagrams, Secure Tropos, Mal-Activity Diagrams, and Secure UML are commonly used languages, such tools have played a great role in supporting security requirements definition as well as information system security at large; however, growth of information system security threats remains a challenge (Geiger, 2014).

Security modeling languages are always working with respect to their defined domain meta models and strength of such tools have commonly been evaluated using alignment approaches for instance with ISSRM (Dubois et al., 2010; Sindre,2007; Mwambe, 2013). Mal-Activity Diagrams (MAD)

as many other security modeling tools was previously being aligned with ISSRM and showed some limitations towards ISSRM risk management process coverage (Mwambe, 2013). To address MAD limitations, additional syntaxes were proposed that led into the syntactic and semantic extension of MAD, Security Oriented Malicious Activity Diagrams (SOMAD) (Mwambe & Echizen, 2017). Security Oriented Malicious Activity Diagrams (SOMAD) is a scenario-based approach that relies on its proposed SOMAD Meta Model which is validated in this study. SOMAD Meta Model is designed to handle normal processes, malicious processes as well as risk treatment processes of information system, this property enables it to take advantage over previously used MAD Metal model. SOMAD meta model complies with Information System Security Risk Management Domain Model (ISSRM) and its comprehensiveness towards ISSRM process coverage and applicability have been evaluated and validated by industrial survey the results show that SOMAD is comprehensive enough to address information system security issues at large scope (83.75%).

This paper consists of six sections, related works and background studies have been briefly discussed in the following chapters; however, our contribution starts from section three.

2. Background study and related work

2.1 Information systems Security risk management approaches

These are procedures and written guides that define how security risk management is implemented so as to preserve the objectives of information security.

2.1.1 The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology

Octave is a risk-based strategic assessment and planning technique for security risk management (Alberts et al., 2003). It is a process driven methodology to identify, priorities and manage security risks in two aspects: operational risk and security practices. In OCTAVE approach Security risk management process is completed based on three-phased approach: Build Asset-Based Threat Profiles, Identify Infrastructure Vulnerabilities and Develop Security Strategy and Plans.Octave approach does support small organisations (OCTAVE-s) as well as big organizations (OCTAVE®) and its distinct characterestics are self directed approach and team based (Alberts et al., 2003).

2.1.2 The Security Quality Requirements Engineering (SQUARE) methodology

This approach is focused on requirement engineering process to convey clear understanding of security risk management for information systems. It consists of nine steps and each step identifies participants, inputs, suggested technique and final output. Its process involves interaction of team of requirement engineers and IT project's stake holders. This approach is most effective and accurate when conducted with a team of security expertise with requirement engineers and stake holders of the project (Haley et al., 2008).

2.1.3 National Institute of Standards and Technology(NIST) methodology

This is a risk-based approach for the development of effective risk management process of information systems as it sets basic principles on connection between business drivers and cybersecurity activities (Cybersecurity, 2014). It consists of three parts: Framework Core-identifies cybersecurity activities, impact and guide for support; Framework Implementation Tiers-identifies risk and mitigation process; Framework profile -shows the outcomes with respect to business requirements. It is flexible and it can cover broad security requirements management processes (Cybersecurity, 2014).

2.1.4 CCTA Risk Analysis and Management Methodology (CRAMM)

This is a qualitative security risk management approach developed by UK's Central Computing and Telecommunication Agency (CCTA) (Yazar, 2002). In this approach risk management process is completed through three stages: identification and valuation of assets –defines data, application software and physical assets; Threat and vulnerability assessment-identifies threats and vulnerabilities; and Risk calculation- calculates risk for each asset.

2.1.5 Method for Harmonized Analysis of Risk (MEHARI)

This is risk analysis (RA) and risk management(RM) method based approach developed by French association of information security professionals (Mihailescu, 2012). Risk analysis is completed through five stages: Context establishment, stakes analysis and assets classification, risk identification, risk analysis and risk evaluation. Risk management is complete through four stages: Risk assessment, Risk treatment, risk acceptance and risk communication.

2.1.6 Expression of Needs and Identification of Security Objectives methodology(EBIOS)

This is French central information systems security division (DCSSI) approach which is widely used in public and private sectors. The approach bases on security requirements and objectives of information systems whereby risk analysis process is completed through five stages: context and environmental analysis, security requirements evaluation, risky analysis, identification of risk objectives and determination of security requirements. It is flexible approach as it can easily be adjusted to support other approaches (Hemery et al., 2007).

