Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

A Software Modeling Method for Integrating Functional and Security Design

Chee-Yang Song[*1], **Yoohwan-Kim**[2]

[1]*Department of Software, Kyungpook National University, Korea*
[2]*Department of Computer Science, University of Nevada Las Vegas (UNLV), U.S.A*

ABSTRACT

Security has become an essential part of the software development process. However, previous researches have not adequately integrated the security properties and policies into the development process systematically covering entirely from an early business model to a software model. This, in turn, makes it difficult to create the application models that combine the functional models and the security models. To support the development of the applications that reflects the security properties and policies, this study proposes a hierarchical modeling approach that integrates the metamodel, the framework, and the process based on the degree of abstraction of the development so as to meet the functional (business) and security requirements of the systems. This study aims to establish a framework and process for integrated modeling of the functional and security (non-functional) design aspects necessary to develop applications. The process of integrated modeling ranging from the business modeling to the software modeling is described following the development phases. With the proposed method, reliable systems can be developed by modeling the application systems more clearly based on the integrated method to meet the functional and security requirements.

KEYWORDS: Function-security integration framework, Security modeling process, Layered modeling, Security metamodel, BPMN, UML

ARTICLE INFO: Received 18 January 2017, Revised 8 February 2017, Accepted 10 February 2017.

[*]Corresponding author is with the Department of Software, Kyungpook National University, 2559, Kyeongsang Dae-ro, Sangju-Si, Gyeongsang Buk-Do, 37224, KOREA. *E-mail address*: cysong@knu.ac.kr

1. Introduction

As the development of the information and communication networks continues, the

convergence between the industries and services has been accelerated, which raises the importance of developing more secure applications. However, the current research has not progressed enough to see a entire and hierarchical development process integrating the security properties which covers the entire development process from an early business service modeling to an execution component modeling. In other words, while the security solutions for network infrastructure and the server platforms have been actively researched and commercialized, the process and guidelines to design those applications providing practical services under this infrastructure, with the functional modeling and the security modeling integrated into the existing development methods, have not been clearly defined yet.[1-16](refer section 2) This makes it hard to apply them in practice. For instance, under the existing development methodologies, security was recognized as a non-functional requirement in the analysis phase and reflected in the architecture in the later design phase. This shows that processes and methods for an integrated and hierarchical modeling for function and security design have not been systematized, and have limitations in developing reliable software that meets security requirements. Hence, it is necessary to develop well-defined modeling framework and process so as to reflect the security properties in functional models.

<Table 1> shows the existing development methods for expressing security requirements along with functional models to meet the functional and non-functional requirements according to development phases. (refer Section 2.3 and 2.4) In <Table 1>, for functional requirements, Business Process Modeling Notation (BPMN) and Event-driven Process Chain (EPC) are used in business modeling, and Unified Modeling Language (UML) is used to visualize the functional models. For instance, under the BPMN model, security requirements are written as text annotations.

표 1. 기능 모델에 보안을 표현위한 기존 모델링 방법

Table 1. The existing modeling methods for representing security to function model

Modeling phase		**Modeling method**	
		Function Requirements (section 2.3)	**Security Requirements (section 2.4)**
Business development methodology	**Business Definition phase**	*BPMN/EPC model* Specifying business function with activities	*SecureBPMN model* Specifying of Icon (graphic, or Annotation (text), Stereotype) related to activity being required security
Software development methodology	**Requirement definition phase**	*Use case model* Specifying function with use case	*Secure use case model* Specifying security with Security use case, Misuse case,Security use case specification
	System analysis Phase	Specifying function with *UML*of class model, sequence model, component model, deployment model, and etc	*UMLsec*, *SecureUML* *MDS (Model-Driven Security)* Specifying security adding Stereotype's notation to modeling element of UMLmodel
	System design phase	Same as above but more detailed design with analysis model of function	Same as above but more detailed design with analysis model of security

However, previously-used modeling languages and development methodologies for function and security modeling have various issues. First, currently used development methods lack a systematic development process covering from early service modeling to software modeling that sufficiently reflects security properties and policies, and that harmonize functions and security. Second, in terms of software development methodologies, it is difficult to create application models that can mutually integrate function modeling and security modeling due to a separation of such modeling process. Third, in terms of software modeling languages, research has been conducted toward expanding the existing modeling elements to reflect the non-functional security requirements into the functional models such as BPMN, use case model, activity model, and class model, etc. Individual models can now provide expressions for functional and security modeling, but modeling methods for integrating functions and security between models are not concrete enough.

This study aims to suggest a functional and security integrated modeling framework and process that can reflect security properties and policies. To this end, first, this study defines integrated modeling framework and process for establishing functional and security (non-functional) models of applications based on security properties. Second, this study also establishes function-security modeling methods that can integrate and interconnect the Domain Specific Language (DSL, *e.g.*,BPMN) based business modeling method and the General Purpose Modeling Language (GPML, *e.g.,* UML) based software modeling method.This is expected to contribute to developing reliable systems that can meet both functional and non-functional requirements.

The rest of this paper is organized as follows: Section 2 analyzes the existing integrated modeling studies for function and security; section 3 defines the layered metamodel and modeling process for integrating functional and security; section 4 applies the proposed modeling process to the Online Shopping Mall System (OSMS) system; and finally, section 5 presents the comparison with the existing methods.

2. Related Studies

2.1 Security Properties

Security is to provide integrity, confidentiality and availability to software systems by shielding them from unapproved access, use, disclosure, modification, destruction, etc. Security properties should be reflected in designing models of an application system in order to meet the goals of security. Security properties are classified into security service, implementation technology and security attribute. A security attribute is a piece of information which is associated with an entity or user controlled for the purpose of the implementation of security policy. The security Services (goals or Objectives) [16] are consisted of confidentiality, authentication, integrity, access control, non-repudiation and availability. The security mechanisms mean the modeling elements

which are security policy, Security mechanisms (solutions), Informational attributes, Access control Attributes, Nondisclosure attributes and Integrity attributes.

2.2 Security Development Methodology

Security development methodologies used previously to model security requirements are as follows: Security architecture that considers three security properties — self-protection, non-bypassability, and domain isolation — were analyzed in [1], and this was mapped in the software architecture. In order to design an architecture customized for the three security properties, 5-phase modeling process was proposed. They, however, handle architectures limited to the three properties only. In addition, software development methodologies that strengthened security were analyzed in [2]. The Comprehensive Lightweight Application Security Process (CLASP) of Secure Software was designed to accumulate security-related activities in application development process used previously.

2.3 Business Model Based Security Modeling Method

BPMN models[3-6] and UML activity models[7] are extended to add security requirements to business models that can express functional practices in the highest level.

In [3], metamodel was defined by extending modeling elements of security requirements in BPMN metamodel so as to express security requirements in high-level BPMN models. To do so, extended security elements were defined as security specifications. In [4], security policy models and security mechanism models were defined, and constraint models were also defined by six security goals (authentification, etc.). These defined security elements were expressed in BPMN models in the forms of stereotype or icon. In [5], expanded methods to model non-functions (security requirements) in BPMN business models in service-oriented ways were suggested. Seven security elements (confidentiality, etc.) were defined using security profile and metamodel. In addition, SecureBPMN models were suggested to express security in ontology-based BPMN models in [6]. With this model, secure business process models are created.

Meanwhile, there are studies on expressing security in business models using an UML Activity Model based on a Service-Oriented Architecture (SOA). [7] shows methods of expressing security in business models by using UML-SOA-Sec.

2.4 UML Based Security Modeling Method

In order to develop an application system, business modeling with security expressed in it is conducted. Then, software modeling is conducted, and at this time security is added to UML with stereotypes or extended elements through specifying practices. In [8], trends, directions and future challenges of studies on integrating security

engineering and software engineering were discussed. To integrate security engineering (social level) and software engineering (technical level), security was integrated through requirements-driven software engineering process by using a social ontology. In [9], a method of expressing security in a use case model was presented. This is to express security in extended use case models by adding "security use case" and "misuse case" modeling elements to existing use cases.

In particular, there are model-based methods (based on UML) [11-12] for secure systems development which do have integrated function and security modeling methods in modeling phases. In [11], it addresses Model Driven Security (MDS) approaches that security model were integrated with UML process models. In [12], it shows a full Systematic Literature Review (SLR) on MDS studies (108 papers) including Model-to-text transformations (MTTs).

Meanwhile, there are extended UML security modeling languages for the RBAC such as UMLsec[13] and SecureUML[14]. The languages are to express access control policies of applications, and they were extended from the UML in order to express security in a class model, activity model and deployment model of UML. In [15], methods of modeling function and security from the requirement definition phase and to the implementation phase were presented.

