제33회 한국정보처리학회 춘계학술발표대회 논문집 제17권 제1호 (2010. 4)

보안 요구사항 모델링을 위한 UML 2.0 확장

조도형*, 주경수**
** *순천향대학교 컴퓨터학과
e-mail : jhodohyung@sch.ac.kr

UML 2.0 Extension for the Modeling of Security Requirements

*Do-Hyung Cho, **Kyung-Soo Joo
** *Dept of Computer Science and Engineering, SoonChunHyang University

요 약

보안은 비즈니스 성능에 있어 결정적인 문제점이지만 대게 보안은 비즈니스 프로세스 정의 후에 고려된다. 많은 보안 요구사항은 비즈니스 업무 레벨에 표현될 수 있다. 비즈니스 업무 모델은 그들이 소프트웨어 디자인과 창조를 위해 필요한 요구사항을 잡아낼 수 있기 때문에 소프트웨어 개발자를 위해 중요하다. 게다가 비즈니스 업무의 모델링은 지휘와 비즈니스 운영이 어떻게 개선되는지를 위한 중심이다. 이 논문은 활동 다이어그램을 통해서 안전한 비즈니스 업무를 모델링하기 위한 UML 2.0 확장을 설명한다. 전형적인 건강관리 업무에 이 접근을 적용할 것이다.

1. 소개

새로운 비즈니스 장에는 많은 참가자와 의사소통 및 정보기술의 집중적 사용에 있어 기업은 그들의 사업을 확장할 뿐만 아니라 그들의 취약성도 증가시킨다. 결과적으로 시스템 공격의 개체 수가 증가함에 따라 시스템 침입이 일어날 수 있다. 이러한 이유로 컴퓨터와 그들의 시스템은 가능한 최상의 방법으로 보호하는 것이 필요하다. 가장 최선의 보안은 반드시 완전한 보안을 의미하지 않고, 주어진 한도 내에서의 고급 보안이다. 다른 한편으로 비즈니스 프로세스는 비교를 유지하는 요소이다.

대부분 비즈니스 프로세서 도메인 전문가는 보안 전문가가 아니라는 사실 때문에 기능의 정확한 방법 프로세스 모델링에 집중해 비즈니스 프로세스 모델의 보안 중요성은 종종 무시된다. 일반적으로 보안은 시스템 정의 후에 고려된다. 비즈니스 프로세스 단계에서 흔히 보이는 고객과 사용자가 보안 필요를 표현할 수 있고, 후에 비즈니스 프로세스의 보안 요구사항을 쉽게 식별할 수 있는 연구 및 실험을 고려한다. 게다가 주요 기본에 동의하고 공통의 목표로 일하는 사업안에 다른 많은 이해 관계자들의 토론을 촉진하기 때문에 소프트웨어 시스템 명세에 가능한 정확해야 한다. 비즈니스 프로세스 모델링은 몇 가지 언어와 표기법이 있는데 UML(Unified Modeling Languag e)는 널리 인정된 표기법이다. 이전 것들에 관하여 UML 2.0의 가장 중요한 변화는 비즈니스 프로세스 표현을 개선하는 활동 다이어그램이다. 우리의 일은 비즈니스 분석가의 관점에서 활동 다이어그램으로 보안 요구사항을 통합하는 것을 허용하는 UML 2.0 확장을 고려한다.

우리의 제안은 MDA(model Driven Architecture)접근에 기반을 두고 있다. 우리는 UML을 이용하여 초기 요구사항을 정의하고 독립적인 명세를 실행 가능하도록 할 것이다. 게다가 우리는 추상적인 보안 레벨을 가진 요구사항에 대해서 두개의 다른 견해가 있다고 믿는다. 그들 중 하나는 비즈니스 분석가와 관련되어 있고 다른 것은 보안 전문가와 관련되어 있다. 이 문서는 우리는 첫 번째 관점인 비즈니스 분석가와 관련이 깊다.

