Towards Security Risk-oriented Mal Activity Diagram

Mohammad Jabed Morshed Chowdhury
Lecturer, Department of Computer Science and Engineering
Daffodil International University, Dhaka, Bangladesh

ABSTRACTS

Recently security has became one of the major concern in Information System (IS) development. Different security modeling language or security extension is used to model security features of IS. Mal Activity Diagram (MAD) is used at the design stage to represent security aspect. But it cannot model all the security risk management concepts. Without full coverage of concepts, it is not possible to model an IS efficiently and correctly. In this paper, first we propose a meta model for MAD which will help developers or other stakeholders to understand and use MAD correctly. Then we propose syntactic and semantic extensions of MAD to model all the risk management concepts. We have used this meta model and extension in a case study. This study shows that the meta model and extensions help us to correctly identify and model different security components of the system.

KEYWORDS

Requirement engineering, Risk management, Mal activity diagrams, Security magement.

1 INTRODUCTION

Risk management discusses about the process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information system. The main goal of information security is to support the mission of the organization. In actual fact all organizations are exposed to uncertainties, some of which impact the organization in a very negative manner. The need of these organisations is to focus on their most important information assets when making decisions about protecting them to achieve optimal return on security investments (ROSI) [5]. However adopting security controls to protect information assets without proper assessment of risks will either overprotect the assets, making security a hindrance to business operations, or under protect and expose the business-critical asset to threat. Implementation of security risk management solution is costly therefore due to high costs of technological security solutions and limited number of resources, the organizations need assurance that they adopt only solutions that will provide significant Return on Investment (ROI).

There are several security risk management methods [1], [2] and frameworks [6], [7] which can be used to investigate, analyze and risk treatment for security risk management. In this work we focus on Mal-activity diagrams [15] (MAD) to define security risk management. MAD is proposed as an extension of UML activity diagrams [14]. It helps developers to elicit the security features, attack method and their countermeasures of an IS. This allows the inclusion of hostile activities together with legitimate activities in business process models. It captures the dynamic behaviour of both the legitimate and illegitimate actors. MAD was applied for different scenarios [15]; however they still lack structured meta-model and application guidelines. In this paper we develop a meta-model for Mal-activity diagrams and illustrate how they can be used to elicit secure assets, security risks and security requirements.

Different studies (e.g., [4] [16]) have showed that security analysis and secure engineering practices could significantly reduce vulnerabilities if they are applied at the requirements engineering and design stages. Thus, this work is motivated to help requirement engineers and developers to understand how they can consider and model security risks at requirement engineering and system design stage. In [3][17], we have seen MAD cannot model all risk management related concepts. Thus this paper is also proposing necessary extensions to cover those concepts.

The structure of this paper is as follows: Section 2 overviews different security risk related frameworks and methods. Section 3 introduces the mal-activity diagrams. In Section 4 we illustrate how Mal-activity diagrams could be aligned to the security risk management domain [10] and also propose the extensions. Finally, Section 5 concludes this paper.

2 BACKGROUND

2.1 The ISSRM Domain Model

Information System Security Risk Management (ISSRM) [11, 12] is a systematic approach, which addresses the security related issues in an IS domain. The model is defined after a survey of risk management and security related standards, security risk management methods and software engineering frameworks [12]. The domain model (see Fig. 1) supports the alignment of security modelling languages. It improves the IS security and security modelling languages as it conforms to the security risk management of organizations. The model describes three different conceptual categories:

Asset-related concepts describe the organization's assets grouped as business asset and ARE asset. It also defines the security criterion as a constraint of a business asset expressed as integrity, confidentiality and availability.

