SOA기반 워크플로우 환경에서 DSML의 구조적 접근방법을 사용한 프라이버시 정책 모델의 통합과 검증☆

Integration and Verification of Privacy Policies Using DSML's Structural Semantics in a SOA-Based Workflow Environment

이 용 환* 얀 워너** 야노스 스테파노비치***
Yong-Hwan Lee Werner Jan Sztipanovits Janos

요 약

본 논문에서는 데이터 보호 규정에 관련된 요구사항들이나 규칙들이 소프트웨어에 잘 표현되어 있는지를 검증하기 위하여 도메인 고유의 언어인 DSML(Domain Specific Modeling Language)을 사용해 정책을 정규화 혹은 계산적 표현에 관련된 솔루션을 제시하고 있다. 모든 정책들은 공식적으로 프롤로그(Prolog) 언어 기반으로 표현된 후 DSML에 통합되며 정책검증은 요구사항 준수가 언제 평가되어야 하는지에 따라 정적 정책검증과 동적 정책검증의 두가지 정책이 존재한다.

Abstract

In order to verify that a lot of legal requirements and regulations are correctly translated into software, this paper provides a solution for formal and computable representations of rules and requirements in data protection legislations with a DSML (Domain Specific Modeling Language). All policies are formally specified through Prolog and then integrated with DSML, According to the time of policy verification, this solution has two kinds of policies: static policies, dynamic policies.

☞ keyword : 도메인 고유의 언어(DSML), 정책모델(Policy Model), 워크플로우 모델(Workflow Model), 모델 검증(Model Verification), 모델 통합(Model Integration)

1. 서 론

최근 많은 의료기관들은 서비스 품질향상, 비용절감 그리고 의료상의 실수를 제거하기 위하여 전자적인 병원 의료 레코드 시스템을 구축하고 배포하고 있으며 이와 더불어 환자 레코드 정보 정책들에 대한 의료 정보시스템들 사이의 호환성을 중요한 문제로 인식하고 있다. 하지만, 미국의 많은 의료 산업계쪽은 DICOM[1]이나 HL7[2]과 같은 확실한 의료정보 보호를 위한 표준 채용에 느리게 반응하고 있고 이는 정책의 호환성 문제를 유발할 수 있다. 이러한 제약사항들을 극복하기 위해 소프트웨어 엔지니어링 공동체에서는 상호 호환성 문제를 해결하기 위해 서비스 기반 아키텍처(SOA, Service Oriented Architecture)를 기반으로 하는 솔루션들을 제시하고 있다[3].

SOA를 기반으로 하는 솔루션들은 다양한 의료 관련 데이터 보호에 관련된 요구사항들을 잘 준수해야 하며 의료 환자 레코드 보호를 위한 보안이나 프라이버시 문제들을 확실하게 하기 위한 메카니즘들을 통합해야 한다. 예를 들면, 미국에

* 정 회 원 : Vanderbilt University 연구원
ylee@isis.vanderbilt.edu(교신저자)
** 준 회 원 : Vanderbilt University 박사과정
jwerner@isis.vanderbilt.edu
*** 정 회 원 : Vanderbilt University 교수
sztipaj@isis.vanderbilt.edu

[2009/06/10 투고 - 2009/06/19 심사 - 2009/07/03 심사완료]
☆ 이 논문 또는 저서는 2007년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원(KRF-2007-357)을 받아 수행된 연구임
☆ This work was supported by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422)

서 HIPAA (Privacy Rule of the Health Insurance Portability and Accountability Act)는 환자의 고유한 정보를 보호하기 위한 기본 레벨들을 정의하며 또한 관리적 혹은 기술적인 레벨에서 표현 되어지는 일반적인 병원의료 레코드인 EHRS (Electronic Health Records)도 가지고 있다[4]. 이러한 의료정보 시스템은 정규화적 표현들이나 메커니즘들을 제공함으로서 프라이버시 요구사항들이 개발 중인 소프트웨어에 잘 표현되어져 있는지를 검사할 수 있게 한다. 하지만, 최근의 발표된 구현들은 이러한 목표를 달성하기에는 만족스럽지 못하며 또한 기존의 전통적인 접근제어 메커니즘은 어떤 범위의 데이터 보호 요구사항들을 만족시킬 수 없다. 이를 해결하기 위해 네개의 눈 원칙(4-eyes Principle) [5], 긴급상황 시 접근제어[6], 문맥기반 접근 통제[7] 그리고 조직 기반의 접근 통제[8]과 같은 좀 더 다양한 발전된 요구사항들과 메커니즘들을 제안해 왔었다. 이런 많은 제안 솔루션 중에 UCON 접근통제 모델[9]이나 SELECT 보안 프레임워크[10, 11] 등과 같은 접근방법들은 모델 기반의 컴퓨팅 환경에 배포되어 진다는 특징이 있다. 하지만 이들 접근방법들은 의료에 관련된 워크플로우 실행들과 어떻게 이것들이 통합되어지는지에 대한 언급이 없다.

