Enhancement of a Business Model with a Business Contextual Risk Model

Zakariya Kamagaté, Jacques Simonin, Yvon Kermarrec

Enhancement of a business model with a Business Contextual Risk Model

Zakariya Kamagaté[1], Jacques Simonin[2], and Yvon Kermarrec[2]

[1] IMT Atlantique – Lab-STICC UMR CNRS 6285, Technopôle Brest Iroise F-29238 Brest cedex, LASTIC-DRIT, ESATIC 18 BP 1501 Abidjan 18, Côte d'Ivoire
zakariya.kamagate@imt-atlantique.fr
[2] IMT Atlantique – Lab-STICC UMR CNRS 6285, Technopôle Brest Iroise F-29238 Brest cedex,
{jacques.simonin , yvon.kermarrec}@imt-atlantique.fr

Abstract. In this paper, we propose an approach of security risk-driven contextual model for software systems development. The approach is model-driven using enterprise business architecture as the basis for the contextual models definition, associating security risk concerns. Enterprise Architecture (EA) enables the description of an organisation's structure, its business and its underlying Information System. By using a Model-Driven Engineering (MDE) approach such as Model-Driven Architecture (MDA), we define an architecture for models, and we provide a set of guidelines for structuring specifications expressed as (EA) contextual models. Then these models are enhanced to integrate security aspects in the overall development process. The proposal aims to analyse enterprise security from a business-oriented view and define security requirements inherited by the lower architectures, particularly IS architecture. The approach provides a meta-model of business contextual risk with a security management process, consisting on a systematic method, guiding to risk modelling and risk treatment strategies.

Keywords: Risk · models · business scenario · security · threats · software engineering · Enterprise Architecture · Model-Driven Engineering · Model-Driven Architecture.

1 Introduction

Model-Driven Security (MDS) has emerged as a specialized Model-Driven Engineering (MDE) [1] approach for supporting the development of security-critical systems. MDE consists of using models and their transformations as primary artefacts for each stage of system development process. Model-Driven Architecture (MDA) [6], an MDE approach, that uses models, promotes a vertical separation of concerns at a high level of abstraction, without any considerations about the target platform. These specificity can be integrated (semi) automatically to produce code compliant with each platform. Throughout its process, MDE gives the possibility to define contextual models as constraints definition [3]. This is a prevailing solution to define system architecture applying gradual constraints by

refining the initial system specification [2]. This methodology directly inspired several MDS proposals [14] that applied this paradigm to information security engineering, bringing several benefits to the domain. Nevertheless, many attacks toward organisations have success because of issues associated with how systems within organizations are structured. In this context, it is necessary to examine security by taking into account all components that influence the organization's systems, including business, application and technologies. Enterprise Architecture (EA) fulfils this need. EA can be defined as an approach that clearly shows how the enterprise's structures (business processes, Information Systems, applications, technologies. . .) are integrated. Also, it reduces organization's complexity by providing specific viewpoints on an integrated entire model [4]. However, "true integration of security in Enterprise architecture requires a system engineering approach. Then security and risk are considered as soon as possible in the system engineering development lifecycle" [5]. In this context, MDA instances are ideal solutions for EA security integration by defining an architecture for models, providing a set of guidelines for structuring specifications expressed as models. The goal of this paper is to present a security risk-driven contextual approach, based on the concepts of well established EA frameworks such as TOGAF [10] and its compositional layers (e.g., business and IS) by leveraging the related-context concept of MDE. As main contribution, we defined contextual models related to TOGAF (business, Information system) architectures with security risk concerns. Then, these models integrate the model-driven Architecture (MDA) process at the CIM stage with a transformation chaining to the Platform Independent Model (PIM) stage. The result is a PIM instance of risk-driven logical architecture of business tasks. The paper is organised as follows. Section 2 is the Background, and next, the related works regarding MDS is describing in Section 3 .The proposed approach of business contextual risk-driven modelling is defined in Section 4, with subsections describing the meta-model and the security management process. We present the Model-driven integration with enhancement of a business contextual risk model into MDA approach in Section 5, and finally we end with conclusion and future work in section 6.