2.2 Information System Security Risk Management (ISSRM)

ISSRM is a concepts based approach derived from different security related standards (La Rosa & Soffer, 2013). Risk management goes through iterative and continuous process (Figure 1). Risk management process based on asset, risk and risk treatment concepts. Asset-related concepts define things that add value to the organization (information and business assets); Risk-related concepts define components of risk (threat and vulnerability); Risk treatment-related concepts define means of which risk can be mitigated.

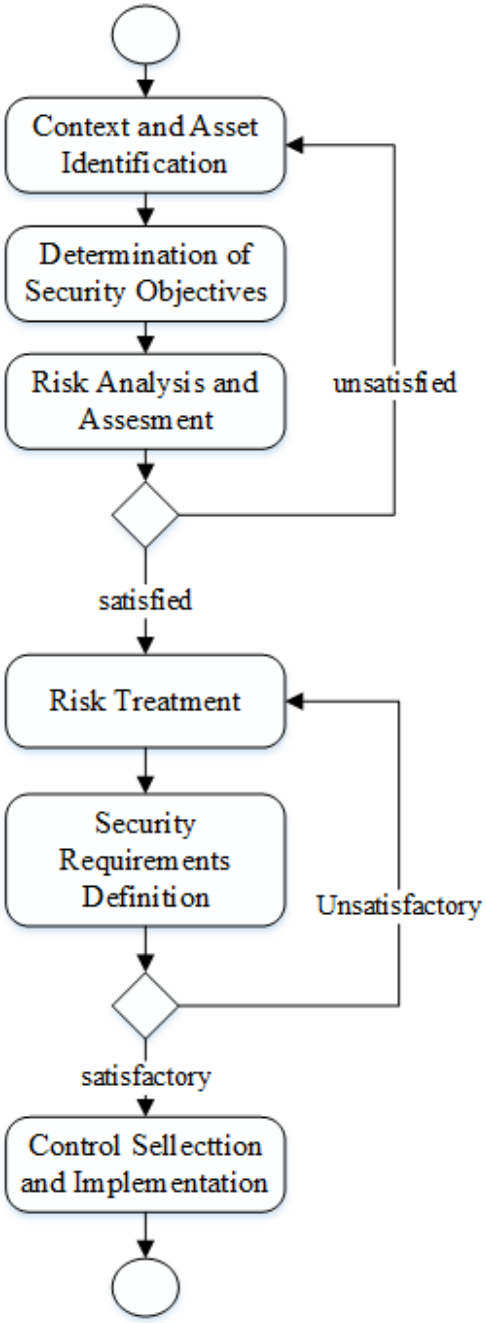

Figure 1 ISSRM Process

Why ISSRM? – Unlike other security risk management approaches, ISSRM is applicable during both information system development and analysis of existing systems (La Rosa & Soffer, 2013) as it integrates risk management process and information system development (Herrmann et al.,2011).This makes ISSRM being suitable for alignment in determination of modeling languages strength (Abbass et al., 2016).

2.3 Related work

Development of security modeling tools with respect to ISSRM process has been an interest of many previous researchers (Mayer, Heymans, & Matulevicius, 2007; Soomro &Ahmed, 2013) due to comprehensiveness of ISSRM domain model. Many previous researchers used ISSRM alignment approach to evaluate their proposed approaches (Chowdhury et al., 2012; Soomro &Ahmed, 2013). Mal-Activity Diagrams and misuse cases both use to model system malicious process, Chowdhury et al. (2012) aligned Mal-activity diagrams with ISSRM to support security requirements definitions, this approach is very useful as it supports software developers during requirement elicitation and designing stage. Mal-Activity is a modified UML Activity (shaded with black color) intended to capture malicious processes, Malicious processes also includes malicious decisions which used by the threat agent (hacker) to harm the system, alignment with ISSRM enables researchers not only to test the strength of the tools but also requirements coverage. Unlike Chowdhury et al. (2012), our approach does not only base on alignment but also semantic extension of Ma-Activity diagrams, SOMAD meta model.