본 논문은 공통 의미론적 플랫폼을 통하여 프라이버시 요구사항들과 의료정보 시스템 워크플로우 모델들과의 통합을 위한 솔루션을 제공한다. 이들 작업은 프라이버시에 대한 기대사항과 그것들의 함축적인 의미를 표현하고 추리하기 위한 문맥적인 무결성[12], SOA 패러다임에서 복잡한 의료시스템 워크 플로우를 표현하기위한 상위 레벨의 모델링 추상화를 제공하는 모델 기반 소프트웨어 툴킷 그리고 MICIS(Model Integrated Clinical Information System) 프레임워크[14] 그리고 공통적인 의미론적 플랫폼 상에서 제약사항들을 표현하고 부과하기 위한 방법인 DSML의 구조적 의미[13]로 구성되어 진다. 본 논문에서 우리는 프라이버시 정책들에 대한 추상적인 표현들을 직접적으로 MICIS 메타모델에 통합했으며 요구사항들을 명확하게 표현하기 위해 MICIS에 설계된 워크플로우, 문서모델 그리고 추가적인 요소들은 재사용 했다. 또한 로직 기반 모델 검사를 사용해 정적 프라이버시 정책들을 모델 레벨에서 확인하고 검사할 수 있게 했으며 동적 프라이버시 정책들은 모델들로부터 생성되어진 후에 PEP에 의해 실행함으로서 정책들을 검사하고 있다.

본 논문은 다음과 같이 구성된다. 먼저 2장은 의료 시스템에서 보안이나 프라이버시와 관련된 여러가지 연구들을 제공한다. 3장은 전체 시스템 아키텍처와 모델 확인방법들의 통합에 대해 기술한다. 4장에서는 본 논문에서 제안한 해결책 내에서 의료 정보시스템의 프라이버시에 대한 여러 정책들에 대한 예제들 뿐 만 아니라 방법들에 대해서 기술한다. 마지막으로 5장에서는 제안한 솔루션의 잠재적인 응용과 미래 연구에 대해 기술한다.

2. 관련지식 및 연구

본장에서는 전자적인 의료시스템 환경에서 프라이버시나 보안 요구사항들을 추출하고 실행하기 위한 기존의 해결책들의 적용 가능성에 대해 검토한다. 먼저 접근제어 모델들에 대한 좀 더 자세한 평가나 분석들은 다음 논문들[6,7,8,11,15,16,17,18,20]을 참조하면 된다. 하지만, 이들 접근 방법들은 제안된 접근제어 모델들과의 통합에 대해서는 확실한 접근방법이 없다. 모델 기반 관점에서 모델기반 보안을 위한 SELECT 프레임워크[21]은 조직간의 안전한 워크플로우를 모델링하고 배포하기 위한 하나의 플랫폼이다. 이 프레임워크에서 모델링은 UML기반의 도메인 고유 언어를 통해 지원되며 보안 요구사항은 서술적인 OCL기반 언어를 통해 표현된다. 이 SELECT 툴은 최근에 UCON 보안모델[9]을 지원하기 위해 확장 되었으며 최근에는 안전한 워크플로우를 위한 모델링과 배포를 위한 프레임워크를 제공하

고 있다.

워크 플로우와 프라이버시 요구사항들을 명세하기 위한 이론적인 프레임워크는 최근에 Barth [13]에 의해 제기되었다. 이 프레임워크는 통신표준을 추론화하고 기술하기 위해 임시 로직을 사용함으로서 문맥적 무결성이라는 개념들을 정규화했다. 이들 접근 방식은 의미 있는 검증 방법들을 제공하고 있지만 워크플로우 기술적 측면에서 실제적인 복잡한 의료 환경이나 의료 정보시스템 구현 안에서 적용하는데 있어 많은 제약사항들이 존재한다.

MICIS[14]는 실험적인 의료정보 시스템을 빠르게 개발하기 위한 프레임워크로서 이 프레임워크에서는 도메인 고유의 모델링 언어 DSML을 사용해 워크플로우, 문서, 구조 그리고 의료환경에 맞게 변경된 정책 모델들을 개발할 수 있다.이들 모델들은 서비스 기술, BPEL 워크플로우, 배포 기술 그리고 정책기술들과 같은 실행 가능한 것들로 변경된다. MICIS DSML을 사용하는데 DSML은 소프트웨어를 설계하고 개발하는 소프트웨어 엔지니어링 방법 중의 하나로서 각 도메인별 고유한 개념들, 개념간의 구조 그리고 제약사항들을 메타모델링 언어로 명시하며 이를 기반으로 도메인별 모델링 인스턴스를 생성하며 이를 기반으로 소프트웨어를 개발하는 것이다. DSML을 사용할 경우 장점은 일반적인 목적의 모델링 언어보다 상위레벨에서 추상화 시킬 수 있으며 훨씬 적은 노력으로 시스템을 명세할 수 있다는 것이다. 본 논문은 프라이버시 요구사항의 정확한 표현과 모델 표현에 대한 확인 절차를 통해 MICIS를 확장하고 있다.