Risk-related concepts define risk, potential harm to business, it is composed of a threat that contains one or more vulnerabilities, if executed successfully, harms the system assets which has negative consequences on assets defined as an impact. They negate the security criterion imposed by the business asset. An event is an abstraction aggregated as a threat and vulnerability where vulnerability is a weakness in a system that can be exploited by threat agent. A threat is a way to inflict an attack. It harms IS and business asset carried out by a threat agent and an attack method to target IS assets. Threat Agent is an attacker that initiates a threat to harm the IS asset. Attack Method is a mean through which a threat agent executes a threat.

Risk treatment related concepts define a risk treatment decision to avoid, reduce, retain, or transfer the potential risks. It is refined by the security requirement. A control implements the security requirement. The ISSRM process [11,12] is a 6-step process, based on existing risk analysis

methodologies and standards. It starts with context and asset identification of the organization, proceeding to determine the security objectives for identified assets. Next, risk analysis and assessment to examine and estimate potential risks and its impacts. In next step, risk treatment decisions are taken to identify the security requirements. Finally, security control is implemented as security requirement. The process is iterative which may identify new risks and security controls.

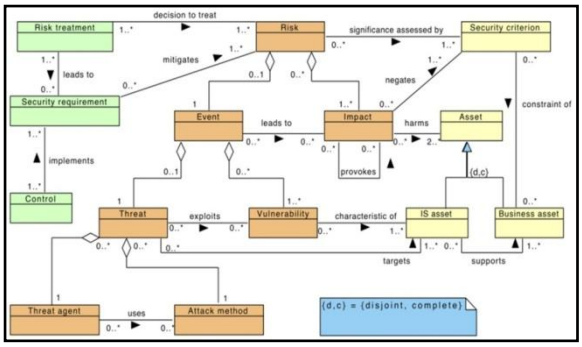

Fig. 1: The ISSRM Domain Model (adapted from [8])

3 MAL-ACTIVITY DIAGRAMS (MAD)

Activity diagrams are part of the UML language [13]. Their major objective is to describe procedural logic, business process, and workflow. They can be used at different stages of the IS development process, including system and software requirement and design. Activity diagrams are often compared to flowcharts, although activity diagrams support the modelling of parallel behaviour.

Mal-activity diagrams [15] extend the concepts of Activity diagrams. They deal with the behavioural aspects of the security problems. Basic way to build a mal-activity diagram is to build a normal process first then add unwanted behaviour to this process. Similarly to the Misuse case [8] diagram, it also allows to add mitigations. It includes some extra concepts such as Mal-Activity, Mal-swimlane and Mal-decision which are opposites of the regular activity diagrams constructs. It also defines MitigationActivity and MitigationLink to show the mitigation process.

In the current literature on Mal activity diagrams we do not find any meta-model for MAD, thus we propose one in Figure 2. MAD start with an InitialState (starting point) and finishes with a FinalState (end point). Next a diagram includes three kinds of activities: Activity, Mal-Activity and MitigationActivity. AnySwimlane holds all the constructs of the mal-activity diagrams. AnySwimlane can be a Swimlane or a Mal-swimlane. Swimlane contains SwimlaneElement, which can be an Activity, a MitigationActivity or a Decision. The Activity is the specification of a parameterised sequence of behaviour. The MitigationActivity shows the improvement of the process to avoid MalciousActivity. The Decision illustrates branching based on order of rejected or order of accepted conditions.

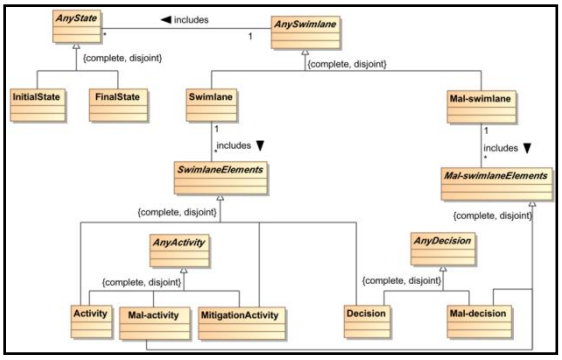

Figure 2: Meta-model of Mal-activity Diagrams

A Mal-swimlane includes Mal-swimlaneElement, which could be a Mal-activity or Mal-decision. Mal-swimlane may also include legitimate activities beside mal-activities. Mal-activity is performed by a malicious actor to harm the normal process. Sometimes Mal-activity can be done by a legitimate user when being fooled by an attacker. Mal-decision is a decision which is made having a malicious purpose.