3. Security Oriented Malicious Activity Diagrams (SOMAD)meta model

3.1 SOMAD meta model

Risk management using SOMAD meta model based on three processes: **normal process**, **malicious process** and risk **treatment process**. The Meta Model consists of three main swim lanes: ***Swimlane, Mal-Swimlane*** and ***Control-Swimlane.*** These swim lanes are structured in such a way that One *AnySwimlane* may include many *AnyState*, One *Swimlane* may include many *SwimlaneElements*, one *Mal-Swimlane* may include many *Mal-SwimlaneElements*, one *control-Swimlane* may include many *Control-SwimlaneElements* and all the elements are complete and disjoint (Figure 2).

All processes start with initial state and end with final state, a process may have more than one final state but single initial state. *Swimlane* captures normal information system processes, all normal activities, decisions, security criterion and vulnerabilities of information system are defined by this swim lane; *security criterion* defines security objective of which security requirements (*mitigation activity*) is fulfilled for, while vulnerability defines system weakness that may result into system security breach. Vulnerability is not only the absence of measure; it can also be the existence of an element that makes the system vulnerable to the threats. Malicious processes are captured using *Mal-Swim lane* where all malicious activities and decisions are defined. Risk mitigation processes are captured using *control-Swimlane* where all mitigation activities and decisions to treat are defined. *Control-Swimlane* enables SOMAD metal model to handle risk treatment.

Unlike the meta model in our previous study, current improved meta model has replaced vulnerability with *vulnerable activity*. It has removed security criterion, instead it has defined security criterion as the property of business assets.

3.1.1 Structure flow

Start : SOMAD start with *InitialState* and end with *FinalState*. SOMAD activities are divided into three categories: *Activity*, *Mal-Activity* and *MitigationActivity*. *AnySwimlane* holds all constructs of Security Oriented Malicious Activity Diagrams.

Swimlane includes *SwimlaneElement*, which consists of *VulnerabilityActivity*, *Activity* and *Decision*. *Activity* defines parameterized sequence of behavior. *Decision* defines branching based on either positive or negative conditions. *SecurityCriterion* defines system security objective (security requirement fulfillment) and it is the property of business assets. *VulnerabilityActivity* defines system vulnerability and it identifies activities that can lead to the system security breach.

Mal-Swimlane includes *Mal-SwimlaneElement*, which is composed of *Mal-Activity* and *Mal-Decision*. *Mal-Activity* defines activities performed by threat agent to harm normal process. *Mal-Decision* defines threat agent decision to fulfill malicious goal.

Control-Swimlane includes *Control-SwimlaneElement*, which consists of *MitigationActivity* and *Decision to treat*. *MitigationActivity* defines process improvement to overcome threat. *Decision to treat* defines the decision performed to eliminate the threat.