3. 워크플로우 모델과 정책모델의 통합

3.1 구조적 의미(Structural Semantics)

모델링에서 구조적 의미라는 것은 DSML[15]의 구조적 의미를 정규화 하기 위한 접근방법 중의 하나로서 본 논문에서는 메타 모델링 기법을 사용해 한 도메인의 구성요소들, 구조 그리고 도메인 제약사항들을 기술하며 메타 모델 해석을 통해 도메인의 여러 가지 제약사항들이 메타모델의 인스턴스인 모델에 주입되게 된다. 따라서 추가적인 요구사항들은 해당 메타모델을 다시 해석함으로서 언제든지 모델에 다시 반영할 수 있다. 메타 모델 해석기는 MICIS 모델 플랫폼의 구성요소 중의 하나인 GME모델링 툴킷[22]에서 제공된다. 메타 모델의 인스턴스인 모델은 일련의 용어 집합으로 변역되며 해당 모델의 올바름을 증명하기 위해 메타모델을 통해 정의된 도메인 제약사항들을 사용해 모델의 용어 집합을 검증한다. 구조적 의미에 대한 정의를 위해 본 논문에서는 Jackson논문[23]에서 사용한 표기법들과 정의들을 사용하며 풍부한 문법을 가지고 있는 DSML를 사용해 도메인을 정규화 형태로 정의한다. 모델링 산출물의 가변성이나 구조를 표현하기 위해서 본 논문에서는 확장된 혼로직을 이용한다.

본 논문에서는 사용하는 표기는 어떤 의미를 지니는데 표기 f(•)의 의미는 한가지 등식이외에 다른 추가적인 등식이 만족되지 않는 어떤 전체집합 U에 대한 단항함수(Uniary Function)이며 기호 Σ는 영어 알파벳을 원소로 해서 구성되어지는 무한 알파벳 상수(Infinite Alphabet Constant)라고 하자. 이러한 전제하에서 앞에서 언급한 모델상의 하나의 용어(Term)는 Σ으로부터 뽑아진 하나의 상수이거나 혹은 알파벳이나 다른 용어들을 매개변수 가지는 즉, 임의의 차수(Arbitrary Arity)를 가지는 해석되지 않는(Uninterpreted) 단항 함수f(•)를 적용한 결과이다. 시그니처(Signature) Y는 n차항 함수 (N-ary Function) 심볼 집합이며 용어 대수학(Term Algebra)인 TY(Σ)는 앞의 함수 시그니처상의 모든 상징(Symbol)들이 해석되지 않는 대수학으로서 여기에서 함수라는 것은 공통 이미지가 없는 즉, 중복 매핑이 없는 일대일 형태의 매핑으로서 이 함수들이 모든 용어들에 적용될 수 있다. 문법적 규칙들은 용어 대수 TY(Σ) 상에서 정의된 혼구문들을 사용하여 추

출 된다. 혼구문은 다음 (h, T)과 같은 쌍으로 표현되면 헤더 h는 어떤 변수들을 가진 하나의 용어이며 테일 T는 변수들을 가진 용어집합이다. 혼구문상의 시멘틱은 용어 집합 T상에서 구문 집합 Θ를 평가함으로서 얻어진다. 구문 집합Θ를 평가하는 방법은 각 구문에 대하여 테일 T에 있는 변수들을 T의 용어들과 매칭시켜서 만일 올바른 대치가 존재한다면 헤더상의 용어 h가 일련의 용어 집합에 포함된다.

앞에서 설명한 구성요소들을 가지고 본 논문에서는 공식적으로 도메인을 다음과 같은 구조 D = {Y, Σ, Θ} 로 정의하며 두개의 불변식 malform(•) 혹은 wellform(•)을 사용해 잘 정의된 혹은 잘못 정의된 도메인 실현에 대한 명세를 할수 있게 한다. 예를 들면 어떤 wellform(•) 용어가 도메인 실현으로부터 파생된다면 이 도메인 실현은 잘 정의된 것이며 비슷하게 어떠한 malform(•) 용어도 모델 실현으로부터 파생되지 않는다면 하나의 모델 인스턴스는 마찬가지로 잘 정의된 것이다. 다시 말해 도메인 모델의 올바름을 확인하기 위해 긍정적 방식 혹은 부정적 방식의 두가지 개념들을 사용하는데 긍정적 방식에서는 도메인 실현 모델에 대해 wellform(•) 용어가 파생되면 도메인 모델 실현 모델이 올바른 것이며 비슷하게 부정적 방식에서는 malform(•) 용어가 파생되지 않으면 도메인 실현 모델이 올바른 것이다.