2. 비즈니스 과정의 안전

비즈니스 프로세스 안전의 중요성에도 불구하고 두 가지 문제점을 찾아냈다. 첫째, 일반적으로 보안 요구사항을 지정하는 사람이 보안 요구사항 지정하는 대신에 아키텍쳐의 특정한 부분을 사용 금지하도록 하는 엔지니어이기 때문에 보안에 대해 만드는 것이 충분하지 않았다. 그리고 둘째, 보안을 응용프로그램의 실제 구현단계, 시스템 관리자 단계 또는 통합되어 아웃소싱과 같이 고려되었다. 모델 보안은 몇 가지 관점을 고려하는 접근 방식을 제시한다.

시스템 프로세스 관점에서의 프로세스 보안 정보에 관하여 정적이거나, 비즈니스 프로세스에 연구되는 수명주기로부터 보안 요구사항에 관하여 동적, 그리고 추상화의 높은 수준의 모든 관점 통합을 우리에게 제공하는 비즈니스 프로세스와 비즈니스 프로세스 관점에서 책임과 관련되어 있다. 게다가 시스템 개발 초기 단계에 시스템 보안 요구사항 확립하고, 깔끔한 비즈니스 기초를 이끌어 내고, 보안 요구사항 명세서처럼 적합한 비즈니스 구조 전망을 제안하는 것은 어려운 작업이다.

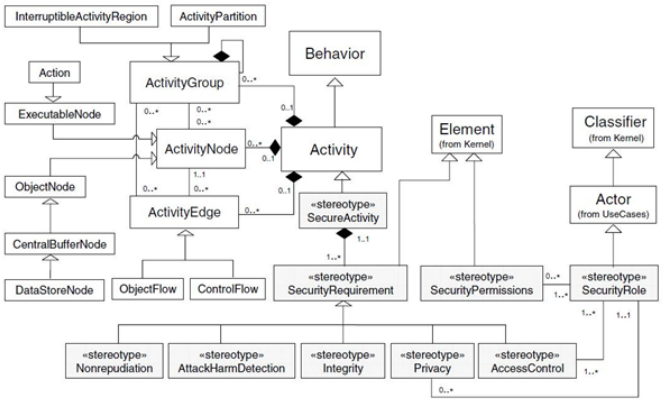
3. UML 2.0 활동다이어그램과 UML 2.0 확장

UML 2.0은 구조와 행동에 관한 설명으로 나누어진다. 행동 모델은 시간이 지남에 따라 시스템 변화의 구조적 측면을 지정한다. UML은 활동, 상태, 상호작용의 세가지 행동 모델을 가지고 있다. 활동이 다른 행동이 호출의 원인인 것은 객체들 사이에 메시지 전달의 상호작용을 설명하고, 이벤트가 다른 행동의 호출과 객체의 상태 변화를 어떻게 야기하는지 보여주는 상태머신이고, 다른 행동의 호출을 위해 입력과 출력 그리고 연속적인 활동 및 상태에 초점을 맞춘다. UML 이전 버전은 표현이 제한적이었고, 모델링에 접근함에 따라 객체에 적응하는데 사용하지 못하는 것으로 사용자들에게 혼란을 준다. 이제 도메인의 다양한 종류와 교차하는 흐름 모델링 지원이 가능하다. acti vity는 컨트롤과 데이터 흐름 모델을 사용하여 종속 동작 실행을 지정한다. 활동은 최후의 개인적인 활동을 결심하는 다른 활동을 기원하는 계층 구조를 형성할 수도 있다. 활동 다이어그램 그래픽 표현은 노드의 결합과 우리가 완전한 흐름 형태로 허용하는 연결이다. 다른 한편으로 프로필 패키지는 그것들을 다른 목적으로 적응시키도록 확장하는 현존하는 meta-model로부터 메타클래스를 허용하는 매커니즘을 표현 한다. 프로파일 매커니즘은 OMG Meta Object Facility(MOF)와 일치한다. UML 프로파일은 스테리오 타입 및 제약과 태그 값으로 이루어져 있다.