4. EXTENSION OF MAL-ACTIVITY DIAGRAMS TO ISSRM

We have used the same research method described in [3]. In that paper, we have seen that MAD does not provide full coverage of ISSRM concepts (Table 5.1 in [3]). Here we will propose the syntactic and semantic extensions of MAD using the example but this time from availability perspective. In order to cover the remaining essential ISSRM features (concepts), we have introduced several new constructs, Availability, Security criterion, mitigation link, leads to, Negates, Harms, Constraint of security, decision to treat to cover the missing parts in ISSRM domain model.

4.1 Abstract syntax

Here we will present an extended meta model in Fig. 3. The improved version of meta model uses approximately the same meta model but with complete coverage of ISSRM domain model as shown in the diagram bellow.

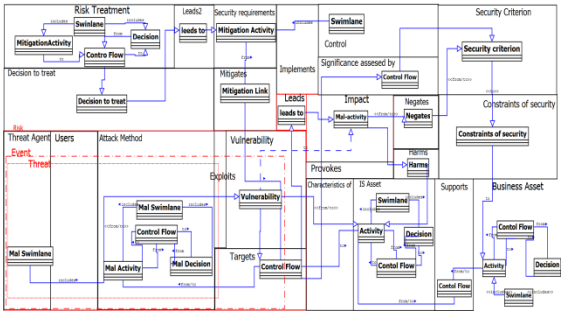

Figure 3: Alignment between improved Mal-Activity diagrams and ISSRM domain model

4.2 Online Marketing Server (Availability)

In this section we are going to illustrate denial-of-service attack (DoS) which negates security objective availability. DoS is a serious networking attack which has led many business organizations into great loss, it is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Networking device (computer/server) is deactivated by flooding it with multiple spoofed requests. Our running example (Online Marketing Server) describes online marketing service (Fig. 4) where customers request new purchase on internet via business firm's website. Hacker is attempting to launch DoS attack (Fig. 6) to make service unavailable to the customers. This attempt directly affects one of the business assets (login- Fig. 5). Hacker is not directly benefited from the attack but he gets paid by other business competitors.

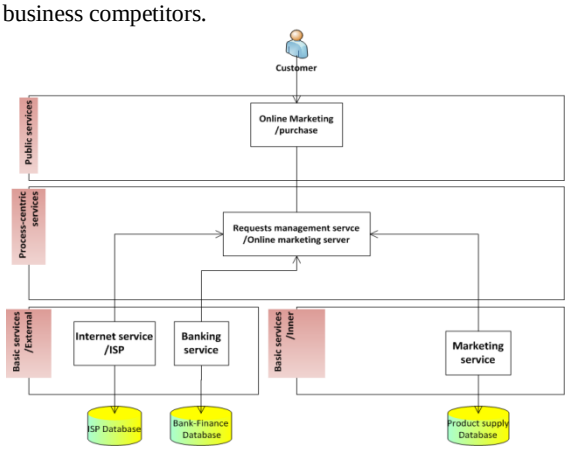

Figure 4: Online Marketing Service Architecture diagram

In Fig. 5, customer initiates the online marketing process with an activity ***request new purchase*** by requesting purchase service via *online marketing server*, server receive request (***Receive request***) and check service availability (***Check service availability***) then processes the request and load the login page (***load login page***) only if the resource is available (***Is service available?***) unless otherwise it sends customer error message (***Send error message***) and process stops upon the delivery of the error message(***Receive 550 Service unavailable***).