3. Layered-integrated Metamodel and Process of Function-security Modeling

This study aims to establish metamodel, framework and process for hierarchical modeling by integrating business (functional) and security requirements based on the abstraction levels of development so as to develop secure applications with security properties and policies added to them. By doing so, reliable systems can be developed, satisfying both functional and non-functional requirements. The study is to add the functional modeling method in [17] (written by author) to the security modeling method.

In terms of business modeling and software modeling, the scope of this study is to hierarchize constructs of BPMN and UML models; define metamodels and framework; and establish hierarchical and integrated business and security modeling process based on these metamodels. Approach models of this study are shown in <Figure 1> in detail. Items in the lower part of the left side include development methodologies and application systems which these methods are applied to. Items in the upper part of the right side are function (business) and security requirements of application systems.

Function/DB/GUI models are created as function models based on functional requirements of systems through the modeling process of business and software methodologies. On the other hand, a security model is designed as non-functional model based on non-functional requirements through security methodologies. Methodologies and functional and non-functional (security) requirements developed herein are shown in the gray boxes (No. 1, 2, 3). In addition, [17] is the proposed integrated modeling

between business modeling and software modeling for function modeling. This study discusses modeling processes that extend the integrated modeling shown in [17] and add security modeling.

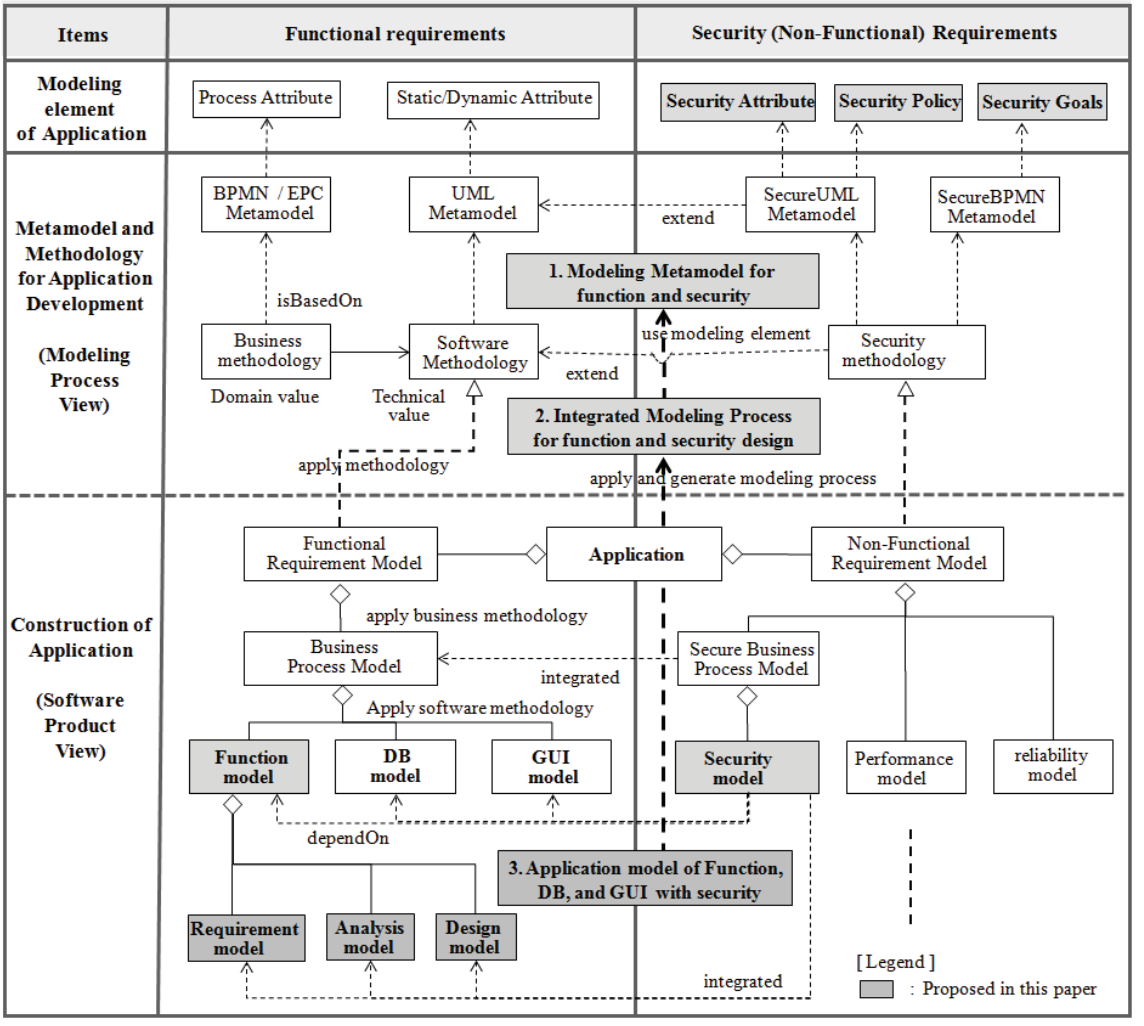

그림 1. 기능과 보안 통합위한 접근 모델

Figure 1. The approach model for integrating function and security

3.1 Integrated Metamodel for Function and Security Design

3.1.1 Integrated Architecture of Function and Security Modeling

Business modeling using the BPMN and software modeling using the UML should be provided to ensure models are designed based on the functional and security requirements of application systems. The Function and Security integrated Modeling Architecture (FSMA) for individual and integrated metamodel, framework and modeling process is required to do so. This architecture, by extending the model in [17], is composed of FSMA-MM (MetaModel) for the integrated modeling of function and security; FSMA-MPF (Modeling Process Framework) based on the construct and elements of the defined metamodels; and FSMA-FSIMP (Function Security Integrated Modeling Process) created as instances by this framework as shown in <Figure 2>.

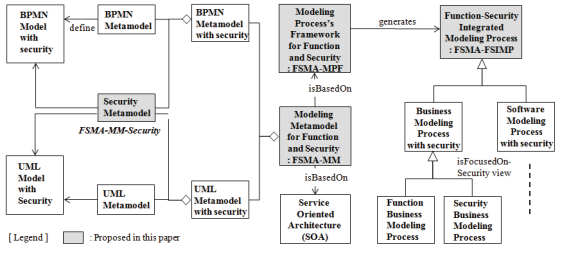

그림 2. 기능과 보안의 통합 아키텍처: FSMA

Figure 2. An integrated architecture of function and security modeling: FSMA

FSMA-MM is herein composed of function metamodels of BPMN and UML, and security metamodel. The integrated modeling process includes processes of business modeling and software modeling, and each of them has their own functional and security modeling process. The gray box in <Figure 2> is the proposal of this study.

3.1.2 Integrated Metamodel with Hierarchy of Function and Security Modeling

Among the components of the FSMA architecture (<Figure 2>), the FSMA- MM (<Figure 3>) is composed of metamodels of models related to the analysis and design of business services, and the implementation of software components according to system development procedures. Integrated metamodel is defined by adding elements of security modeling to the service-oriented function modeling in [17]. In other words, security modeling elements are added to individual metamodels and security metamodel and function-security integrated metamodel are added newly. For function and security modeling, the FSMA-MM presents integrated metamodels for mapping between BPMN and UML (use case, class, component, deployment) from business modeling to software modeling.

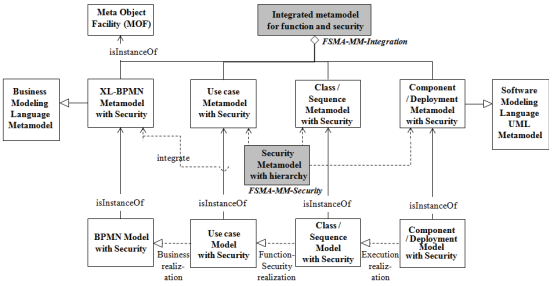

그림 3. 기능과 보안 모델링의 개략 통합 메타모델: FSMA-MM

Figure 3. The overview integrated metamodel of function and security modeling: FSMA-MM (overview)

In order to provide hierarchical modeling according to development abstraction levels, layered security metamodel is defined as follows: These layered security metamodel can be defined

as instances of the Layered Metamodel (L-MM) defined in [18].

Definition 1 (Layered – Security Metamodel: L-SM). A layered security metamodel L-SM = {*n*, *SAL*, *SMECla, Rel,Mul ,SST ,RelLab*} consists of: (i) a security metamodel name *n*; (ii) an security abstract level *SAL* of a hierarchical or layered application model (CIM, PIM, or PSM); (iii) a finite-set *SMECla* of the modeling element classes for security construct (security service, security policy, ...); (iv) four relations *Rel* between *MECla* (association, inheritance, aggregation, dependency), where Rel ⊆ (*SMECla* x *SMECla*); (v) two multiplicity numbers *Mul* between *MECla,* where *Mul* ⊆ (*MECla* x *MECla*) (O..1, 0..*); (vi) a finite-set *SST*(option) of stereotyped security classes (authentification, ...) for a *SMECla*; (vii) and a finite-set *RelLab* of relationship labels between *SMECla.*

The FSMA-MM-Security added in <Figure 3> has key and essential elements of security properties, analyzed in paragraph 2.1, for designing security models, and this can be defined as shown in <Figure 4>.