스테리오 타입은 이름과 기본 클래스에 의해 정의되는 모델 요소이다. 제약은 제한을 나타내는 목적으로 스테리오타입에 적용된다. 태그값은 스테리오 타입, 이름 쌍으로 열거에 할당되는 meta-attribute에 추가된다.

4. 보안 요구사항을 가진 비즈니스 프로세스 모델링을 위한 UML 2.0 확장

우리의 제안은 활동 다이어그램을 사용하는 비즈니스 프로세스에서 비즈니스 분석가가 보안 요구사항 연결하는 것을 허용한다. 보안 분석가에 의해서 차후에 보완되는 것을 가지고 있을 보안 요구사항 명세서의 첫 번째 부분이다. 두 가지 관점은 우리가 비즈니스 프로세스 보안 요구사항 명세서를 풍부하게 알려준다.



(그림 1) 보안 스테리오 타입을 포함한 UML 2.0확장

그림1은 보안 활동 명세서를 위한 스테리오 타입으로 UML 2.0 meta-model 확장 보여준다. Secure Activity는 Activity에서 파생된 스테리오 타입이다. «SecureActivity»은 보안 요구 스테리오 타입과 강하게 연관된다. «SecurityRequirement»은 «SecureActivity»와 연관관계를 가지고 있다. «SecurityRequirement»를 위한 제시한 표기법은 우리가 지정된 타입의 요구사항 유형을 확인하는 것을 허용할 것을 추가해서 써 넣어야 한다.

«SecurityRequirement»에서 파생된 스테리오 타입은 활동 다이어그램 요소에 추가될 수 있다. 어느 보안 요구사항(NR, AD, I, P or AC)은 활동 다이어그램 요소에 추가될 수 있다.(표1 참고) 예를 들어 «Integrity»요구 사항은 데이터 저장소, 흐름 제어 또는 객체 흐름에 지정될 수 있다. «SecurityRole» 와 «Security Permissions»은 둘다 UML 2.0 활동 다이어그램 요소에서 얻어질 수 있기 때문에 다른 방법으로 연관된다. 예를 들어 «SecurityRole»은 활동, 분할 또는 지역별 명세서에서 얻어질 수 있지만, 활동 다이어그램 요소에 명백한 방법으로 지정되지 않는다. «SecurityPermission»은 권한은 연관되어 있는 각 활동 다이어그램 요소에 의지하기 때문에 특별한 케이스 이다. 예를 들어, 활동 개체는 실행이나 실행 검사 작업은 지정되어야 한다.(표3 참조)

<표 1> 보안 명세서와 활동 다이어그램 요소

	활동 다이어그램의 견제를 위한 UML 2.0 요소					
	Activity	Activity Partition	Interruptible Activity Region	Action	Data StoreNode	Object Flow
Nonrepudiation (NR)						√
AttackHarmDetection (AD)	√	√	√	√	√	√
Integrity (I)					√	√
Privacy (P)		√				
AccessControl (AC)	√	√	√			
Security Role	√	√	√			
SecurityPermissions				√	√	√

추가적으로 우리는 약간의 새로운 태그값이 정의된 데이터 타입 정의가 필요하다. 표2는 새로운 데이터 스테리오 타입 명세를 보여줄 것이다. 모든 새로운 데이터 타입은 열거 클래스에서 파생되었다.

<표 2> 새로운 데이터 타입

이름	설명	관련 가치
SecReqType	보안 요구사항의 유형을 대표한다. 비거절, 공격/해, 무결성, 기밀성 또는 접근제한 지정되어야 한다.	NR, AD, I, P, AC
PerOperations	활동 다이어그램에 있는 목표에 가능한 연산들을 열거해 놓은 것이다. 이 연산들은 목표에 부여되는 허가와 관련 있다.	Execution, CheckExecution, Update, Create, Read, Delete, SendReceive, CheckSendReceive
ProtectDegree	강조를 대표하는 수준이다. 급은 low(l), medium(m), 또는 high(h) 일 수 있다.	l, m, h
PrivacyType	익명(a) 또는 기밀성(c)으로 이루어져 있다.	a,c
AuditingValues	비즈니스 프로세스에 있는 보안 요구사항 명세서와 관련 있는 다른 보안 이벤트를 대표한다.	ElementName, SourceName, DestinationName, DateTimeSend, DateTimeReceive, Date, Time, RoleName