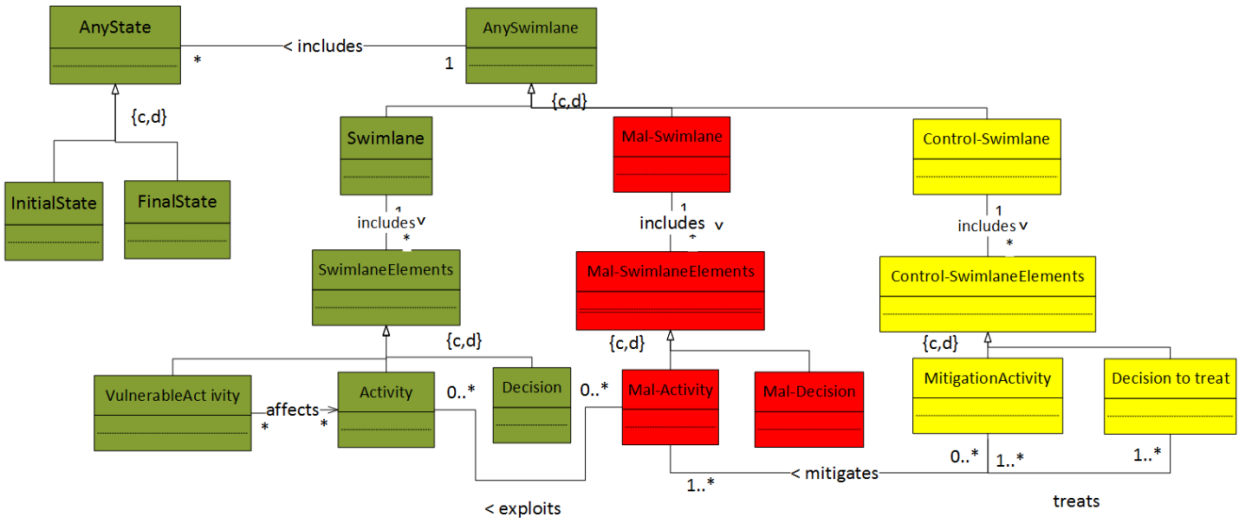

Figure 2 SOMAD meta model

4. Evaluation and validation

SOMAD meta model Comprehensiveness was evaluated based on the analysis of the malicious scenarios applied on test case study “student online information system- SAIS". Evaluation included both alignment approach as well as experimental analysis of the industrial survey. The data was analyzed using IBM SPSS Statistics.

4.1 SOMAD meta model alignment with ISSRM domain model

SOMAD meta model and other security modeling tools were aligned with ISSRM Domain model towards ISSRM risk management process coverage. Out of 13 key security features of ISSRM domain

model, SOMAD meta model could fully address all features of ISSRM domain model (Table1) and took advantage over other modeling tools.

Table 1 Security modeling languages alignment with ISSRM

ISSRM Domain Model		Misuse cases Diagrams Constructs	Secure Tropos Constructs	Secure UML Constructs	Mal-Activity Diagrams Constructs	SOMAD Constructs
Asset-related concepts	Asset	Actor, use cases	Actor, goal, plan, softgoal	Modelelement Class	-	
	Business assets			Class attributes	Activity, decision, control flow	Activity, decision, control flow
	IS assets			Role class, association permission, operation	Swimlane, activity, control flow	Swimlane, activity, control flow
	Security criterion	-	Softgoal,security constraint	-	-	Security constraint
Risk-related concepts	Risk	-	-	-	-	Combination of event and impact
	Threat	Misuser, misuse case	Goal, plan	Role class, association permission	Mal-swimlane,mal-activities, mal-decision	Mal-swimlane,mal-activities, mal-decision
	Threat Agent	misuser	Actor	Role class	Mal-swimlane	Mal-swimlane
	Attack method	Misuse case	Attacks relation, plan	Association permission attributes	Mal-activities, mal-swimlane, mal-decision, control flow	Mal-activities, mal-swimlane, mal-decision, control flow
	Vulnerability	-	Belief	-	-	Vulnerability
	Impact	-	Softgoal and threat combination	-	Mal-activites	Mal-activities
	Event	-	threat	-	-	Combination of threat and vulnerability
Risk treatment-related concept	Risk treatment	-	-	-	-	Combination of control swimlane, mitigation activities,decision to treat and control flow
	Security requirement	Use case	Actor, goal, softgoal, security constraint	Constraint ,constrained elements	Mitigation activity	Mitigation activity
	Control		additional model	additional model	swinlane	Control-swimlane

4.2 SOMAD meta model comprehensiveness validation

Validation based on the findings of the industrial survey that was conducted not only to obtain experts' approval on the comprehensiveness but also to test industrial applicability of the proposed tool. Survey involved 12 experts whereby respondents were provided with detailed description of SOMAD modeling tool and they were supposed to model and give complete analysis of the given scenarios by responding to the questionnaires, response time took around 15-20 minutes. The questionnaires were designed to test the comprehensiveness of SOMAD meta model with respect to ISSRM process coverage.

Scenarios: Hacker launched two attempts to harm student online information system. "Firstly, he flooded student online information system with multiple fake requests; Secondly, hacker used malware to

steal students 'credentials by altering normal flow of online registration process and redirect student to hacker's page".

4.2.1 Demographic information of the respondents and response rate

100% response rate was attained whereby 12 respondents participated in the study, including 7 software developers (66.7%),2(16.7%) system analysts and 2 (16.7%) security experts. 91.7% of respondents were males except one female (8.3%). Regarding education, majority (66.7%) of the respondents were holding masters, many were PhD students, 2 (16.7%) were holding bachelor degree, and 2 PhD (16.7%). All respondents had at least three years working experience in their fields of expertise.