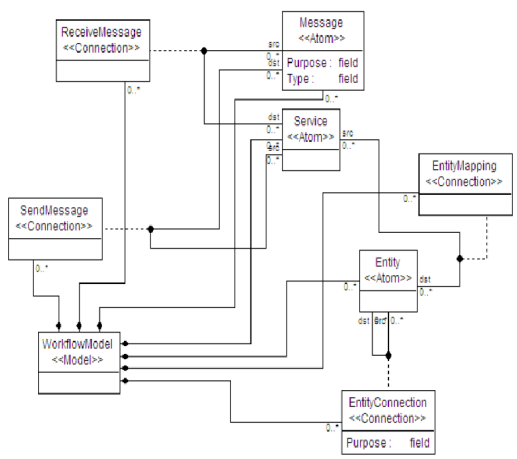
3.2 모델링 시점의 프라이버시 정책통합

모델링 시점의 프라이버시 정책통합

프라이버시 정책 제약 사항들을 가지고 SOA 기반의 워크플로우 메타모델을 어떻게 정의 하는가에 대해서 설명한다. SOA는 모델 추상화를 매핑하거나 조직간 워크플로우를 구축하기 위한 여러가지 풍부한 기본적인 것들을 제공한다. 모델링 언어들에는 서비스, 메시지, 통제 그리고 데이터 흐름 등과 같은 많은 SOA 구성요소를 반영하도록 구성되어지며 프라이버시 정책들을 표현하기 위하여 메시지 타입, 통신 목적 그리고 서비스에 관련된 당사자들 사이에 관계등을 매핑시키는 추상화 기법을 통해 모델링 언어가 확장된다. 아주 간단한 워크플로우 언어에 대한 메타모델은 그림1에 묘사되어 있다.

그림1의 메타모델에 따르면 Service 들은 SendMessage와 ReceiveMessage를 통해 Message들과 연결된다. EntityMapping을 통해 Service들은 Entity들과 연결되며 Entity들간의 연결은 EntityConnection을 사용한다. 각 Message는 타입과 목적과 같은 두개의 속성을 가진다. 그림 1의 모델링 언어는 잘 정의된 규칙을 사용해 표현된 프라이버시 제약사항들을 포함하기 위한 하나의 프레임이다. 본 논문에서 우리는 풍부한 언어상의 문법들을 표현하기 위하여 구조적 의미의 접근방법들을 사용해 프라이버시 정책들을 표현하고, 확인하며 그리고 실행한다. 다음은 그림1의 메타모델 구성요소들을 시그니처를 사용해서 인코딩한 것이다.

Y = {workflowModel(•),sendMessage(•,•),
receiveMessage(•,•),service(•,•),
message(•),type(•,•),purpose(•,•),
entityMapping(•,•),entityConnection(•,•),
entity(•), type(•,•), purpose(•,•) }



(그림 1) 워크플로우 추상화를 기술하고 있는 간단한 워크플로우 메타모델

프라이버시 정책들을 확인하고 실행하기 위하여 본 논문에서는 워크플로우를 부정적 도메인 검증 방식을 사용해서 검사한다. 여기서 부정적 도메인 방식의 검사라는 것은 어떤 정책의 위반이 발견된 경우에 그 모델을 무효화하는 것을 말한다. 여기에서 정책들은 언어의 문법적 제약사항들을 표시하는 malform(•) 용어집합 형태로 표현된다. 본 논문에서는 구문 규칙에 맞지 않는 규칙을 의미하는 malform(•)을 혼구문 규칙을 사용해 표현한다. 다음 예제는 모델에 Message가 없고 Message가 Service로부터 나온것이 아니라면 이 모델은 구문 규칙에 맞지 않다라는 것을 나타내는 아주 간단한 2개의 예제이다.

```
malform(message(X)):- ₩+ message(X).
malform(message(X)):- message(X),
                      ₩+ sendMessage(Y,X)
```

그림1에 표현된 워크플로우 메타 모델을 기반으로 모델 인스턴스를 생성할 수 있다. 이 모델들은 다음 용어집합을 사용해 인코딩 된다.

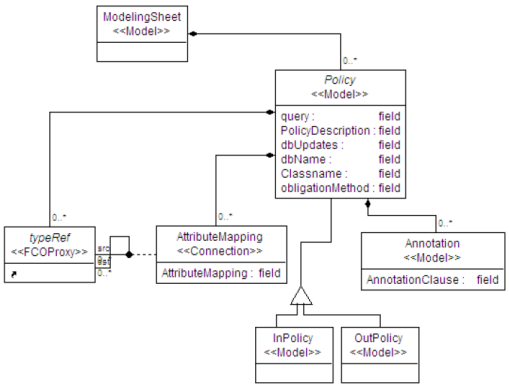
M = {service(Data Provider), service(De-Identification), message(Message), type(PHI record, phi), purpose(PHI record, de-identification), entity(CoveredEntityentity(Business Associate), sendMessage(sm1, Data Provider, PHI record), receiveMessage(rm1, PHI record, De-Identification engine), entityMapping(em1, Data Provider, Covered Entity), entityMapping(em2, De-Identification engine, Business Associate), entityConnection(ec1, Business Associate, Covered Entity) }