<표 3> 보안 활동과 보안 요구사항 스테리오타입들

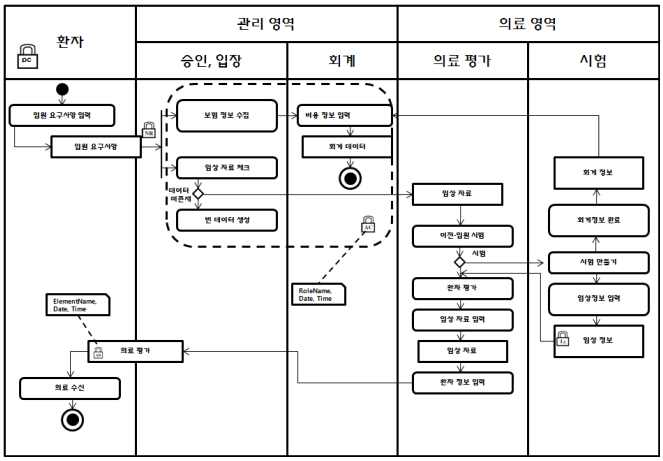
Name : SecureActivity **Base Class : Activity**	Secure Activity는 요구사항, 역할식별, 권한과 연관된 보안 명세를 포함하고 있다.	
[제약조건]	적어도 하나의 SecurityRequiment 와 연관되어 있어야 한다.	
Name : SecurityRole **Base Class : Actor** **(fromUseCase)**	역할 명세를 포함하고 있다. 이 역할은 엑세스 제어 및 개인 정보 사양에서 얻을 수 있어야 한다.	
[제약조건]	보안 역할은 stereotype의 역할에서 얻을 수 있다. : Activity, 엑세스 제어 명세서와 연관되어 있어야 하며 보안 및 보안 권한과 연관될 수 있다.	
Name : SecurityPermission **Base Class : Element** **(fromKernel)**	권한 명세서를 포함한다. 권한 명세서는 목표와 연관된 방법의 세부사항을 포함해야 한다.	
[제약조건]	보안 역할 명세서와 연관되어야 한다. 목표와 운영의 쌍을 지정해야 한다.	
Name : **SecurityRequirement** **Base Class : Element** **(fromKernel)**	보안 요구 명세서를 포함하는 추상 클래스. 각 보안 요구사항 타입은 몇가지의 하위 클래스로 표시되어야 한다.	
[제약조건]	보안 요구사항은 보안 활동과 연관되어야 한다. 표기법은 각 보안 요구사항에 대한 하위 클래 스 명세서에 완료되어야 한다. 하나의 보안 요 구사항 타입을 사용해야 한다.	**표기법**
Name	**Nonrepudiation**	**표기법**
Base Class	SecurityRequiment	
[설명]	상호작용을 필요로 하는 모든 부분을 거부하지 않도록 설정한다. 검사 요구사항은 코멘트에 에 표기될 수 있다.	
[제약조건]	표1의에 표기된 다이어그램 요소만 지정할 수 있다.	