4.2.2 Asset identification

Table 2 shows respondents' rate of response to the questionnaires, "able" shows number respondents who provided correct answers, "not able" false answers and "not sure" are those who left the question blank. 91.7% of respondents successfully identified both business and information system assets (IS).

Table 2 Asset Identification

Result	Frequency	Percentage
Able	11	91.7%
Not able	1	8.3 %
Not sure	0	0%
Total	12	100%

4.2.3 Security objectives determination

75% of the respondents managed to determine security objective defined by the security requirement, two (16.7 %) respondents were not able to determine security objective as they confuse with security requirement and one (8.3%) respondent was not sure (Table 3).

Table 3 Security Objective determination

Result	Frequency	Percentage
Able	9	75 %
Not able	2	16.7 %
Not sure	1	8.3%
Total	12	100%

4.2.4 Risk assessment and analysis

83.3% of respondents were able to identify the vulnerability of information system(SAIS),91.7 % of respondents were able to identify system threat, 83.3% of the respondents were able to identify malicious event, 91.7% managed to identify the attack method used by the threat agent to harm the system and only 75% managed to identify security requirements while 25% failed to identify security requirements (Table 4).

Table 4 Risk assessment and analysis

Result	**Frequency**			
	Able	**Not Able**	**Not sure**	**Total**
Vulnerability	10 (83.3%)	1 (8.3%)	1 (8.3%)	12 (100%)
Threat	11 (91.7%)	1 (8.3)	0	12 (100%)
Event	10 (83.3%)	1 (8.3)	1 (8.3)	12 (100%)
Attack Method	11 (91.7%)	1 (8.3)	0	12 (100%)
Security requirements	9 (75%)	3 (25%)	0	12 (100%)
Average	**85%**	**11.65 %**	**3.32 %**	

4.2.5 Risk treatment

83.3% of the respondents successfully captured security risk treatment process (Table 5) whereby 83.5% of software developers as well as all (100%) system analysts and all (100%) security experts successfully managed to capture risk treatment process and thus completed ISSRM process (Figure 1).

Table 5 Risk treatment

	Frequency	Percentage
Able	10	83.3 %
Not able	2	16.7 %
Not sure	0	0%
Total	12	100%

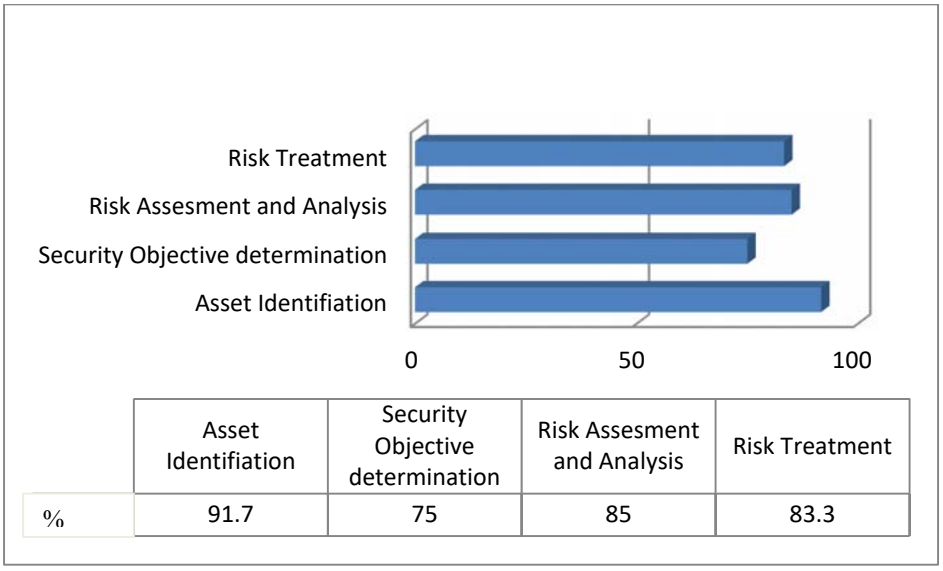

Figure 3 ISSRM Process coverage

4.3 Discussion

Alignment of modeling languages with ISSRM domain model determines the strength of the security modeling tool as it provides clear understanding of the differences and similarities exist in various modeling tools. Regarding the ISSRM risk management process, this wide coverage of ISSRM process gives SOMAD meta model capability to address security issues of information systems at large scope.