이들 용어집합들은 모델의 구조를 나타내고 프라이버시 정책 검증을 위한 기본적인 사항들이다. 이들 모델의 구문 규칙 적합성과 프라이버시 정책들을 잘 준수하고 있는지를 증명하기 위해서는 이 도메인을 위해 정의된 malform(•) 용어가 일련의 용어집합 M으로부터 파생 되어서는 안된다. 이 모델에 부과된 일련의 제약 사항 집합은 워크플로우 이용성과 프라이버시를 보장해야 하는데 유용성에 대한 표현 예는 “Message는 올바른 시작점에서 시작해 올바른 도착점으로 보내져야 한다”와 같으며 프라이버시 보장에 대한 예제는 “Messasge는 인가되지 않는 대상에 도달될 수 없다” 와 같다. 위의 예제에서 하나의 워크플로우가 유용성 목표를 달성하고는 있으나 프라이버시 목표를 달성하지 못하고 있다라는 것을 증명할 수 있다. 예를 들면 다음 표현 “하나의 Message가 데이터 제공자에서 데이터 수신자로 전송되었지만 데이터 수신자가 어떤 메시지를 받아서는 안된다” 은 유용성은 달성되었지만 프라이버시가 달성되지 못하는 모델이라는 것을 증명할 수 있다. 이와 비슷하게 프라이버시 요구사항을 만족하고 있지만 유용성 목표를 달성하지 못하는 모델도 구축할 수 있다. 프라이버시 요구사항을 가진 비즈니스 로직을 통합하는 것은 앞에서 언급한 두 개의 목표를 분석하게 할뿐만 아니라 동시에 올바른 모델을 구축할 수 있게 한다.

3.3 실행시점의 프라이버시 정책통합실행

프라이버시 정책들은 많은 경우에 어떤 메시지의 구체적인 내용에 의존하는 경우가 많다. 따라서 이런 정책들을 실행하기 위해서는 메시지 인스턴스를 분석해야 하는데 이러한 분석은 모델링 단계동안에는 수행할 수 없다. 런타임에 평가되는 정책들을 실행하고 표현하기 위한 문제점들을 해결하기 위해 정책문서들을 생성하기 위한 추상성을 가지고 우리는 과거 우리연구[14]의 워크플로우 모델링 언어의 문법을 확장했다. 런타임 시간에 이들 정책들을 실행하기 위하여 우리는 Axis2의 웹서비스 컨터이너 위에 정책실행을 위한 확장플랫폼을 구축했다. 본 논문에서 제공한 해결책은 메시지들의 내용이나 워크플로우 실행에 대한 과거이력을 사용해 정책들을 평가할 수

있게 하며 더욱이 정책상의 추가적인 컨디션들이 정책안에 정의된 의무를 기반으로 서버 측에서 실행될 수 있다. 정책안의 의무는 정책 결정상에서 실행되는 추가적인 행위들을 정의하며 워크플로우나 문서모델과 관련된 정책 언어는 혼로직을 사용해 정책들을 표현하며 또한 교환되는 메시지들을 서로 관련시킬 수 있게 한다. 메타 모델를 통해 정의된 정책 모델은 그림2에 표현되어 있다.

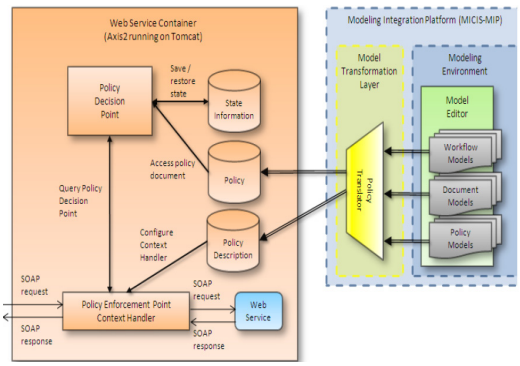


(그림 2) MICIS 모델링 언어와 함께 통합된 프라이버시 정책 구조에 대한 메타모델

그림2에서 모델에는 Annotation 변수 안에 정책문서들을, AttributeMappings를 사용해 typeRef라는 문서모델 구성요소 사이의 관계를 그리고 PEP 설정 정보도 저장하고 있다. Annotation 변수 안에 정의된 정책들은 프롤로그 규칙형태로 표현된다.

이런 접근방법은 풍부한 룰 기반의 정책들을 구축할 수 있게 하지만 정책 구현자에게서 프롤로그 문법에 대한 지식을 요구하게 된다. 통과하는 메시지의 필요한 정보를 추출하기 위해 PEP 설정을 위한 문서 모델로부터 변수들이 사용되어지며 정책 평가를 위해 PDP에게 추출된 이 정보를 제공한다. 추가적인 옵션들은 정책 실행 시점(예를 들면, 들어오는 메시지 혹은 나가는 메시지), 워크플로우 실행이력 정보 그리고 의무사항들을 명세하게 한다. 정책 번역기는 워크플로우, 문서 그리고 정책 모델들로부터 XML과 같은 정책문서 그리고 정책 기술을 생성한다.

생성된 정책기술들과 더불어 정책문서들은 보호되고 있는 서비스를 가지고 있는 웹서비스 컨테이너에 배포되며 이들 배포 아키텍처는 웹서비스 프로토콜이나 표준을 기반으로 하고 있다. 그림3은 모델링 환경에 대한 아키텍처 확장과 그 원소들 사이의 관계들에 대한 세부적인 것들을 표현하고 있다.