2 Background

Model-driven Architecture (MDA) deals with models and uses different levels of abstraction to address the problem and the solution domain. It defines methodologies to lower the level of abstraction by defining relationships between the participating models. The goal of MDA is to create an Enterprise Architecture(EA) modeling capability helping analysts and developers to describe a company's business and software assets[20]. Model-driven Security (MDS) takes advantage of the (MDA) techniques by providing guidelines to support the construction of systems with security mechanisms integration. [17] defines (EA) as "a coherent whole of principles, methods and models that are used in the design and realization of the enterprise's organizational structure, business processes, information systems, and infrastructure". A large number of frameworks for enterprise archi-

tectures have been proposed. Among the most, important ones are the Zachman Framework [8], the Department of Defense Architecture Framework [9] and the Open Group Architectural Framework (TOGAF) [10]. TOGAF is considered as one of the best frameworks concerning business and technical layers, as it provides many structures and details for these. At the core of TOGAF is the Architecture Development Method (ADM), eight phases that provide an iterative process of continuous architecture development. In this paper we combine TOGAF and MDA for enterprise architecture development, with security concern. The approach is a Model-Driven security oriented Enterprise Architecture.

3 Related works

in a white paper published in 2016 [5], The Open Group analyses different approaches to integrate risk and Security within a TOGAF Enterprise Architecture. It examines a selection of risk and security modelling paradigms and extracts a set of core concepts for them. Then it maps most of the concepts to ArchiMate language elements. Contrary to this white paper, our approach uses UML for graphical representation of security concerns as contextual models. We create an enterprise architecture modeling capability based on MDA approach. Then we generate specific applications to implement the architecture.. In [11], the authors proposed an integration of security risk management and enterprise architecture management. The integration is in the form of concepts mapping between Information System Security Risk Management (ISSRM) and the Enterprise Architecture Management (EAM) metamodels. The approach leverages enterprise architecture modelling to support the identification of business and IS assets. It also proposes to model the treatment of the risk, especially in relation with the value of the risk. However, contrary to our, this approach does not give real support in the identification of the threats and risk associated with the elements of the architecture. In our proposal, threats and risk are analysed with the STRIDE [18] method, as a basis for security requirements from business point of view. The model-driven security provides supports for modelling security requirements as a concern from the requirements stage. Here, security relevant information are provided at the right level of abstraction as contextual models. Then, model transformation mechanisms are useful to integrate these models into the overall system architecture. The following section describes the risk-driven business contextual model proposed within our approach.

4 Risk-driven business contextual model

This section is dedicated to the introduction of the business contextual risk model supported by a security management process. Our main contribution of risk-driven business model is based on the Open Group guide that describes how the TOGAF architecture development can be used to create security risk-driven system's architecture [5]. We use UML as a modelling language to describe the architecture artifacts in the meta-modelling. Our approach is a Transformation

Contextual Model (TCM) defined by a risk expert to influence the development process from the early stage (Computation Independent Model) of the development life cycle. Next, the description of the business contextual risk meta-model.

4.1 Business contextual risk metamodel

The TCM-BR (TCM - Business Risk) model (see Fig.1) corresponds to the business risk model in the TOGAF Enterprise Architecture related to Risk and Security integration. Business Risk model is the result of threat/risk analysis from the business scenario model. **Threat** is based on threats identification, risk like-

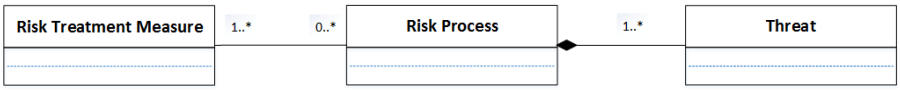

Fig. 1. Business Contextual Risk meta-model .

lihood of materializing, and impact of an incident on business assets (business tasks). NIST defines threat as "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service". [15] A threat is always related with a specific business task (sequence) and is evaluated measuring its probability and potential impact resulting in a measurement of its risk. **Risk process** is risk identified from threat analysis in the organisation's business in the context of business scenarios. Risk is the combination of a threat with one or more vulnerabilities leading to a negative impact harming one or more of the assets. **Risk Treatment measure** is an action, device, procedure, or technique that reduces a threat, vulnerability, or an attack. It comprises two steps: -Risk Treatment decision: consisting on action against risk (i.e.: risk mitigation, risk elimination, risk transfer or risk acceptation); and -security requirements: defines security objectives (in term of CIA, authentication, authorisation. . .) considered to select corresponding security strategies (services) and appropriate control measures to implement. The following paragraph presents the process guiding to security management.

4.2 security management process for Business contextual risk model

The security risk management process proposed below is compliant with ISO 27005 [13] and ISO 31000 risk management standards, defined by ISO. The method comprises the classical steps of risk management: Context Establishment, risk assessment and risk treatment. Our approach presents the particularity to execute the actions of the process with the basis of contextual enterprise

architecture models supported by the model-driven architecture (i.e.: CIM level). The process described below (see fig. 2) puts the focus on how the enterprise architecture can support each action of the process from the enterprise business scenario and the IS supporting the business. Here the description of each action:

Fig. 2. Security management process.