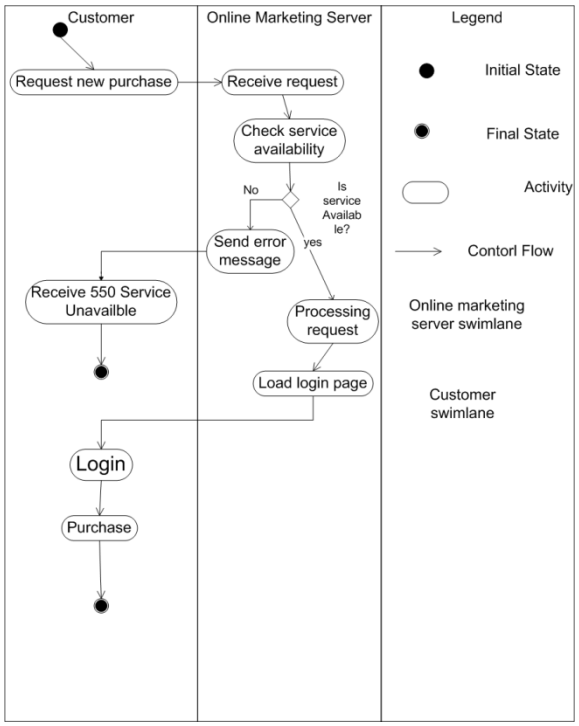

Figure 5: Asset model- Online marketing server

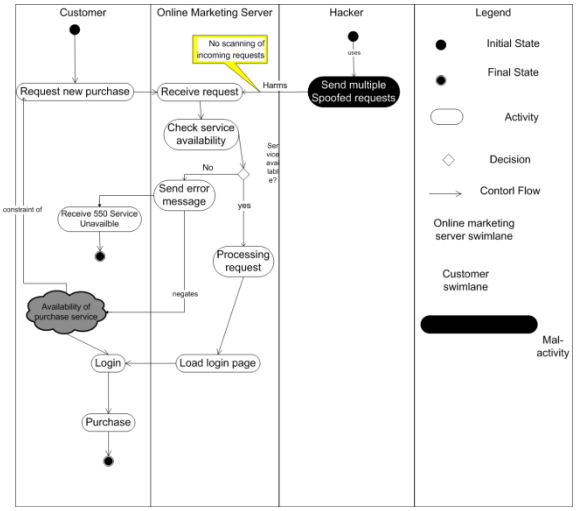

Figure 6: Threat model- Online marketing server

Threat model is presented in (Fig. 6) where a ***hacker*** (Mal-swimlane) launched attack on online marketing server by sending excessive requests (*Mal-activity* ***Send multiple spoofed requests***). As a result unprotected ***Online marketing server*** is deactivated due to its weakness(*vulerability* ***No scanning of incomming requests***) and causes unavailability of a essential *business asset* (***login***).

However DoS attack can be avoided by considering our security model (Fig. 7) where Internet service provider/ISP (Swimlane) uses packet filtering technique (ingress filtering) which can prevent source address spoofing of Internet traffic (Mitigation activity: ***Filter out requests send by Network intruder***). Therefore any malicious request is denied and ends the process.

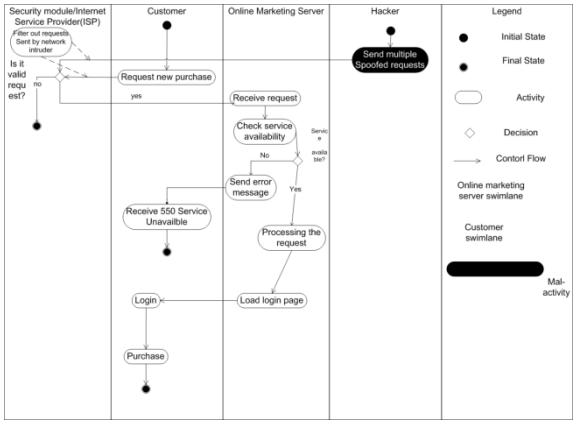

Figure 7: Security model- Online marketing server

4.3 Concrete syntax

Asset related concepts

This example is modelling ISSRM assets using Activity, Decision, Control Flow and swimlane where control flow is representing support which connects others. Security criterion and Constraint of security are modelled by new constructs Security criterion and Constraint of security respectively.