(그림 3) 정책 모델링과 실행을 위한 시스템 아키텍처

워크플로우 로직을 구현한 웹서비스들은 모든 들어오며 나가는 SOAP 메시지를 가로채는 Context Handler를 사용해 보호된다. PEP는 웹서비스 보안계층 위에 존재하며 기밀성, 무결성 그리고 이용성과 같은 기본적인 보안요구사항들을 처리한다. Context Handler는 첫 번째 서비스 호출을 가로챈 후에 메시지를 어떻게 처리할 것인지를 지시하는 정책표현을 올린다. 들어오는 메시지에 대해 정책이 적용되어야 하고 상태가 저장되어 있다면 PEP는 그 저장된 상태를 복구하고 정책문서를 올려서 접근 요청을 평가한다. PDP로부터 결정을 기반으로 PEP는 의무를 실행하고 호출을 서비스에게 넘겨준다. 만일 접근제어가 PDP에 의해 거부된다면 해당 메시지를 버린다. 비슷한 절차가 서비스 응답을 위해서도 실행되는데 나가는 메시지를 위해 PDP는 SOAP의 요청과 응답 모두에 접근해서 서비스에서 제공되는 결과들을 기반으로 결정을 한다.

4. HIPPA 프라이버시 정책모델 검증 예제

4.1 모델링 단계에서 시나리오의 규칙준수: 비즈니스 관계를 통한 신분확인

여기에 예로든 정책들은 미국의 HIPAA(Health Insurance Portability and Accountability)의 섹션 160.45.2.d에서 나온 것으로서 환자의 건강정보에 대한 사용과 정보공개 정책의 컨디션들을 표현하고 있다.

"대화 당사지들 사이에 계약적인 협약이 존재하는 경우에 한하여 보호되어야 할 대상 은 신분확인 목적을 위해 환자의 건강정보를 비즈니스 파트너에게 전달한다"

앞의 그림2에 표현된 모델은 이런 규칙의 요구사항을 만족하는 통신 인스턴스를 표현한 것이다. 보호받아야 할 대상자에 속하는 의료 레코드 데이터베이스는 메시지의 목적과 타입을 기술하는 속성을 가진 PHI(Protected Health Information) 레코드를 포함하고 있는 메시지를 비지니스 파트너의 신분확인 엔진에게 전송한다. 보호받아야 할 대상과 비즈니스 파트너 사이에는 대상 관계가 존재하며 이는 두 당사자 사이의 기존 관계를 표현하고 있다. 워크 플로우 모델은 부정적 도메인 형태로 표현되기 때문에 프라이버시 정책을 가지고 모델링된 시스템의 규칙준수를 증명하기 위해서는 malform(•) 규칙을 만들어지는 것이 불가능해야 한다. 프라이버시 정책은 혼구문 형태로 기술 되는데 다음과 같이 잘못 형성된 규칙 형태로 기술되어 진다.

no-connection (E1, E2) : \+ entityConnection(X,E1, E2)
malform(message(M)) :- message(M), sendMessage(MF, S1, M), receiveMessage(MF2, M, S2), entityMapping(EM1, S1, S2), entityMapping(EM2, S2, E2), type(M,'phi'), no_connection(E1, E2).

잘못 형성된 구문을 만들어 내기 위하여 정책 표현의 말미 부분에 있는 모든 용어들이 일단 만족되어야 한다. 이 모델은 일단 'phi'와 같은 속성 타입을 가진 메시지를 가지고 두개의 서비스(S1과 S2)들을 연결할 필요가 있다. 여기서 'phi' 와 같은 속성은 메시지에 보호해야 할 의료정보가 있으며 통신 서비스를 포함하고 있는 대상들(E1과 E2)이 연결되지 않았다는 것을 의미한다. 앞의 예제에서 제약사항, no-connection은 혼로직 확장으로서 정책에 대한 부정적 방식의 표현예제이다. 이들 제약 사항은 규칙 no-connection(X, E1, E2)안에 있는 변수 X, E1 그리고 E2를 대체될 수 있는 어떤 용어가 존재하지 않을 때에만 만족된다. 다시 말해, 통신 당사자들이 공식적인 비즈니스 관계를 형성하지 않는다면 시스템은 워크플로우 모델을 무효화 할 수 있다. 모델에 대한 이런 확인 절차는 malform(•) 용어가 파생될 수 없고 따라서 이 모델은 프라이버시 정책을 준수한 것으로 분류될 수 있음을 증명한다.

4.2 런타임 단계에서 규칙 준수 확인성 : Break- Glass

다음 예제는 "Break Glass"라는 정책을 사용해 실행시점의 정책 확인 방법에 대해 설명한다."환자 의료 기록에 대한 접근은 의료기록에 나열되어 있는 주치의 에게만 허용되어야 하거나 혹은 긴급 상황의 경우에는 다음의 "Break Glass" 정책에 따라 어떤 의사들에게만 제공되어야한다"

이들 정책은 "Break Glass"[20] 정책 응용을 위해 임의의 컨디션들 뿐 만 아니라 환자와 의사 들 사이에 관계를 기술하기 위한 세세한 접근제어(Fine-Grained Access Control)를 요구하며 이들 정책들은 SOA용어들을 사용해 표현된다. 그림5의 예제에서 RetrieveData 서비스는 다음 두 가지 중의 하나인 경우에 한하여 요청자에게 의료정보를 전송한다. 첫 번째는 서비스 요청이 긴급상황에서 발생한 경우이고 두 번째는 서비스 요청 메시지 내부에 의사들의 비밀정보를 가지고 있는 의사