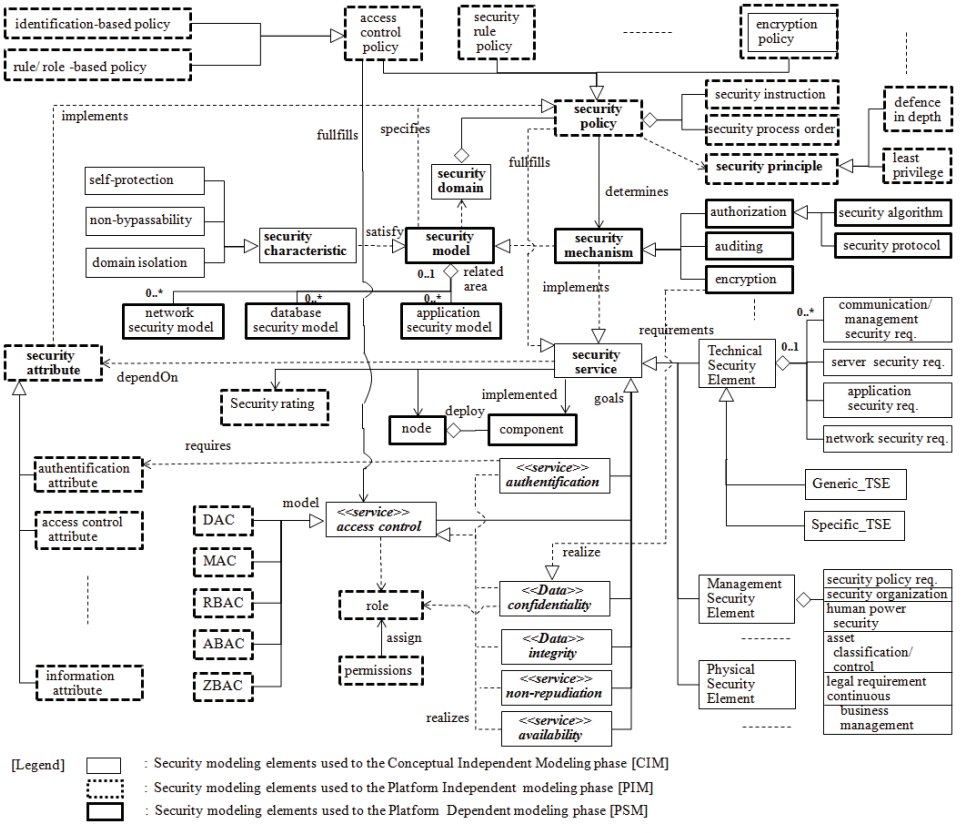

그림 4. 계층적 보안 메타모델: FSMA-MM-Security

Figure 4. A layered security metamodel with hierarchy: FSMA-MM-Security

The FSMA-MM-Security are defined by the relationships between security-related elements including attribute, service (goal), characteristics, mechanism, policy, principles, element, etc. For instance, through this metamodel, it can be easily understood that security service is dependent on security attribute and implemented by security mechanism.

In addition, security modeling elements should be hierarchized in order to provide hierarchical modeling based on the Model Driven Architecture (MDA) that supports modeling according to development abstraction levels. The MDA method[17] defines security metamodel with three phases based on the patterns of the Conceptual Independent Modeling (CIM), Platform Independent Modeling (PIM) and Platform Specific Modeling (PSM). For example, security element, security domain and security characteristics are security elements to be designed in the CIM phase; security policy and access control model in the PIM phase; and security model and security mechanism in the PSM phase. With this, security models can be created and reused based on abstraction levels by using modeling elements designed by development phases.

Meanwhile, since the FSMA-MM-Security is defined by hierarchizing existing security elements, not adding new modeling elements, profiles defining individual modeling elements are excluded herein.

Among the components in <Figure 3>, the FSMA-MM-Integration is defined as shown in <Figure 5> by using key elements of individual metamodels required to establish function and security models through three-layered modeling phases.

For function objects and security objects, key elements of each metamodel are recognized first, and modeling elements are connected and defined vertically (specifying models) and horizontally (connecting functions with security) in modeling process. BPMN metamodel[19] and UML metamodel[18] are targeted to model function objects. For security objects, the FSMA-MM-Integration is defined using the FSMA-MM-Security in <Figure 4>. The FSMA-MM-Security is hierarchized to ensure application models (function, security) can be established according to their levels based on CIM, PIM and PIM modeling phases.

Vertical mapping of business development methodology and software development methodology (between BPMN and UML) expresses detailed realization according to development abstraction levels based on [20]. This means that elements of BPMN models such as swimlane, activity, and gateway (AND, OR, etc.) are individually converted and mapped to actor and use case of use case model. For instance, the “AND” gateway of the BPMN model is converted into the “include” relationship between use cases of a use case model. In addition, mapping between UML models − such as relationship between a use case model and a class model, sequence model, component model or deployment model − is defined based on the FSMA-MM-Integration suggested in [18].

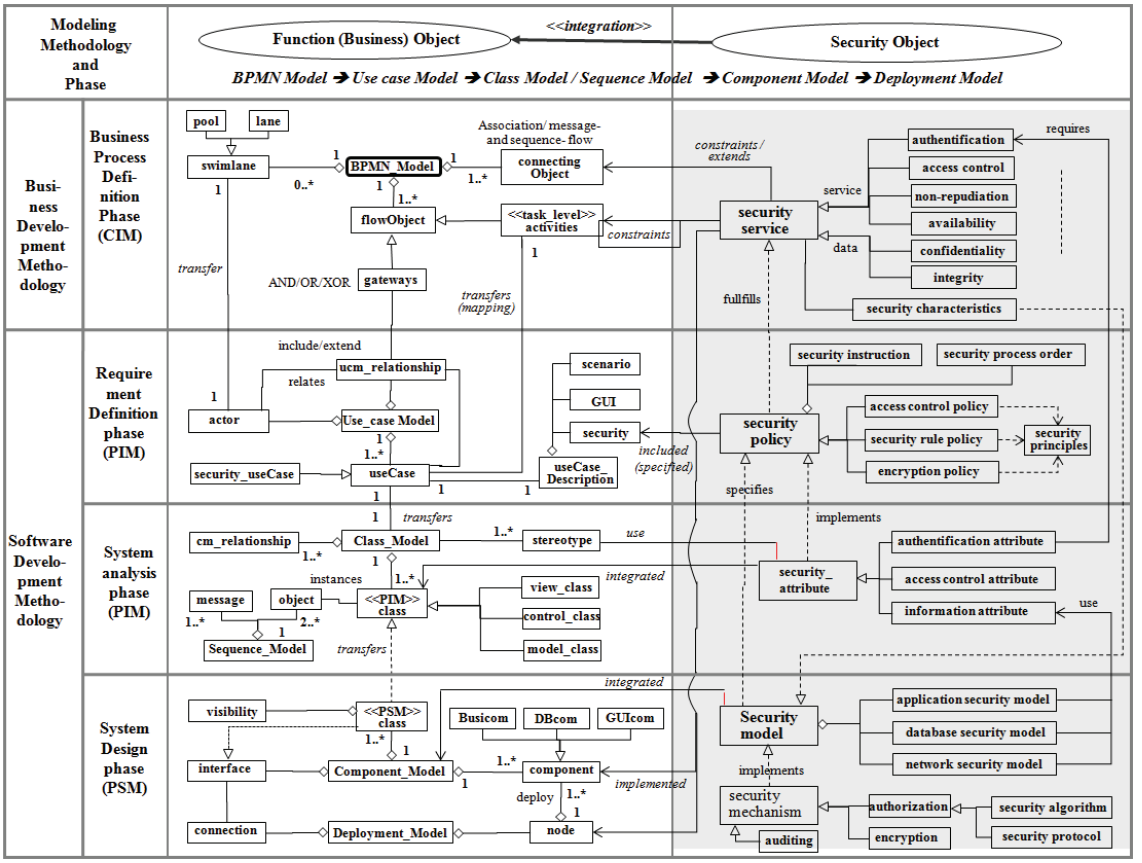

그림 5. 기능과 보안 모델링의 상세 통합 메타모델: FSMA-MM-Integration

Figure 5. The detailed and integrated metamodel of function and security modeling: FSMA-MM-Integration

Horizontal mapping of business objects and security objects is expressed by relating security elements that can limit function elements between models. The activity and function elements of connecting objects (association, message flow, sequence flow) of BPMN models can demand the security goal elements of the security model based on the characteristics (or constraints) of the practice. This can be expressed with a link of the security service (or goal) that should meet the related activity. Therefore, the limits can be expressed with the relationship between activity/connecting objects of BPMN and the "constraint" between security goal elements of security.