Successful asset identification and security objectives determination implies that SOMAD metal model is not only capable of addressing ISSRM assets but also security criterion of information system .Vulnerability, threat and event identification justifies SOMAD meta model is capable of addressing ISSRM risk management process at large scope in turn it can successfully support security analysis of information system. However, 25% of respondents who could not clearly identify security requirements (Table 4) were software developers, due to conflicting requirements elicitation. Thus conflict in requirements elicitation during system design may have significant effect not only on the system but also on system security analysis.

Successful address of risk treatment (Table5) implies that SOMAD metal model is capable of covering ISSRM risk management process at large scope and also reflects the contribution of newly added syntaxes. Huge number of experts successfully managed to capture risk treatment process (Figure 3), this implies that SOMAD can be used not only by software developers but also system analysts and security experts. On average the SOMAD metal model manages to cover 83.75% of ISSRM process (Figure 3), this implies that SOMAD can successfully address information systems security issues at large scope.

5. Managerial Implications

This study suggests that Security Oriented Malicious Activity Diagrams (SOMAD) meta model is industrially applicable and comprehensive enough to address information system security issues at large scope. One of the managerial implications from the results and discussion is the need for the security modeling tools to provide comprehensive framework that can enable software engineers, security experts and system analysts to capture all system security requirements with respect to ISSRM concepts (assets, risk and risk treatment). Fully coverage of ISSRM concepts strengthens the modeling tool as it provides security experts with needful support to address information system security issues.

Risk treatment plays a crucial role in determination of information system security. However, it can only be accomplished successfully if the security requirements and controls are well defined. The introduction of control features and security requirements definition enables software developers and security experts to fully address all system security requirements with respect to ISSRM process.

Non-functional requirements (e.g. availability, vulnerability, confidentiality, integrity etc.) play a crucial role not only in determination of security objectives but also in implementation of organizational security criterion. Having non-functional requirements well defined and emphasized enables software

developers, system analysts and security experts to take such requirements into consideration during requirements elicitation, system design and system analysis.

Both information and business assets are very important and characteristics of such assets determine system security requirements. Thus, illustrating features that define such characteristics enable software developers, security analysts and security experts to determine security objectives and implement objective risk treatment process. Such properties also play crucial role in determination of security objectives during system security analysis.

Requirements conflict resolution plays a very crucial role not only during the requirements elicitation but also in the designing of information systems. It is critical success factor in requirements engineering. Based on the obtained result and discussion, having conflicting requirements is inevitable especially when multiple stakeholders are involved. Thus, it is indeed very important to give conflict resolution high consideration as it does have impact on system security analysis.

6. Conclusion

The study has validated comprehensiveness of Security Oriented Mal-Activity Diagrams(SOMAD) meta model toward ISSRM process coverage and also tested applicability of the model. The results show that SOMAD meta model is applicable and comprehensive security tool for management of information systems security, it can be useful tool not only for software developers but also security experts and system analysts. It is easily understood as it provides clear description of the attack and risk mitigation activities. Due to time constraints and nature of the study, the survey could not include large number of respondents as the analysis of the scenarios provided during the industrial survey was time consuming, however majority of the respondents participated in the survey managed to clearly model and analyze risk scenarios and their treatment processes. Thus, SOMAD meta model can address information system security issues at large scope.

References

Abbass, W., Baina, A., & Bellafkih, M. (2016, March). Survey on information system security risk management alignment. In *Information Technology for Organizations Development (IT4OD), 2016 International Conference on* (pp. 1-6). IEEE.

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). *Introduction to the OCTAVE Approach.* Pittsburgh, PA, Carnegie Mellon University.

Chowdhury, M. J. M., Matulevičius, R., Sindre, G., & Karpati, P. (2012, March). Aligning mal-activity diagrams and security risk management for security requirements definitions. In *International Working Conference on Requirements Engineering: Foundation for Software Quality* (pp. 132-139). Springer, Berlin, Heidelberg.

Cybersecurity, C.I. (2014). Framework for Improving Critical Infrastructure Cybersecurity.

Dubois, É., Heymans, P., Mayer, N., & Matulevičius, R. (2010). A systematic approach to define the domain of information system security risk management. In *Intentional Perspectives on Information Systems Engineering* (pp. 289-306). Springer, Berlin, Heidelberg.