리스트를 포함하고 있는 경우이다. 추가적으로, "Break Glass"정책을 사용해 서비스 요청이 허용된다면 PEP는 관리적인 검토목적을 위해 규칙상의 의무 형태로 수행되는 감사추적을 생성한다. 그림5는 의료 레코드를 제공하는 워크플로우 형태의 서비스 모델을 구축하고 그 서비스에 대한 접근제어를 통제하는 프라이버시 정책을 기술하고 통합하는 예시이다. 통합모델은 모델 번역기를 사용해 아래에 나열된 정책기술과 PEP를 위한 설정정보와 같은 문서들의 쌍으로 변환된다. 다음은 통합 모델로부터 모델 변역기를 통해 생성된 XML기반 정책기술 내용이다.

```
<PolicyList>
  <PolicyDescription>
    <methodName> RetrieveData </methodName>
  <query> retrievedata(MRN,DocID) </query>
<policyDbName> 'c:/Policy/factsdb.pl' </policyDbName>
  <inPolicy> False </inPolicy>
  <outPolicy> True </outPolicy>
  <requestFields>MRN, critical
  </requestFields>
  <replyFields> DocID</replyFields>
  <relations> is_critical(MRN,critical), treats(MRN, PCP)
  </relations>
  <dbUpdates> accessed(DocID, MRN) </dbUpdates>
    <classname>
        edu.vanderbilt.isis.bepltools.logCriticalAccess
  </classname>
  <obligationMethod>obligationmethod
   </obligationMethod>
  </PolicyDescription>
</PolicyList>
```

다음은 정책문서에 대한 예제이다.

```
%% definition of helper symbols
 :- dynamic treats/2.
:-dynamic critical/2.
%% access rule
:-dynamic retrievedata/2
%%define break glass rule allow access in emergency context.
break_glass(RecordNo):-is_critical(RecordNo, X), X > 0.
%%access control rules for the record
%%only physicians who treats the patient can access his record
%%access is provided if patient is marked as in critical state
retrievedata(RecordNo, DocID):- treats(RecordNo, DocID): break_glass(RecordNo).
```

프롤로그 규칙들 형태에서 긍정적인 정책 허용뿐만 아니라 특별한 컨디션들에 대해 접근을 거절하는 부정적 정책을 사용할 수 있으며 또한, 임의의 정책조합을 허용하며 정책들 사이의 가능한 충돌을 해결하기 위해 다수의 전략들을 사용할 수도 있다. 여기 예제에 표현된 정책들은 긍정적인 허용을 사용하는 것으로서 질의 retrievedata(MRN, DocID)가 추론될 수 있다면 접근은 허용된다. 이 retrievedata 추론을 위한 정책조건들로 환자를 치료하는 의사만이 레코드를 접근할 수 있거나 혹은 환자상태가 긴급 상황일 때에는 지정된 의사에게만 접근이 허용된다.

5. 결론 및 향후 연구

본 논문에서 우리는 어떤 공통적 의미상의 플랫폼(Common Semantic Platform)을 통해 프라이버시 정책들의 논리적인 표현과 워크플로우 모델들을 어떻게 통합하는지에 대해 제안했다. 우리는 본 논문에서 설명한 프레임워크내에서 프라이버시 요구사항들을 공식화하고 확인하기 위하여 어떻게 구조적 의미의 접근방법을 적용하는지에 대해 설명했다. 의료정보 시스템을 개발하기 위하여 우리는 기존에 연구했던 도메인 고유의 모델이 통합되어 있는 프레임워크 인, MICIS 시스템을 사용해 모델들이 프라이버시 규정들을 잘 준수하고 있는지를 확인하기 위한 방법을 제시했다.

이를 위해 특별한 잘 알려진 규제 요구사항에 대한 몇개의 예제를 통해 이 접근 방법을 어떻게 적용하는지에 대한 예시도 제시했다. 우리는 실행시에 프라이버시 정책들의 실행을 가능하게 하는 서비스 기반 아키텍처 플랫폼에 대한 확장을 제공했다. 최근에 우리는 구조적 의미의 접근방법을 사용하여 실행되고 표현될 수 있는 HIPAA 규칙들을 분류하는 작업을 했으며 미래에는 대규모 분산 환경에서 적용 가능성과 실행시점의 정책 실행에 의해서 나타나는 과부하에 대해 평가할 계획이다. 또한 요구사항이나 정책들의 명세를 통하여 의료 워크플로우 모델들을 통합하는 모델 생성을 위한 툴을 개발할 것이다.

참 고 문 헌

[1] Digital Imaging and Communications in Medicine Standard. ftp://medical.nema.org/medical/dicom/2008/

[2] Health Level Seven Standard. http://www.hl7.org/

[3] Vogl, R., Breu, M., Schabetsberger, T., Wurz, M.: Architecture for a distributed national electronic health record in Austria aiming at an open source solution. In Proc. 24th International EuroPACS Conference EuroPACS 2006, pp. 67-77, 2006.

[4] Health Insurance Portability and Accountability Act http://www.hhs.gov/ocr/hipaa/

[5] Vogt, G.: Multiple authorization - a model and architecture for increased, practical security. In Proc. IFIP/IEEE Eighth International Symposium on Integrated Network Management (IM2003), Colorado Springs, CO, IFIP/IEEE, Kluwer Academic Publishers, pp. 109-112, 2003.