In designing application models here, these hierarchical modeling elements of the metamodels (BPMN, Use case, security, etc.) can be applied to create hierarchical models according to abstraction levels for function and security requirements.

3.1.3 Transformation Profile between Models

As seen in the FSMA-MM-Integration, function and security modeling is specified and created through transforming and mapping between different models.

<Table 2> shows the comprehensive transformation profile between modeling elements for vertically mapping between individual metamodels in <Figure 5>. Transforming and mapping between UML models were based on the proposals in [18]. This provides mapping between modeling elements from a use case model to a deployment model. In mapping between elements for the function modeling in <Table 2>, the "activity" element of BPMN is transformed to the "use case" element of a use case model, and later to the "class" element of a class model. In mapping between modeling elements for security modeling, for instance, the policy of security is coding user information through operation within the class of the class model. Thus, the policy is converted and expressed as <<entity>> class.

표 2. 기능과 보안 설계를 위한 모델간 변환 프로파일

Table 2. Conversion profile among models for function and security design

Model / Modeling element		BPMN model	Use case model	Class model	Component model	Deployment model
Function	**activity**	activity	use case	class	component (set of class)	Node (set of component)
	process	connecting object(flow, sequence)	Null	*relationship (association)*	Null	Null
	interface	Null	Null	interface	interface	connection
Security	**service (goal)**	<<security>> service	Secure use case Misuse case	<<security service>> class	<<security service>> component	<<security service>> node
	policy	Null	Security policy (UCDescription)	*<<security>> <<entity>> class(operation)*	*<<security>> component*	*<<security>> node*
	Attribute	Null	Null	*<<security>> <<entity>> class (attribute)*	*<<security>> component*	*<<security>> node*
	Mechanism (protocol, algorithm)	Null	Null	*<<security>> <<control>> class (operation)*	*<<security>> component*	*<<security>> node*

3.2 Integrated Modeling Process for Function and Security Design

In order to establish an integrated modeling process for function and security design, a framework should be first defined and based on the framework the modeling process can be created. The modeling process show modeling practices (creating function and security models) required to be written by development phases. The practices of creating models here are performed by using the components of individual

(integrated) metamodels discussed in paragraph 3.1.2.

3.2.1 Integrated Modeling Framework of Function and Security Design

As shown in <Figure 6>, the FSMA-MPF (Modeling Process Framework) organizes components of individual (<Figure 4>, etc.) and integrated metamodel (<Figure 5>, etc.) according to modeling development procedures based on the architecture (FSMA in <Figure 2>) defined above.

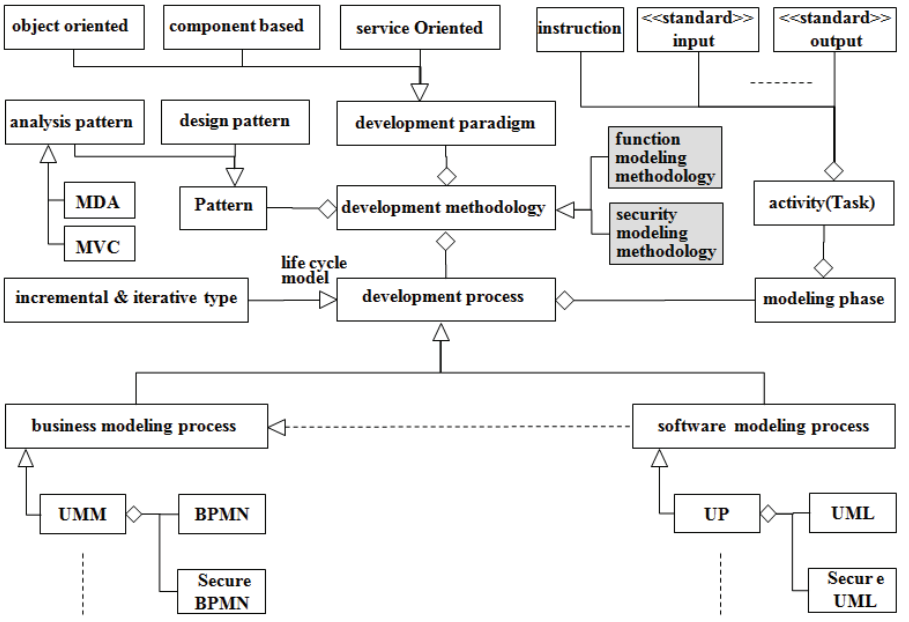

그림 6. 기능과 보안 통합을 위한 모델링 프로세스 프레임워크의 메타모델: FSMA-MPF

Figure 6. Metamodel of Modeling Process's Framework for integrating function and security: FSMA-MPF

This modeling framework added elements of function and security modeling methodologies in [17] (in the lower part). Development methodologies are composed of paradigms and process. Business modeling process and software modeling process provide methods of functional modeling and security modeling respectively.

3.2.2 Integrated Modeling Process of Function and Security Design

First, the FSMA-FSIMP (Function Security Integrated Modeling Process) created under this framework is defined as follows:[19]

Definition 2 (Function Security Integrated Modeling Process: FSMA-FSIMPro). A function - security integrated modeling process

FSMA-FSIMPro = (n, *FSIMP*, —, I)

consists of: (i) the function - security integrated modeling process name n; (ii) a finite-set FSIMP

of function-security integrated modeling phases; (iii) a process order relation (between modeling phases) — ⊆ (FSIMP x FSIMP); and (iv) flow iteration *I* (iteration#1, iteration#2, ...) over the modeling process according to the spiral model.

Definition 3 (Function Security Integrated Modeling Phase: FSMA-FSIMPha). A function - security integrated modeling phase

FSMA-FSIMPha = (*n*, *ACT*, →, *WP*)

consists of: (i) the function - security integrated modeling phase's name *n*(business process definition phase,…); (ii) a finite-set *ACT* of activities I, j, k ∈ FSIMP, where ACT is a subset of FSIMP, where the activity can contain options ([ACT]) or can be mandatory (ACT); (iii) a transition relation → ⊆ (ACT x ACT), where → contains the relation type of previous/after and fork/join among the activities; and (iv) the output or work product *WP* of an activity.

Based on [Definition 2] and [Definition 3], the FSMA-FSIMP is defined with metamodels as shown in <Figure 7>.

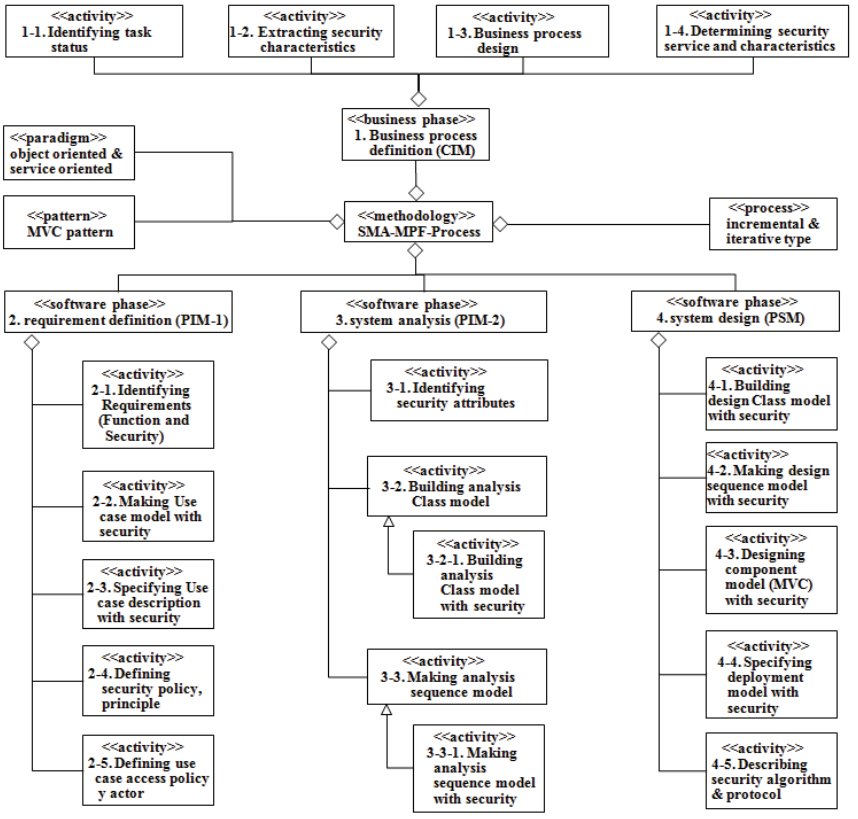

그림 7. 기능과 보안 설계를 위한 통합 모델링 프로세스의 메타모델: FSMA-FSIMP

Figure 7. Metamodel of Integrated Modeling Process for function and security design: FSMA-FSIMP

The process is composed of four phases from business modeling to software modeling, and each phase is composed of required activities. In the modeling phase, activities such as business process definition, system analysis and system design are conducted. Each phase is composed of multiple activities and each activity includes modeling practices related to function and security design. Through such phases and activities, application models for function and security design are created hierarchically by using modeling elements (<Figs.> 7 and 8) layered according to abstraction levels. <Figure 8> shows that activities of the FSMA-FSIMP can be organized in order and visualized by adding relationships between activities based on <Figure 7>. This modeling process is organized with a spiral and repetitive lifecycle through six development phases based on the MDA to do modeling function and security of development systems and can continuously upgrade and extend models.