- **Context and assets identification** : consists in knowing the field of the organization, its environment, determining precisely its limits and identifying its resources, assets and services. An Asset (business assets and IS assets) is considered as anything that has value to the organisation and contributes for achieving its goals [11].
- **Security goals**: Security goals also known as security properties are criteria that act as indicators to assess the significance of a risk [12]. It is generally defined in term of confidentiality; integrity; availability, non-repudiation, accountability.
- **Threat and Risk analysis**: In our approach, we use STRIDE [19] threat modeling method to support threat and risk analysis by providing a checklist of threat models with the corresponding security property violated. In this way, security objectives are defined based on the need to guarantee these security properties. To each security property, correspond a security strategy (service) proposed to mitigate risk as security requirement. In addition, for each mitigation strategy, a list of controls or mitigation techniques are proposed for the implementation. STRIDE [19] method is a mnemonic for things that go wrong in security. It stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (see definition in table 1).
  Assumed, the following threats/attacks in the context of an online shopping that can lead to loss of money (business financial loss). We defined a list of risks as (R1 to R6) to characterise each threat:
  - R1 (Risk 1): Credentials spoofing; R2 (Risk 2): Phishing; R3 (Risk 3): Sniffing; R4 (Risk 4): Session hijacking; R5 (Risk 5): Buffer Overflow; R6 (Risk 6): Unauthorized.

  The mitigation methods listed in the table (see Tab.1) are intended to serve as examples to illustrate ways to address threats for threat analysis, risk process, and Risk Treatment in the online shopping context: As shown in the table 1, the column (1) describes STRIDE threat model, which corresponds to threat element in TCM-BR.Column (2) is the definition of each element. Each threat model corresponds in column (3) to a security property

(goals/drivers). The column (4) is the security services proposed as threat mitigation strategy. Threat mitigation strategy corresponds to threat treatment measure (decision) taken to how to treat threat. From this decision, a security requirement is defined based on violated security properties that determine security objectives in term of CIA, authentication, authorization... and the corresponding strategy controls as security services. The column (5) proposes some technical means that can be applied to tackle threats. The corresponding elements of STRIDE helps identify risks related to a specific domain (e.g.: risks to online shopping) and propose a treatment measure. A threat is always related with a specific business task (or sequence of tasks) and the underlining IS components (applications and operations). A threat is evaluated, measuring its probability and potential impact resulting in a measurement of its risk.

Table 1. STRIDE threat models and mitigation measures (adapted from [19]f .

Threat model	**Definition**	**Security property**	**strategy (Security service)**	**Mitigation techniques**	**Example : Risks of online shopping**
Spoofing	Impersonating something or someone else.	Authentication	Authentication	Passords, Tokens, Biometrics, HTTPS, Ipsec, Crypto tunnels, Digital signatures or authenticators	R1, R4, R6
Tampering	Modifying data or code	Integrity	Integrity, permissions	Digital Signatures, Keyed MAC, IPSEC, HTTPS, ACLs/permissions , Crypto tunnels	R6
Repudiation	Claiming to have not performed an action.	Non repudiation	Fraud prevention, logging, signatures	Digital signatures, Logging	R2, R3, R6
Information Disclosure	Exposing information to someone not authorized to see it	Confidentiality	Permissions, encryption	SSL : IPSEC, HTTPS, Permissions, File encryption , Disk encryption (FileVault, itLocker)	
Denial of Service	Deny or degrade service to users	Availability	Availability	Fail over, Load balancing, Elastic cloud, design more capacity	
Elevation of privilege	Gain capabilities without proper authorizaLon	Authorization	Authorization, isolation	Roles, privileges, Input validation (fuzzing*), Sandboxes, firewalls	R1, R4, R6

- **Security requirements**: Security requirements are the security needs to treat identified risks. It is defined by the decision of how to treat risk designed as risk treatment decision. There are four types of measures (related decisions) to treat risk: risk mitigation or reduction (decision), risk avoidance (decision), risk transfer (decision) and risk acceptance (decision). Risk mitigation (reduction) decisions lead to security requirements.
- **Security control engineering**: Control (also called countermeasure or safeguard) is a designed means to improve security, specified by a security requirement, and implemented to comply with it. The column (5) of table 1 corresponds to control techniques for threats mitigation.