<표 4> 보안 요구사항을 위한 스테리오 타입 명세서

Name	**AttackHarmDetection**	**표기법**
Base Class	SecurityRequiment	
[설명]	공격 손상의 시도 또는 성공이 감지되고, 등록되고 알려 지는 정도를 가리킨다. 검사 요구사항은 코멘트에 표기 될 수 있다.	
[제약]	표1의에 표기된 다이어그램 요소만 지정할 수 있다.	
Name	**Integrity**	**표기법**
Base Class	SecurityRequiment	
[설명]	계획되고 비 허가된 타락의 보호 정도를 설정한다. 요소는 고의적인 손상으로부터 보호된다. 검사 요구사항은 코멘트에 표기될 수 있다.	
[제약]	표1의에 표기된 다이어그램 요소만 지정할 수 있다. 보호 등급은 PDI 태그 값에 따라서 소문자로 추가하여 지정되어야 한다.	
Name	**Privacy**	**표기법**
Base Class	SecurityRequiment	
[설명]	허가되지 않은 민감한 정보를 얻기 위해 피하는 정도를 가리키는 정보를 가리킨다. 검사 요구사항은 코멘트에 에 표기될 수 있다.	
[제약]	표1의에 표기된 다이어그램 요소만 지정할 수 있다. 개인정보 요구사항은 하나의 보안 역할 명세서를 가지고 있다. 개인정보 타입 은 Pv 태그 값에 따라서 소문자로 추가하여 지정되어야 한다. 개인정보 타입이 기입되지 않으면 익명과 기밀로 고려된다.	
Name	**AccessControl**	**표기법**
Base Class	SecurityRequiment	
[설명]	활동다이어그램에서 특정 구성요소에 대한 엑세스 정의 및 엑세스 메커니즘(신원확인, 인증 및 권한)을 설정한 다. 검사 요구사항은 코멘트에 에 표기될 수 있다.	
[제약]	표1에 표기된 다이어그램 요소만 지정할 수 있다. 적어도 하나의 보안 역할을 지정해야만 유효하다.	

5. 예

건강관리 기관에서 전형적인 환자의 입원 비즈니스 프로세스를 설명한다. 환자, 관리 영역과 의학영역에 따라 분석 하였다.



(그림 2) 의료기관에 있는 환자의 입회

비즈니스 분석가는 안전의 몇몇의 측면을 고려했다. 그/그녀는 환자에 관하여 고도 기밀 정보의 노출 방지 목표와 더불어 활동 분할 “환자”를 위해 기밀성을 지정했다. «Nonrepudiation» 는 활동 “입원 요구사항” 행동, “보험 정보 수집” 과 “임상 자료 체크” “입원 요구사항” 가입 거부 회피의 목적으로 가는 흐름 제어에 정의되어 있다. «AccessControl»은 방해 활동 영역에 정의되어 있다. «SecurityRole» 은 명세서에 파생될 수 있다. 입원/회계 역할이 될 것이다. 방해되는 모든 목적은 권한 명세서에 반드시 고려해야 한다.(표5 참조) 이것은 역할 이름, 시간 그리고 방해 영역과 관련 있는 모든 이벤트 등록해야만 한다는 것을 의미한다. 무결성 요구사항은 “임상 정보” 데이터 저장 명세서를 가진다. 마지막으로 비즈니스 분석가는 요구사항을 감사와 함께 공격 탐지를 지정했다. 공격의 성공 혹은 손상의 시도와 관련된 모든 이벤트는 등록된다.(이름은 이 경우에 임상정보, 날짜와 시간이다.)

<표 5> «SecurityRole» 과 «SecurityPermission» 명세서

	권한		
권한	객체		연산
입원 / 회계	Action	보험정보 수집	Execution
		비용 정보 입력	CheckExecution
		임상 자료 체크	Execution
		빈 임상 데이터 생성	Execution
	DataStoreNode	Accounting Data	Update

6. 결론 및 지속적인 작업

활동 다이어그램을 통해서 비즈니스 프로세스를 표현하기 위해 개선한 UML 2.0버전은 소프트웨어 개발 초기 단계부터 시스템 보안 요구사항을 통합 기회 측면을 제공한다. 비즈니스 분석가의 풍부한 표현의 범위를 증가시킬

활동 다이어그램의 보안 요구사항을 통합하는 것을 허용하는 UML 2.0 확장을 제시했다. 다음 단계는 가장 구체적인 모델에 모델을 변환하는 MDA(Model Driven Architec ture)접근 방식을 적용하는 것이다. 따라서 미래의 작업은 적격 규칙과 OCL에 보완하기 위하여 UML 확장 명세서를 개량하는 보안 요구사항 명세서의 질을 높이는 것을 지향해야만 한다.