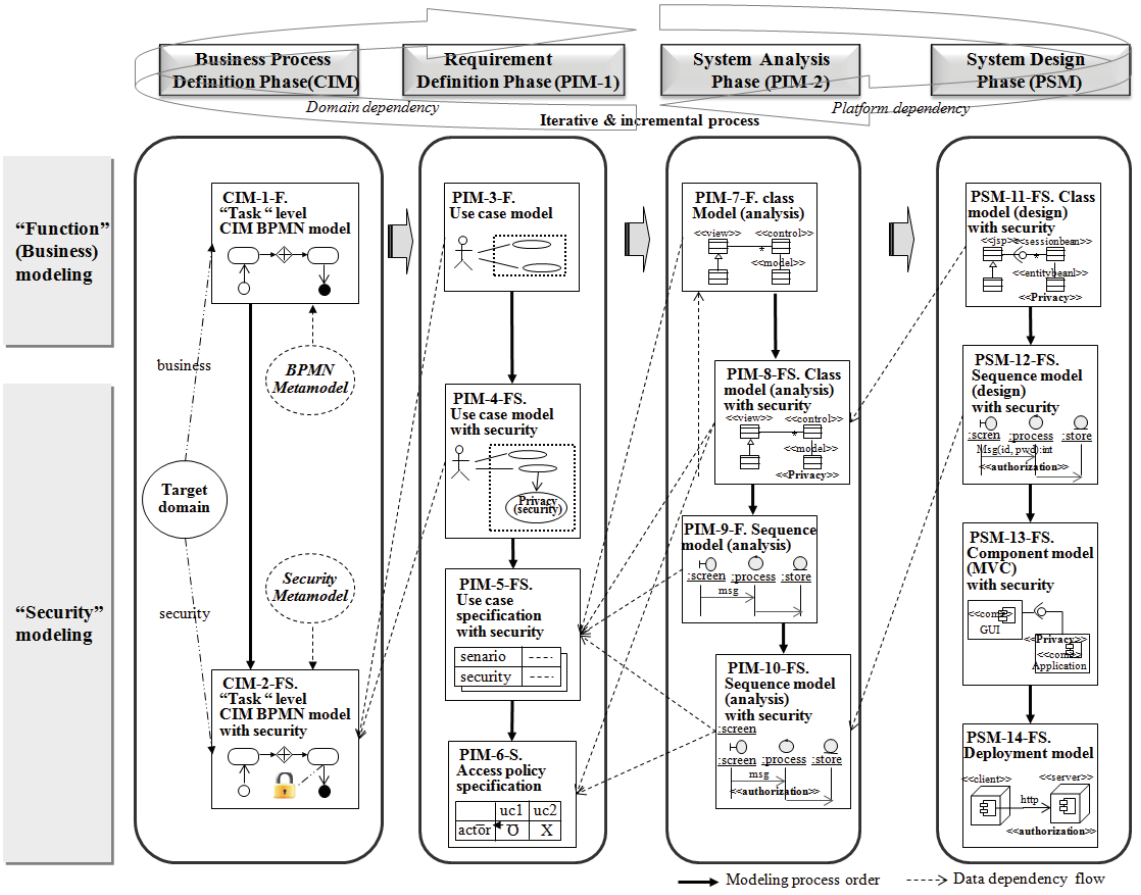

그림 8. 기능과 보안 설계를 위한 통합 모델링 프로세스: FSMA-FSIMP

Figure 8. Integrated Modeling Process for function and security design: FSMA-FSIMP

The process should be established to ensure that each phase is composed of activities; that each activity defines detailed process guidelines; that deliverables are obtained through activities; and that individual deliverables have connections between themselves.[19] The application models of function and security design here create models using hierarchical modeling methods based on the patterns of CIM/PIM/PSM in different forms by abstraction levels. This modeling process is as follows:

In the business process definition phase of the business modeling (CIM), application models for function requirements are created by using modeling elements of the XL-BPMN metamodel in [19]. By adding security requirements (6 security services) and properties to this model, integrated BPMN application models of function and security design are created.

Next, for UML-based software modeling, a use case model is created by applying a transformation profile between BPMN and use case model shown in paragraph 3.1.3 in the requirement definition phase (PIM-1), and security elements related to each use case are added. In this phase, security policies and grades are specified. In the system analysis phase (PIM-2), security is added to class models and sequence models by each use case independent from platforms in order to describe security in detail. In the system design phase (PSM), system architecture models and internal objects are designed by harmonizing function and security dependent on certain platforms. System architecture designs should first create component models that express function and security and develop deployment models based on these components. In designing objects comprising the inside of the component, the platform environment is reflected based on class models and sequence models in the analysis phase, and interfaces are added to create object models to ensure security is added to the final function model.

4. Case Study

To test the effectiveness of the proposed methods, practices are conducted and deliverables by activities are described based on the procedures of the FSMA-FSIMP in <Figure 8> and the transformation mapping between modeling components in <Table 2>, targeting the OSMS (Online Shopping Mall System). Each activity is conducted to do modeling by using modeling components of the FSMA-MM-Security (<Figure 4>), UML MM[18], and FSMA-MM-Integration (<Figure 5>) hierarchized by development phases.

4.1 Business Process Definition Phase for OSMS System (CIM)

In the business process definition phase, the control flow of the business process of the OSMS system is specified centering on domains at the conceptual level. First, the function of business is modeled through the practice of “CIM-1-F. Task level CIM BPMN model” (<Figure 8>), and security is added to this model through the practice of “CIM-2-FS. Task level CIM BPMN model with security.” In other words, the BPMN model is created with the activities of the task size by using the BPMN

metamodel[19] and modeling components such as activity and gateway (AND-split, etc.) in <Figure 5>. Then, in the FSMA-MM-Security (<Figs.> 4 and 5), security requirements are added to and expressed in the BPMN model by using modeling components (<Figure 4>) of the CIM level - security service (goal) and security characteristics. The expressions of security in the BPMN model use those in [3-7].

The deliverable of this phase is the integrated business model of function and security design as shown in <Figure 9>. Security requirements are expressed using stereotypes on the control flow of the BPMN model. <<① Authentification>> in <Figure 9> requires authenticating users to allow only subscribers to use the system. To do so, the security of authentification is expressed as the "provide customer info." activity in the customer section. This means that customer should provide the information (id, password for login) for authentification. Therefore, <<① Authentification>> is attached to "provide customer info." activity. As <<② Confidentiality>> requires confidentiality of access to product information, Authentification is expressed as data object of "product information" in the "search product list" activity.