A model of logical components, composed by logical operations, which supports the core business of the company, represents a view of the logical architecture. This consists in a static view made up of logical application components and logical risk management components, which supports the business model described in CIM and the contextual business model described just before in (TCM-BR). The following section describes the logical architecture and presents the overall model-driven integration architecture of our approach.

5 Business contextual risk model integration into MDA approach

This section presents our approach of integrating a contextual risk model into a Model-Driven Engineering process with business architecture of the Enterprise Architecture. The proposal aims to extend the CIM model, representing business context models of EA with an enhancement transformation using the MDA approach mechanisms. Model-driven architecture (MDA), comprises three levels of abstraction: computation independent model (CIM) or (requirements), platform independent model (PIM) or (design and architecture) and platform specific model (PSM) or (implementation). A CIM presents what the system is expected to do, a PIM represents how the system reaches its requirements out specific platform details and a PSM combines the specification in PIMs with details required to describe the system implementation on a particular type of platform. A series of transformations are performed to build a software system: transformation from CIM to PIM, transformation from PIM to PSM, and transformation from PSM to code. Our approach concerns a CIM enhancement with a transformation of CIM to PIM. The overall development process integrates the different models involved (including the business contextual risk model described previously) in the architecture, by a model transformation chaining in a MDA compliant development process. A contextual transformation for enhancement (CTe) and enhancement transformation (ET) are useful for this purpose. At each stage of the transformation chaining, a new contextual model is created by a TCM integration during the enhancement process, taking into account the previous model. These models are used to build a PIM model that is a risk-driven logical architecture of business tasks. The models description instances

are illustrated with a scenario of two tasks of an online shopping performed by a customer:

1. Read customer login and password
2. Open a customer session

As follow the description of the overall architecture and the composing model

The CIM is a model of a business scenario. The CIM concepts target the description of business task(s) composing a business scenario:

- **"Business Scenario"** (close to the Business Service concept defined in the TOGAF meta-model) describes a business scenario (*BSCustomerAuthentification*).
- **"Business Task"** specifies the name of a task composing a business scenario (Read customer login and password and Open a customer session business tasks of the *BSCustomerAuthentification* business scenario).
- **"Business Task Sequence"** represents a temporal sequence of two tasks (Read customer login and password before Open a customer session).

The CICM-R (CICM – Risk) meta-model shows a mapping relationship between a task of a business scenario and business risks. This mapping is achieved by a business expert and a security risk expert with the instantiating of the "Contextualized Business Task with Business Risk" concept that links (represented below by the "→" symbol) a "Business Task" instance and a "Business Risk" instance *(Read customer login and password → R1 and R6)*.

TCM-LIS (TCM – Logical Information System) is the contextual model in relation to integration with enhancement. This enhancement by a logical architecture model of the IS (which is designed by Enterprise Architects) needs the following concepts:

- "Logical Application Component" defined in the TOGAF meta-model (*LACUserManagement and LACSessionManagement*).
- "Logical Application Component Dependency" (*LACSessionManagement depends on LACUserManagement*).
- "Logical Application Operation", which composes a logical application component (*LAOReadCredentials* in *LACUserManagement*, *LAOCreateSession* in *LACSessionManagement*).

A Logical Application Component (*LAC*) is dedicated to risk management. This component designed as *LACRiskManagement* encapsulates operations that treat each risk: *LAOProcessR1* and *LAOProcessR6* in our illustration.

The CICM-L (CICM – Logical) meta-model is a mapping relationship ("Contextualized Business Task with Logical Application Operation" concept) between a business task and IS logical application operations packaged into logical application components ("Logical Application Operation" concept) designed by the Enterprise Architects (*Read customer login and password→ LAOReadCredentials and Open a customer session→ LAOCreateSession*). A sequence of business tasks involves a possible mapping with a logical application component

dependency between components owning the operations mapped with the business tasks (*Read customer login and password* before *Open a customer session*) → *LACSessionManagement* on *LACUserManagement*)
LACRiskManagement depends on A business scenario is generally a sequence of tasks consisting in "request" and "access" operations of resources (e.g: data). Thus, in one hand, a Logical Application Component depends on a Risk Logical Application Component when the "request" operation is identify as critical (risky) and requires a treatment before its execution. In addition, in the other hand, a Risk Logical Application Component depends on a Logical Application Component when the "access" operation is identify as critical (risky) and requires a treatment after its execution. Hence, a representation of logical data provided by logical operation can give details of business operations and help to identify precisely the resources concerned by the related risks. In this case, risk process can be highlight dynamically by an UML sequence diagram to perform a better analysis and management of risk.