Risk related concepts

ISSRM vulnerability is modelled by new Mal construct vulnerability, ISSRM impact also modelled by Mal-activities. Threat agent is represented by Mal-swimlane; threat agent holds Attack method (Combination of Mal-activity, Mal-decision, Mal-swimlane and Control Flow) using ISSRM relationship uses which is modelled by new mal construct uses. Impact is modelled by Mal-Activity Send multiple spoofed requests. Threat is represented by combination of constructs that compose threat agent and attack method while event is composed by threat and vulnerability. Event and Impact result into risk. Impact negates security criterion (new mal construct security criterion) through ISSRM relationship negates which is represented by new mal construct negates.

Risk treatment concepts

ISSRM Security requirements are represented by Mitigation Activity which mitigates risk through ISSRM relationship mitigates which is also represented by mitigation link. Control is represented by swimlane while Risk treatment is represented by combination of constructs 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.

Table 1: Alignment between Mal-Activity diagrams and ISSRM-Online Marketing server

ISSRM Domain Model		**Mal Activity**	**Example**
Asset Related	**Asset**		
	Business	-Activity,Decision,ContolFlow constructs	Request new purchase,availability of purchase service,login,purchase,is i t valid request?,filter out requests sent by network intruder,Receive 550 service unavailable.
	IS aset	-Activity,decision(connected using Control flow constructs) -Swimlane	Receive request,Check service availability,Processing the request,load login page,Is service available?,send error message, Online marketing server
	Security criterion	-Security criterion	Availability of login operation
Risk Related	**Risk**	-combination of event and impact	Send multiple spoofed requests,hacker,no scanning of incoming requests
	Impact	Activity	Send errow message
	Event	-combination of threat and vulnerability	Send multiple spoofed requests,hacker,no scanning of incoming requests
	Vulnerability	Vulnerability	No scanning of incoming requests
	Threat	-combination of threat agent and Attack method	Send multiple spoofed requests,Hacker
	Threat Agent	Mal-swimlane	Hacker
	Attack Method	-Mal-Activity,Control flow and Mal-swimlane	Send multiple spoofed requests,hacker
Risk Treatment	**Risk Treatment**	- Described by combination of control ,mitigation activity ,decision to treat and security requirements supported by control flowconstructs	-Filter out requests sent by Network intruder.
	Security reqirements	- MitigationActivity	-Filter out requests sent by network intruder
	control	- Swimlane	- Security module

5. CONCLUSION AND FUTURE WORK

Firstly, this paper has shown how the ISSRM domain model could guide application of MAD. But like many other analysis it also has some shortcomings. This analysis has a certain level of subjectivity to interpret the language constructs regarding the ISSRM concepts. To mitigate this threat other examples could be analyzed by other people (e.g., practitioners, if they are willing to use MAD).

Secondly, in our study, we have found that currently MAD lacks a meta model and we have also seen that the exiting constructs of MAD could not model all ISSRM concepts. Thus, the contribution of this paper can be seen as,

1. It first presents a meta model from the exiting MAD literature [15] and then proposes an extended meta model to cover all the ISSRM related concepts.
2. It shows how the new constructs can be used to model security related concepts with the help of an example.

The auto code generation from the exiting model will help to produce more secured code and help the developers with less trouble to fight against known and unknown attacks. Validation of the new extension and auto code generation from the model is remained as the future work.