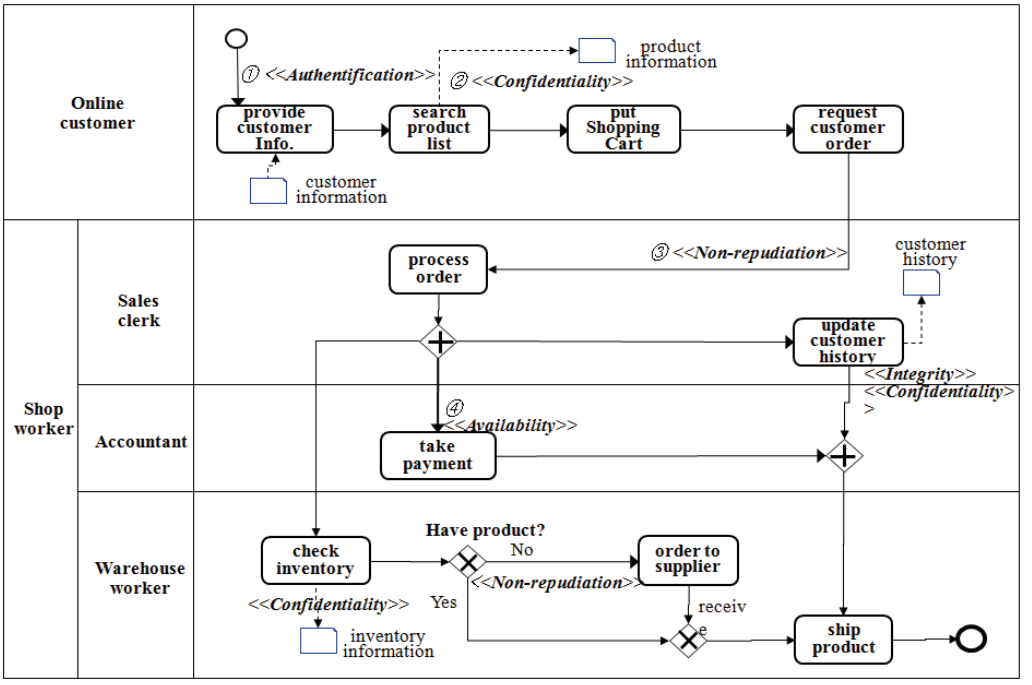

그림 9. OSMS 시스템의 보안이 가미된 CIM BPMN 모델: CIM-2-FS

Figure 9. CIM BPMN model with security of OSMS system: CIM-2-FS

4.2 Requirement Definition Phase for OSMS System (PIM-1)

In the requirement definition phase, requirements of function and characteristics of the

OSMS system are specified based on the BPMN business model. Through the “PIM-3-F. Use case model” practice (<Figure 8>), the function of software is modeled, and security is added to this model through the practice of “PIM-3-FS. Use case model with security.” Then, requirements of function and security design are specified and described through the practice of “PIM-3-FS. Use case specification with security.” In addition, security polices of individual use cases are defined. In this phase, security is expressed by defining the roles and types of PIM-level modeling components including security policy and access control (<Figure 4>).

In converting the BPMN model to the use case model, activities on the BPMN model (<Figure 9>) are expressed as function (or normal) use cases of the use case model (<Figure 5> and <Table 2>); pool/lane as actor; and security limitations on the control flow as stereotyped use cases or security use cases respectively. The use case model (not including misuse cases) with security added to it is shown in <Figure 10>.

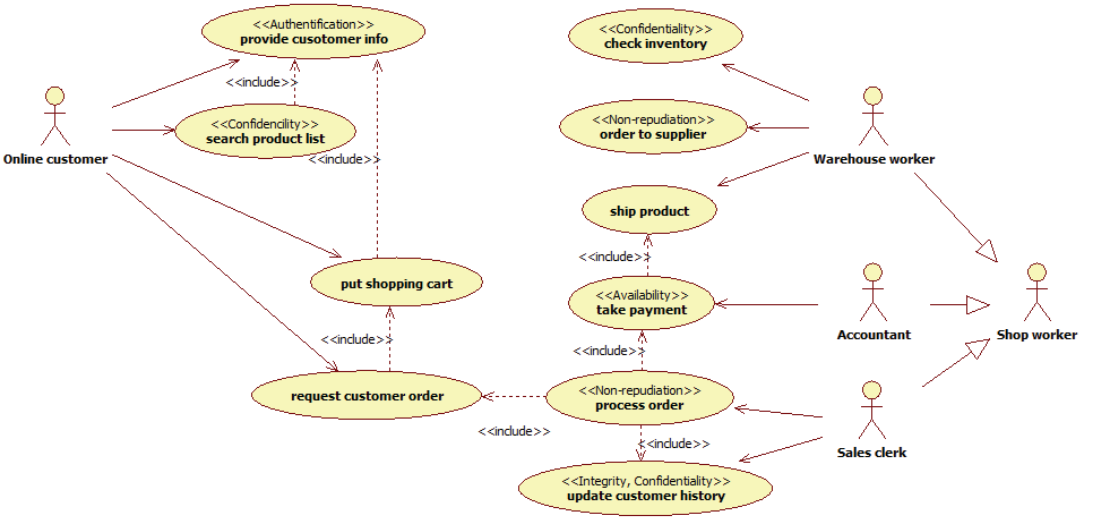

그림 10. OSMS 시스템의 보안이 가미된 유스케이스 모델: PIM-4-FS

Figure 10. Use case model with security of OSMS system: PIM-4-FS

Next, in order to specify use cases, use case specifications are written. For instance, function and security are expressed in the “provide customer info.” use case as shown in <Table 3>. Security requirements of “Authentification” that this use case should meet are listed in this form in detail.

In this phase, for hierarchical modeling of security, security policies on access should be defined by use cases provided from the OSMS system as shown in <Table 4>[15]. In addition, security policies on data should be written under format items such as security objects, persons in charge, related security policies, risk, security measures, affected areas in case of infiltration, measures to reported incidents, time required, etc.

표 3. 보안이 가미된 “provide customer info." 유스케이스명세서: PIM-5-FS

Table 3. The “provide customer info.” use case specification with security: PIM-5-FS

Use case name	provide customer info.		
actor	Online customer	**priority**	1 (high)
Overview	For using OSMS service, online customer provides login information.		
Pre-condition	Non-login Member-registration	**Post-condition**	login
Normal(basic) Scenario	1. Customer accesses to OSMS system. 2. System displays login screen. 3. Customer inputs the information of ID and Password, then select login button. 4. System check whether customer is the registered menber or not.		
Non-function requirements (security)	- Only the registered customer has access authority to OSIS system - It needs login to use the OSMS system. (**Authentication**) - Reading and writing from unauthorized entity is forbidden. (**Confidentiality, Integrity**)		

표 4. 유스케이스별 접근 제어의 보안 정책: PIM-6-S

Table 4. Access control security policy of use case: PIM-6-S

Name of use case	Online customer	Sales clerk	Accountant	Warehouse worker
Provide customer info.	○	○	○	○
Process order	X	○	△	X
Take payment	X	○	○	X
Ship product	X	△	△	○
….	….	….	….	….

[legend] ○:All authority, △:Partial authority, X:No authority

In addition, <Table 5>[2] is shown security rating.

표 5. 보안 서비스의 보안 등급

Table 5. Security rating for security services (goals)

Name of security service	Security rating
Confidentiality	customer secret, top secret, external secret, general secret
Integrity	high, middle, low
Availability	1 minute, 1 hour, 1 day, 1 week, 1 month
… .	…….

4.3 System Analysis Phase for OSMS System (PIM-2)

In the system analysis phase, components of the OSMS system that can meet requirements are specified based on the use case model and the use case specifications at the PIM level independently from the platform environment. Class models are created by adding the “PIM-7-F” function modeling to the “PIM-8-FS” security modeling based on the use case model. In addition, dynamic sequence models are created by adding security through the “PIM-9-F” and “PIM-10-FS” practices.

In the security modeling that uses hierarchical modeling components in <Figure 4> in this phase (PIM phase), detailed properties required for implementing security policies are specified under the class attribute section, and their actions under the operation section. The same procedure is also conducted in the sequence model. At this point, important security property information (“Security attribute” in <Figure 4>) should be described in a separate form of profile in detail. In addition, the RBAC is selected as access control model (type) in the OSMS system. With this, the role of authority is granted by actors in <Figure 10>.

The class model with security added to it is shown in <Figure 11>. For instance, in the "<<Authentification>> provide customer info" use case (<Figure 10>), authentification is performed by the operation section within the "login_manage" class (<Figure 11>).