참고문헌

[1] Alfonso Rodríguez, Eduardo Fernández-Medina, and Mario Piattini.; Towards a UML 2.0 Extension for the Modeling of Security Requirements in Business Processes, S. Fischer-Hübner et al. (Eds.): TrustBus 2006, LNCS 4083, Springer-Verlag Berlin Heidelberg. (2006). pp. 51-61

[2] Backes, M., Pfitzmann, B. and Waider, M.; Security in Business Process Engineering, International Conference on Business Process Management. Vol. 2678, LNCS. Eindhoven, The Netherlands. (2003). pp.168-183.

[3] Bock, C.; UML 2 Activity and Action Models, Journal of Object Technology. Vol. 2 (4), July-August. (2003). pp.43-53.

[4] Bock, C.; UML 2 Activity and Action Models, Part 2: Actions, Journal of Object Technology. Vol. 2 (5), September-October. (2003). pp.41-56.

[5] Eriksson, H.-E. and Penker, M., Business Modeling with UML, OMG Press. (2001).

[6] Firesmith, D.; Engineering Security Requirements, Journal of Object Technology. Vol. 2 (1), January - February. (2003). pp.53-68.

[7] Firesmith, D.; Specifying Reusable Security Requirements, Journal of Object Technology. Vol. 3 (1), January-February. (2004). pp.61-75.

[8] Giaglis, G. M.; A Taxonomy of Business Process Modelling and Information Systems Modelling Techniques, International Journal of Flexible Manufacturing Systems. Vol. 13 (2). (2001). pp.209-228.

[9] Kalnins, A., Barzdins, J. and Celms, E.; UML Business Modeling Profile, Thirteenth International Conference on Information Systems Development, Advances in Theory, Practice and Education. Vilnius, Lithuania. (2004). pp.182-194.

[10] List, B. and Korherr, B.; A UML 2 Profile for Business Process Modelling, 1st International Work shop on BestPractices of UML (BP-UML2005) at ER-2005. Klagenfurt, Austria.(2005).

[11] Lodderstedt, T., Basin, D. and Doser, J.; SecureUML: A UML-Based Modeling Language for Model-Driven Security, UML 2002 - The Unified Modeling Language, 5th International Conference. Vol.2460. Dresden,Germany. (2002).pp.426-441.

[12] Lopez, J., Montenegro, J. A., Vivas, J. L., Okamoto, E. and Dawson, E.; Specification and design of advanced authentication and authorization services, Computer Standards & Interfaces. Vol. 27 (5). (2005). pp.467-478.

[13] Maña, A., Montenegro, J. A., Rudolph, C. and Vivas, J. L.; A business process-driven approach to security engineering, 14th. International Workshop on Database and Expert Systems Applications (DEXA). Prague, Czech Republic. (2003). pp.477-481.

[14] Maña, A., Ray, D., Sánchez, F. and Yagüe, M. I.; Integrando la Ingeniería de Seguridad en un Proceso de Ingeniería Software, VIII Reunión Española de Criptología y Seguridad de la Información, RECSI'04. Leganés, Madrid. España. (2004). pp.383-392.

[15] Mouratidis, H., Giorgini, P. and Manson, G. A.; When security meets software engineering: a case of modelling secure information systems, Information Systems. Vol. 30 (8). (2005). pp.609-629.

[16] Röhm, A. W., Herrmann, G. and Pernul, G.; A Language for Modelling Secure Business Transactions, 15th. Annual Computer Security Applications Conference . Phoenix, Arizona. (1999). pp.22-31.

[17] Roser, S. and Bauer, B.; A Categorization of Collaborative Business Process Modeling Techniques, 7th IEEE International Conference on E-Commerce Technology Workshops (CEC 2005). Munchen, Germany. (2005). pp.43-54.

[18] Stefanov, V., List, B. and Korherr, B.; Extending UML 2 Activity Diagrams with Business Intelligence Objects, 7th International Conference on Data Warehousing and Knowledge Discovery (DaWaK2005). Copenhagen, Denmark. (2005).

[19] Zuccato, A.; Holistic security requirement engineering for electronic commerce, Computers & Security. Vol. 23 (1). (2004). pp.63-76.