6 Conclusion and future Works

In this paper, we proposed a business contextual risk-driven model integration into the MDA approach based on TOGAF Enterprise Architecture. A contextual enhancement transformation was useful to achieve the contextual models integration within the CIM to PIM model. Then we leveraged the concepts of model-driven security paradigm by analyzing information security risk from a business (scenario) point of view. The integration results into a PIM instance of risk-driven logical architecture of business tasks. The PIM describes a static architecture of the model that illustrates the logical application components and the logical risk management component. We are currently working on the dynamic logical contextual risk model that defines rules for the dynamic management of logical application components, composed by logical operation risks.

References

1. SELIC, Bran. MDA manifestations. The European Journal for the Informatics Professional, IX (2), 2008, p. 12-16. [2] A. Kleppe, J. Warmer, W. Bast: MDA explainedthe model-driven architecture: practice and promise. Addison-Wesley, Boston, 2003.
2. DAVIES, Jim, GIBBONS, Jeremy, MILWARD, David, et al. Compositionality and refinement in model-driven engineering. In : Brazilian Symposium on Formal Methods. Springer, Berlin, Heidelberg, 2012. p. 99-114.
3. SIMONIN, Jacques et PUENTES, John. Automatized integration of a contextual model into a process with data variability. Computer Languages, Systems Structures, 2018, vol. 54, p. 156-182.
4. INNERHOFER-OBERPERFLER, Frank et BREU, Ruth. Using an Enterprise Architecture for IT Risk Management. In : ISSA. 2006. p. 1-12.
5. Open Group Guide. Integrating Risk and Security within a TOGAF® Enterprise Architecture ISBN: 1-937218-66-9 Document Number: G152 Published by The Open Group, January 2016.

6. KLEPPE, Anneke G., WARMER, Jos, WARMER, Jos B., et al. MDA explained: the modeldriven architecture: practice and promise. AddisonWesley Professional, 2003.
7. ASNAR, Yudistira, GIORGINI, Paolo, MASSACCI, Fabio, et al. From trust to dependability through risk analysis. In : The Second International Conference on Availability, Reliability and Security (ARES'07). IEEE, 2007. p. 19-26.
8. John A. Zachman. A Framework for Information Systems Architecture. IBM Systems Journal, 38(2/3):454–470, 1999.
9. Department of Defense Architecture Framework Working Group: DoD Architecture Framework, version 1.5. Department of Defense, USA (2007)
10. The Open Group: TOGAF 2007 edition, Van Haren Publishing, Zaltbommel, Netherlands (2008)]
11. GRANDRY, Eric, FELTUS, Christophe, et DUBOIS, Eric. Conceptual integration of enterprise architecture management and security risk management. In : 2013 17th IEEE International Enterprise Distributed Object Computing Conference Workshops. IEEE, 2013. p. 114-123.
12. DUBOIS, Éric, HEYMANS, Patrick, MAYER, Nicolas, et al. A systematic approach to define the domain of information system security risk management. In : Intentional Perspectives on Information Systems Engineering. Springer, Berlin, Heidelberg, 2010. p. 289-306.
13. Hervé Schauer Consultants. ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management, 2010
14. LUCIO, Levi, ZHANG, Qin, NGUYEN, Phu H., et al. Advances in model-driven security. In : Advances in Computers. Elsevier, 2014. p. 103-152.
15. threat - Glossary — CSRC , https://csrc.nist.gov/glossary/term/threat, Arpil 2020
16. CHOWDHURY, Mohammad Jabed Morshed. Security risk modelling using SecureUML. In : 16th Int'l Conf. Computer and Information Technology. IEEE, 2014. p. 420 -425.
17. JONKERS, Henk, LANKHORST, Marc M., TER DOEST, Hugo WL, et al. Enterprise architecture: Management tool and blueprint for the organisation. Information systems frontiers, 2006, vol. 8, no 2, p.63-66.
18. MYAGMAR, Suvda, LEE, Adam J., et YURCIK, William. Threat modeling as a basis for security requirements. In : Symposium on requirements engineering for information security (SREIS). 2005. p. 1-8.
19. SHOSTACK, Adam. Threat modeling: Designing for security. John Wiley Sons, 2014.
20. https://www.omg.org/mda/mda$_files$/09−03−$WP_Mapping_MDA_toZachman_Framework1.pdf$