Haley, C., Laney, R., Moffett, J., & Nuseibeh, B. (2008). Security requirements engineering: A framework for representation and analysis. *IEEE Transactions on Software Engineering*, *34*(1), 133-153.

Hemery, H., Akmouche, W., & Tatout, F. (2007). Utilisation de la methodologie EBIOS en securite globale. *REE. Revue de l'électricité et de l'électronique*, (10), 29-125.

Herrmann, A., Morali, A., Etalle, S., & Wieringa, R.J., (2011). RiskREP: risk-based security requirements elicitation and prioritization. In *Perspectives in Business Informatics Research*. Springer Verlag.

Jasiul, B., Śliwa, J., Gleba, K., & Szpyrka, M. (2014, September). Identification of malware activities with rules. In *Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on* (pp. 101-110). IEEE.

La Rosa, M., & Soffer, P. (Eds.). (2013). Business Process Management Workshops: BPM 2012 International Workshops, Tallinn, Estonia, September 3, 2012, Revised Papers (Vol. 132). Springer.

Mailloux, L. O., McEvilley, M. A., Khou, S., & Pecarina, J. M. (2016). Putting the" Systems" in Security Engineering: An Examination of NIST Special Publication 800-160. *IEEE Security & Privacy*, 14(4), 76-80.

Mayer, N., Heymans, P. & Matulevicius, R. (2007). Design of a Modelling Language for Information System Security Risk Management. In *RCIS* (pp. 121-132)

Mihailescu, V. L. (2012). Risk analysis and risk management using MEHARI. *J. Appl. Bus. Inf. Syst.*, *3*, 143.

Mwambe, O. O. (2013). Syntactic and Semantic Extensions of Malicious Activity Diagrams to Support ISSRM. *International Journal of Computer Applications*, *67*(4).

Mwambe, O. O., & Echizen, I. (2017, March). Security Oriented Malicious Activity Diagrams to Support Information Systems Security. In *Advanced Information Networking and Applications Workshops (WAINA), 2017 31st International Conference on* (pp. 74-81). IEEE.

Scaife, N., Carter, H., Traynor, P., & Butler, K.R. (2016, June). Cryptolock (and drop it): stopping ransomware attacks on user data. In *Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on* (pp. 303-312). IEEE.

Sindre, G. (2007, June). Mal-activity diagrams for capturing attacks on business processes. In *International Working Conference on Requirements Engineering: Foundation for Software Quality* (pp. 355-366). Springer, Berlin, Heidelberg.

Soomro, I., & Ahmed, N. (2013). Towards security risk-oriented misuse cases. In *International Conference on Business Process Management* (pp. 689-700). Springer, Berlin, Heidelberg.

Yazar, Z. (2002). A qualitative risk analysis and management tool–CRAMM. *SANS InfoSec Reading Room White Paper*, *11*, 12-32.

About the authors

Othmar Othmar Mwambe*
Graduate School of Engineering and Science, Shibaura Institute of Technology
3 Chome-7-5 Toyosu, Koto, Tokyo 135-8548
Email: mg17007@shibaura-it.ac.jp

Isao Echizen
National Institute of Informatics
Chiyoda, Tokyo, 101-8430, Japan
Email: iechizen@nii.ac.jp

*Corresponding author

Othmar Othmar Mwambe is a graduate student at Shibaura Institute of Technology (SIT). He studied Computer engineering, specialized in Computer Systems and Networks at Kharkiv National University of Radio-electronics (KNURE), Ukraine. He studied software engineering at the University of Tartu (UT), Estonia. Before joining SIT, he was working for Tumaini University, Dar es salaam Institute of Technology (DIT) as instructor and National Institute of Informatics (NII) as a research student. His current research interests include Cyber security, Management Information Systems (MIS), Ubiquitous computing and Brain Computer Interfaces (BCI).

Isao Echizen is a Professor at National Institute of Informatics (NII), Advisor to the Director General (NII). He graduated from the Tokyo Institute of Technology, graduate school of science and engineering. Before joining NII, he worked for Hitachi Ltd as a researcher (Systems Development Laboratory). He is a visiting professor at the University of Freiburg, Halle University, Germany. He is also a Professor at the Graduate University of Advanced Studies (SOKENDAI). His current research interests include media security, media information processing and information Hiding.

♦