6. ACKNOWLEDGMENT

I thank God for this achievement. I would also like to acknowledge Dr. Raimundas Matulevicius (Estonia) for his support, guidance and encouragement. I am also grateful to), Guttorm Sindre (Norway), Péter Kárpáti (Norway).

7. REFERENCES:

[1] Asnar Y., Moretti R., Sebastianis M. and Zannone N.: Risk as Dependability Metrics for the Evaluation of Business Solutions: A Model-driven Approach. In: proceedings of the 3rd International Conference on Availability, Reliability and Security, (2008)

[2] Braber F. D., Hogganvik I., Lund M. S., Stølen K. and Vraalsen F.: Model-based security analysis in seven steps—a guided tour to the CORAS method. BT Technology Journal, Volume 25 Issue 1, pages 101–117 (2007)

[3] Chowdhury M. J. M., Modeling Security Risks at the System Design Stage: Alignment of Mal-activity Diagrams and SecureUML to the ISSRM Domain Model, Master These, 2011, http://nordsecmob.tkk.fi/thesis.html

[4] Dubois E., Heymans P., Mayer N. and Matulevičius R.: A Systematic Approach to Define the Domain of Information System Security Risk Management. Springer-Verlag, 2010.

[5] Firesmith D. G.: Engineering Safety and Security Related Requirements for Software Intensive Systems. In: Companion to the proceedings of the 29th International Conference on Software Engineering (COMPANION '07), p.169, IEEE Computer Society, (2007)

[6] Haley C. B., Laney R. C., Moffett J. D. and Nuseibeh B.: Security Requirements Engineering: A Framework for Representation and Analysis. IEEE Transactions on Software Engineering, 34: 133-153, (2008)

[7] Lee S. W., Gandhi R. A., and Wagle S.: Towards a Requirements-driven Workbench for Supporting Software Certification and Accreditation. In: proceeding of the 3rd International Workshop on Software Engineering for Secure Systems, (2007)

[8] Matulevičius R., Mayer N. and Heymans P.: Alignment of Misuse cases with Security Risk Management. In: proceedings of the 3rd International Conference on Availability, Reliability and Security (2008)

[9] Matulevičius R., Mayer N., Mouratidis H., Dubois E., Heymans P. and Genon N.: Adapting Secure Tropos for Security Risk Management in the Early Phases of Information Systems Development. In: Proceeding CAiSE '08 Proceedings of the 20th international conference on Advanced Information Systems Engineering (2008)

[10] 10.Mayer N.: Model Based Management of Information System Security Risk. Doctoral Thesis in Computer Science, University of Namur, Belgium (2009)

[11] 11.Mead N. R., Hough E. D. and Stehney T. R. II.: Security Quality Requirements Engineering (SQUARE) Methodology. Technical Report CMU/SEI-2005-TR-009, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, Pennsylvania (2005)

[12] 12. Mellado D., Blanco C., Sánchez E. L., Eduardo and Medina F.: A systematic review of security requirements engineering. Journal of Computer Standards and Interfaces, 32 (4), 153-165, 2010,

[13] 13. Object Management Group (OMG): Unified Modelling Language: Superstructure. Technical report, version 2.0 (2004)

[14] 14. Rodríguez A., Medina E. F., Trujillo J. and Piattini M.: Secure business process model specification through a UML 2.0 activity diagram profile. UML'01, Springer Verlag, 76-90, 2001

[15] 15. Sindre G.: Mal-Activity Diagrams for Capturing Attacks on Business Processes. In: proceedings of the Working Conference on Requirements Engineering: Foundation for Software Quality (2007)

[16] 16. Viega J. and McGraw G.: Building Secure Software: How to Avoid Security Problems in the Right Way. Addison Wesley, 2002

[17] 17. Chowdhury M. J. M., Matulevicius R., Sindre G., Kárpáti P.: Aligning Mal-activity Diagrams and Security Risk Management for Security Requirements Definitions. REFSQ 2012: 132-139