[6] Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC). breakglass – an approach to granting emergency access to healthcare systems. http://www.nema.org/prod/med/security/.

[7] Tzelepi, S.K., Koukopoulos, D.K., Pangalos, G.: A flexible content and context-based access control model for multimedia medical image database systems. In Proc. 2001 Workshop on Multimedia and Security: New Challenges,2001.

[8] Kalam, A.A.E., Baida, R.E., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miege, A., Saurel, C., Trouessin, G.: Organization based access control. In: Proc. IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2003), pp. 120-131, 2003.

[9] Park, J., Sandhu, R..: Towards usage control models: beyond traditional access control. In: Proc. 7th ACM symposium on Access control models and technologies (SACMAT "02), ACM Press, New York, NY pp.57 – 64, 2002.

[10] Hafner, M., Agreiter, B., Breu, R., Nowak, A.: SECTET: an extensible framework for the realization of secure inter-organizational workflows. Journal of Internet Research, 2006.

[11] Alam, M., Hafner, M., Memon, M., Hung, P.: Modeling and enforcing advanced access control policies in healthcare systems with SECTET. In: Proc. ACM/IEEE Workshop on Model-Based Design of Trustworthy Health Informaton Systems, 2007.

[12] Barth, A., Datta, A., Mitchell, J.C., Nissenbaum, H.: Privacy and contextual integrity: framework and applications. In: Proc. 2006 IEEE Symposium on Security and Privacy, 2006.

[13] Jackson, E.K., Sztipanovits, J.: Towards a formal foundation for domain specific modeling languages. In: Proc. 6th ACM International Conference on Embedded Software (EMSOFT"06), Seoul, South Korea, 2006.

[14] Mathe, J., Werner, J., Lee, Y., Malin, B., Ledeczi, A.: Model-based design of clinical information systems. Methods of Information in Medicine, pp.399-408, 2008.

[15] Ferraiolo, D., Kuhn, D.R., Hu, V.C.: Assessment of access control systems. Technical Report NISTIR 7316, National Institute of Standards and Technology, US Department of Commerce , 2006

[16] National Institute of Standards and Technology. Role Based Access Control. http://csrc.nist.gov/groups/SNS/rbac/

[17] Mavridis, I., Pangalos, G., Khair, M.: eMEDAC: Role-based access control supporting discretionary and mandatory features. In: Proc. IFIP Workshop on Database Security, pp. 63-78, 1999.

[18] Beznosov, K.: Requirements for access control: US Healthcare domain. In: Proc. 3rd ACM Workshop on Role-Based Access Control, Fairfax, Virginia, 1998.

[19] Hu, J., Weaver, A.C.: Dynamic, context-aware access control for distributed healthcare applications. In: Proc. Pervasive Security, Privacy, and Trust Workshop , 2004.

[20] Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC). breakglass – an approach to granting emergency access to healthcare systems. http://www.nema.org/prod/med/security/

[21] Hafner, M., Agreiter, B., Breu, R., Nowak, A.: SECTET: an extensible framework for the realization of secure inter-organizational workflows. Journal of Internet Research Vol.16, Issue5, pp.491-506, 2006.

[22] K. Balasubramanian, A. Gokhale, G. Karsai, J. Sztipanovits, and S. Neema: Developing applications using model-driven design environments, IEEE Computer, vol. 33, no. 2, pp. 33-40, Feb 2006.

[23] Jackson, E., Schulte, W., Sztipanovits, J.: The power of rich syntax for model-based development. Technical Report MSR-TR-2008-86, Microsoft Research, Redmond, WA, 2008.

◐ 저 자 소 개 ◑

이 용 환

1997 Konkuk University, Korea, BS in Public Administration
1999 Konkuk University, Korea, MS in School of Computer Science and Engineering, College of Information and Telecommunication
2006 Konkuk University, Korea, Ph.D. in School of Computer Science and Engineering, College of Information and Telecommunication
Research Interests: Model-Integrated Computing, Distributed System, SOA, Workflow Model
E-mail : ylee@isis.vanderbilt.edu

Jan Werner

2000-2005 M. SC Computer Sciences Nicolaus Copernicus University Torun
2002-2005 Bachelor Applied Physics Nicolaus Copernicus University Torun
2007～Current ISIS, Department of Electrical Engineering and Computer Science, Vanderbilt University, USA, Graduate Student in Ph.D. course
Research Interests: Policy Model, Model-Integrated Computing, SOA
E-mail : jwerner@isis.vanderbilt.e

Janos Sztipanovits

1970 Technical Univ Of Budapest Diploma Electrical Engineering.
1980 Hungarian Academy of Sciences, CSc. Electrical Engineering
1980 Technical Univ Of Budapest, Ph.D. Electrical Engineering
2007～Current ISIS, Department of Electrical Engineering and Computer Science, Vanderbilt University, USA, E. Bronson Ingram Distinguished Professor of Engineering
Research Interests : Model-Integrated Computing, Embedded Software, Structurally adaptive systems
E-mail : sztipaj@isis.vanderbilt.edu