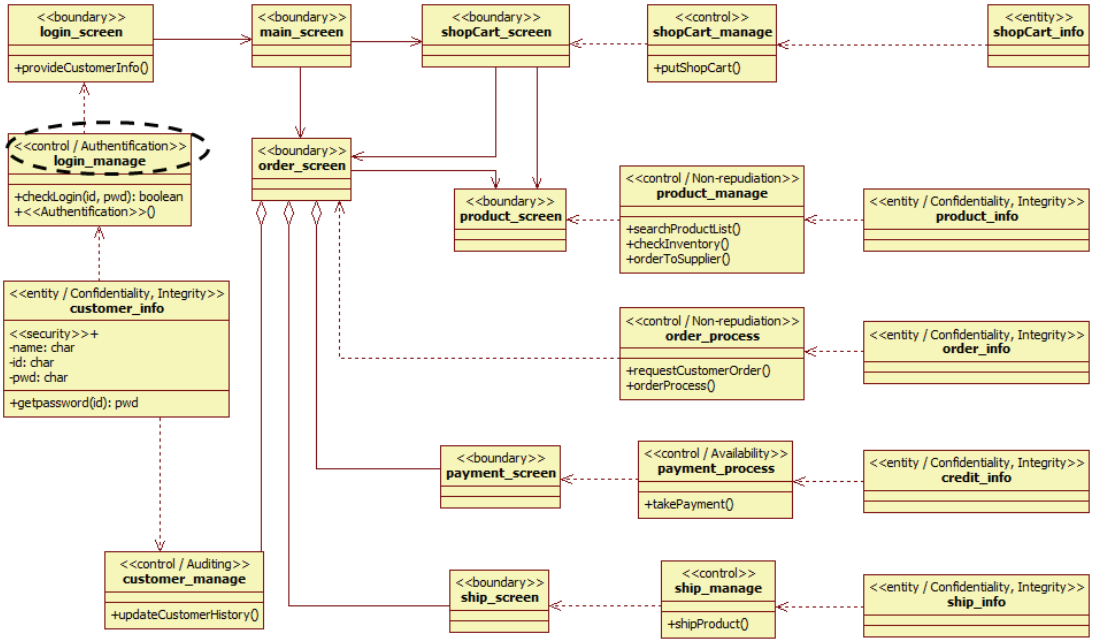

그림 11. OSMS 시스템의 보안이 표현된 클래스 모델: PIM-8-FS

Figure 11. Class model with security of OSMS system: PIM-8-FS

Figure 12 shows the sequence model of the login of the OSMS system.

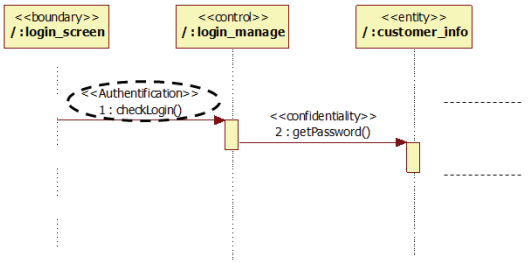

그림 12. OSMS 시스템의 "login" 보안 가미된 순차모델: PIM-10-FS

Figure 12. Sequence model with security of "login" in OSMS system: PIM-10-FS

4.4 System Design Phase for OSMS System (PSM)

In the system design phase, subject to the platform environment (applying EJB in this paper), system architecture and detailed internal components and actions (movements) are designed to implement the OSMS system based on the analysis model (class model and sequence model).

The object design specifies in detail the inside of the class (attribute, operation) and creates the class model ("PSM-11-FS") and the sequence model ("PSM-12-FS") that include security. The system architecture designs the component model

and deployment model where security is added to.

The security design in this phase is for environment security and application security. Environment security describes security on network, server, DB, backup/restoration, access control, etc. Application security describes in detail security mechanism, security algorithm, security protocol, etc. under the operation section of the class in order to realize the security (for instance, authentification) of the class(<Figure 13>) at the PSM level (<Figs.> 7 and 8).

As system architecture cases, <Figure 13> shows a deployment model of execution components. In the case of large-sized systems, architecture models are written after being segmented into application model (function), data base model and network model.

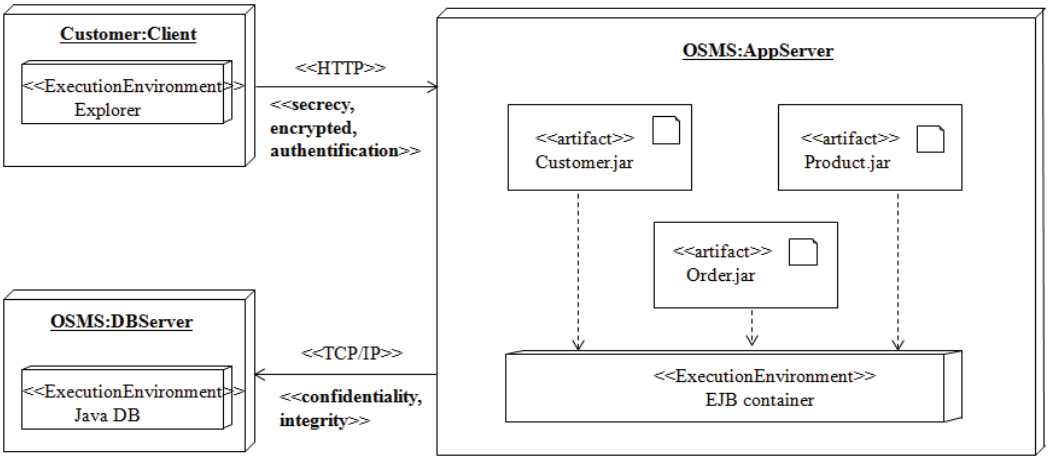

그림 13. OSMS 시스템의 보안이 표현된 배치 모델: PSM-14-FS

Figure 13. Deployment model with security of OSMS system: PSM-14-FS

5. Evaluation

5.1 Comparative Evaluation with the Existing Method

In order to compare proposed methods in this study and existing methods together, matrices related to metamodel and modeling process was analysed as shown in <Table 6>.

In <Table 6>, the perfect score of each item was 1.0. In addition, support levels or degrees of compared methods were listed by individual items. SG-SSDI proposed security development methodologies that covered security activities and detailed guidelines by phases from developing software to testing, and ISSE proposed SOA-based security modeling methods and integrated modeling between security and software engineering. D-OOADM also suggested UMLSec-based integrated modeling methods for function and security design from defining requirements to implementing.

표 6. 메타모델과 프로세스에 대한 기존 방법과의 비교

Table 6. Comparison of metamodel and process with legacy method

Assessed items (point)	SG-SSDI [2]	ISSE [8]	D-OOADM [15]	Proposed method
Function – security Integrated architecture (1.0)	0.25	0.50	0.25	0.75
Function – security integrated Layered metamodel (1.0)	0.25	0.25	0.25	0.75
Layered security metamodel (1.0)	0.25	0.25	0.25	1.00
Security development Methodology (1.0)	1.00	1.00	0.50	0.25
Function – security Integrated modelling process (1.0)	0.25	0.75	0.75	0.75
Hierarchical designing by layered metamodel or process (1.0)	0.50	0.50	0.50	0.75
Business – software linked Modelling (1.0)	0.25	0.50	0.25	0.75
MDA/MVC-based modelling (1.0)	0.25	0.75	0.25	0.75
Conversion profile between Models (1.0)	0.00	0.00	0.00	0.25
Weight total 100% (9.0)	37.5% (3.00)	56.6% (4.50)	37.5% (3.00)	75% (6.00)

[Legend] 1.00: very highly supported; 0.75: highly supported; 0.50: medium supported; 0.25: low supported; and 0.0: not supported

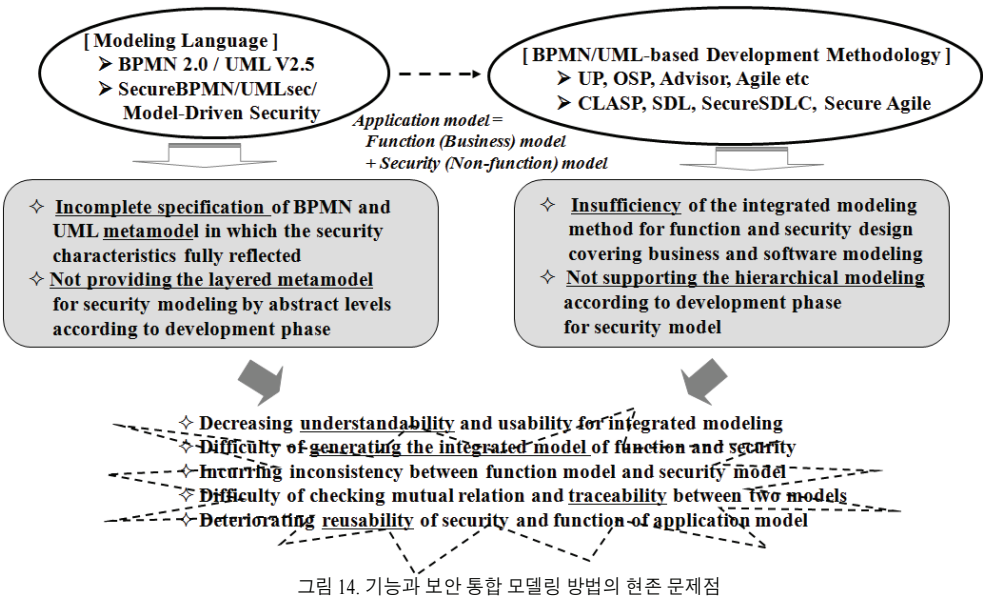

그림 14. 기능과 보안 통합 모델링 방법의 현존 문제점

Fig 14. The legacy problems of function and security modeling methods

However, they did not cover all the ranges of the connected business and software modeling and the integrated modeling of function and security design, and the unified architecture, metamodel and process was not detailed enough. Methods of transforming between models, for example, how function and security was hierarchically modelled through development phases and what kinds of modeling components were used were not clear enough. As shown in Fig. 14, however, previously-used modeling languages and development methodologies for function and

security modeling have various issues. In other words, metamodel of BPMN and UML has not been clearly defined to sufficiently provide security properties in such languages.

5.2 Characteristics

The characteristics and expected effects of proposed methods are as follows:

- Security property-driven
  - Security metamodel is proposed based on security properties such as service, attribute, policy, technique, etc.
  - Security models by abstraction levels can be created by using hierarchical security metamodel.
- Metamodel-driven
  - Modeling practices become convenient by using standardized modeling elements of and their relationships of individual and integrated metamodel.
  - More flexible extendability and alterability can be secured by providing metamodel-driven architecture and framework.
- Integration-driven
  - Flexible connected modeling is provided to express security elements, centering on function models.
  - Connected modeling is supported from business to software modeling practices.
- Model pattern-driven
  - The number of reuse models can be maximized by using approaches such as the CIM/PIM/PSM of the MDA, and Model/View/Control methods.
  - Independent modularity between models is strong, and effects of modification can be minimized.

6. Conclusion

This study proposed metamodel and development process for integrated modeling of function and security that covers from business modeling to software modeling. For ensuring the reliability of this approach, this method was applied to the design of an OSMS system. Application models were made in clear and seamless by using more formalized modeling elements (in layered metamodel) and hierarchical modeling process according to the abstraction level of system development. As regards the expected effectiveness, it was possible to establish application models that could integrate function and security consistently from the early business service modeling to the software modeling for execution components. In particular, integrated models of function and security design can be created according to abstraction levels based on hierarchical modeling elements and process, improving the reusability of application models. As follow-up studies, it is required to specify guidelines for related activities within the FSMA-FSIMP, and practices of more application cases need to be created.

References

[1] Korea Information Security Agency, *Development of software architecture-based*

design model and architecture specification method, 2007.

[2] Korea Information Security Agency, *Security guide V1.0 for secure software development and Introduction*, 2008. [SG-SSDI]

[3] A. Rodriguez, E. F. Medina, and M. piattini, *A BPMN extension for the modeling of security requirements in business processes*, IEICE TRANS. INF. &SYST., Vol. E90-D, No. 4, pp. 745-751, 2007.

[4] C. Wolter, M. Menzel, and Christoph Meinel, *Modelling security goals in business processes*. In Modellierung 2008, LNI P-127, 2008.

[5] S. H. Turki, F. Bellaaj, A. Charfi, and R. Bouaziz, *Modeling security requirements in service based business processes*, Enterprise, Business-Process and Information Systems Modeling, Lecture Notes in Business Information Processing, pp. 76-90, 2012.

[6] Y. Cherdantseva, J. Hilton, and O. Rana, *Towards secureBPMN - aligning BPMN with the information assurance and security domain, business process model and notation*, Lecture Notes in Business Information Processing, pp. 107-115, 2012.

[7] M. Q. Saleem, J. B. Jaafar, and M. F. Hassan, *Secure business process modeling of SOA applications using UML-SOA-SEC*, International Journal of Innovative Computing, Information and Control, Vol. 8, No. 4, pp. 2729-2746, 2012.

[8] H. Mouratidis and P. Giorgini, *Integrating security and software engineering: Advances and future vision*, IGI Publishing Hershey, PA, USA, 2006. [ISSE]

[9] D. G. Firesmith, *Security use cases*, Journal of Object Technology, Vol. 2, No. 3, pp. 53-64, 2003.

[10] G. Popp, J. Jurjens, G. Wimmel, and R. Breu, S*ecurity-critical system development with extended use case*, Tenth Asia-Pacific Software Engineering Conference, pp. 478-487, 2003.

[11] L. L´ucioa, Q. Zhangb, P. H. Nguyenb, M. Amrani, J. Klein, H. Vangheluwe, and Y. L. Traon, *Advances in model-driven security*, Advances in Computers, pp. 103-152, 2014.

[12] P. H. Nguyen, M. Kramer, J. Klein, and Y. L. Traon, A*n extensive systematic review on the Model-Driven Development of secure systems*, Information and Software Technology, Vol. 68, pp. 62-81, 2015.

[13] D. Hatebur, M. Heisel, J. Jürjens, and H. Schmidt, *Systematic development of UMLsec design models based on security requirements, fundamental approaches to software engineering*, LNCS 6603 Springer, pp. 232-246, 2011.

[14] D. Basin, and J. Doser, *Model driven security: from UML models to access control infrastructures*, Journal ACM Transactions on Software Engineering and Methodology (TOSEM), Vol. 15, No. 1, pp. 39-91, 2006.

[15] K. S. Joo, and J. W. Woo, D*evelopment of object-oriented analysis and design methodology for secure web applications*, International Journal of Security and Its Applications, Vol. 8, No. 1, pp. 71-80, 2014. [D-OOADM]

[16] M. Bishop. *Computer security: art and science*, Vol. 200, Addison-Wesley, 2012.

[17] C. Y. Song, and E. S. Cho, *An integrated design method for SOA-based business modeling and software modeling*, International

Journal of Software Engineering and Knowledge Engineering, Vol. 26, No. 2, pp. 347-377, 2016.

[18] C. Y. Song, and D. K. Baik. *A layered metamodel for hierarchical modeling UML*, International Journal of Software Engineering and Knowledge Engineering, Vol. 13, No. 2, pp. 191-214, 2003.

[19] C. Y. Song, and E. S. Cho, *An service oriented XL-BPMN metamodel and business modeling process*, Journal of Korea Information Processing Society, Vol. 2, No. 4, pp. 1-12, 2013.

[20] Y. Rhazali, Y. Hadi, and A. Mouloudi. *Transformation method CIM to PIM: from business processes models defined in BPMN to use case and class models defined in UML*, International Journal of Computer, Electrical, Automation, Control and Information Engineering 8.8, pp. 1453-1457, 2014.

기능과 보안의 통합 설계를 위한 소프트웨어 모델링 방법

송치양[1], 김유환[2]

[1] *경북대학교 소프트웨어학과*

[2] *네바다대학교 라스베가스, (미국)*

요 약

보안은 소프트웨어 개발 프로세스의 중요한 부문이 되어 왔다. 기존 연구에서 보안의 특성과 정책이 충분히 반영되고 기능과 보안이 조화된 초기 비지니스 모델링에서 소프트웨어 모델링에 이르는 체계적인 개발 프로세스가 미약하다. 이에, 기능 모델과 보안 모델이 상호 통합된 어플리케이션 모델의 생성이 어렵다. 본 연구는 보안의 특성과 정책이 가미된 어플리케이션을 개발하기 위하여, 시스템의 기능(비지니스)과 보안의 요구사항에 대해서 개발의 추상화 정도에 따라 상호 통합되어 계층적으로 모델링 할 수 있는 메타모델, 프레임워크와 프로세스를 제시한다. 즉, 어플리케이션 개발의 기능과 보안(비 기능)을 위한 통합 모델링 프레임워크와 프로세스를 정립한다. 이 통합 모델링의 프로세스는 개발 단계에 따라 비즈니스 모델링과 소프트웨어 모델링의 방법에 걸쳐서 정의한다. 이로서, 기능과 보안 요구사항을 제시 통합 방법의 프로세스에 따라서 좀더 명확한 응용 시스템의 모델화를 통해서 신뢰성이 있는 시스템 개발을 도모할 수 있다.

Acknowledgments

This Research was supported by Kyungpook National University Research Fund, 2012

이 논문은 2012학년도 경북대학교 연구년 교수 연구비에 의해 연구되었음

Chee-Yang Song received the bachelor and master's degrees in Computer Science from the Hannam university in 1985 and the Chungang University in 1987, respectively. He received the Ph.D. degree in Computer Science from Korea University in 2003. From 1990 to 2004, he was a researcher Research center of Korea Telecom (KT). He has been a Professor in the Department of Software at Kyungpook National University since 2008. His research interests include service oriented modeling, business-software integrated design process, component based software engineering, and security design.

E-mail address: cysong@knu.ac.kr

Yoohwan Kim received the bachelors in Economics from Seoul National University in 1989. He received the M.S. degree and the Ph.D. degree in Computer Science from Case Western Reserve University, USA in 1994 and 2003, respectively. Between 1997 and 1999, he was a Member of Technical Staff at Bell Laboratories of Lucent Technologies. He has been an Associate Professor at the University of Nevada Las Vegas(UNLV) since 2004. His research interests include network security, secure systems design, cyber-physical system (CPS) security, and secure air traffic communications.

E-mail address: Yoohwan.Kim@unlv.ed