사용목적 분류화를 통한 프라이버시 보호를 위한 보안 접근제어 모델*

나석현° 박석
서강대학교
{shna°, spark}@sogang.ac.kr

A Secure Access Control Model for Privacy Protection using Purpose Classification

Seokhyun Na°, Seog Park
Sogang University

요 약

사용목적(Purpose)은 최근 개인 프라이버시 보호와 관련하여 데이타 수집과 수집 후 보안관리에 있어서 중요한 요소로 사용되고 있다. W3C(World Wide Web Consortium)는 데이타 제공자가 자신이 방문한 웹 사이트에 개인정보를 제공하는 것을 통제할 수 있도록 하는 표준을 제시하였다. 그러나 데이타 수집 후 유통과정에서 개인정보에 대한 보안관리에 대한 언급이 없다. 현재 히포크라테스 데이타베이스(Hippocratic Databases), 사용목적기반 접근제어(Purpose Based Access Control)등은 W3C의 데이타 수집 메커니즘을 따르고 있으며, 데이타 수집 후 보안관리에 대하여 사용목적 관리와 접근제어 기법을 사용하여 관리를 하고 있으나 사용목적에 대한 표현과 사용목적 관리의 미흡함으로 인하여 그에 따르는 개인정보의 프라이버시 보호에 있어서 효과적인 해결책을 제시하지 못하고 있다.

본 논문은 사용목적의 표현력을 향상시키면서, 사용목적의 효과적인 관리기법을 제시한다. 또한 개인의 프라이버시 보호를 위한 방법으로 사용목적의 분류화를 통해 최소권한의 원칙을 따르는 접근제어 기법을 제시한다. 본 논문에서는 사용목적을 상속적, 시간적 그리고 독립적 구조로 분류화하였으며, 이렇게 분류화된 사용목적에 대한 각기 다른 관리기법을 제시한다. 또한 접근제어의 유연성을 위해 RBAC의 역할계층 구조를 사용하였으며, 일의 최소 단위인 태스크(task)의 최소권한을 얻기 위한 조건으로 몇몇 특성의 사용목적을 사용하여 만족할 경우 태스크를 처리하기 위한 기존 모델보다 향상된 최소사용권한을 제공하는 기법을 제시한다.

1. 서 론

최근 들어 사적인 데이타가 인터넷을 통하여 데이타베이스에 점점 더 많이 저장되고 있으며, 이렇게 저장된 사적인 데이타가 개인과 기업 그리고 기업들 간에 유통이 됨으로써 인해 개인 프라이버시(privacy)의 민감한 문제로 대두되고 있다.

현재 개인의 프라이버시 보호와 관련하여 많은 관심을 가지고 활발한 연구가 수행되어 지고 있으며, 그 예로 W3C에 의해 표준으로 제안되어진 P3P(Platform for Privacy Preference)[1]와 IBM에 의해 제안되어진 EPAL(Enterprise Privacy Authorization Language)[2]이 있다.

그러나 P3P와 EPAL은 데이타의 수집과 사용방법을 제시하였으나, 데이타 수집 후 유통과정에서 보안관리에 대한 언급이 없다. IBM의 히포크라테스 데이타베이스(Hippocratic Databases)[3]는 P3P와 EPAL의 데이타 수집 메카니즘을 이용하며 또한 보안관리기법을 적용한 것이다. 그 이외에 Purdue University의 사용목적기반 접근제어(Purpose Based Access Control)[4], 이재길의 히포크라테스 XML 데이타베이스(Hippocratic XML Databases)[5]등이 연구되고 있으며, 이들 연구는 데이타 수집 후 보안관리에 대해 사용목적과 그에 따른 접근제어를 통하여 이루어진다. 그러나 이들 연구에서 제시하는 사용목적의 관리는 사용목적 특성에 따르는 표현력의 부족으로 인하여 관리에 어려움이 있으며, 이로 인해 개인정보 제공에 대한 최소권한의 원칙을 만족하지 못한다.

본 논문에서는 사용목적을 다각적인 면에서의 분석을 통하여 상속적, 시간적 그리고 독립적 구조로 분류화하였으며, 이렇게 분류화된 사용목적들에 대한 접근제어 기법을 제시한다. 또한 접근제어의 유연성을 위해 RBAC의 역할계층 구조를 사용하였으며, 일의 단위인 태스크의 최소권한을 얻기 위한 조건으로 위에서 언급된 몇몇 특성의 사용목적을 사용하여 만족할 경우 태스크를 처리하기 위한 기존 모델보다 향상된 최소의 사용권한을 제공하는 기법을 제시한다.

* 본 연구는 정보통신부 정보통신연구진흥원에서 지원하고 있는 정보통신기초기술연구 지원사업(B1220-0501-0050)의 연구 결과의 일부임.

2. 관련연구 및 문제점

2.1 사용목적관리 측면

사용목적기반 접근제어와 히포크라테스 XML 데이타베이스 모델은 사용목적을 각각 내포관계의 특성을 고려한 하나의 내포관계 특성과 DGA 계층구조 형식을 고려한 하나의 사용목적 트리 형식으로 분류·관리 한다. 그러나 이 두 가지 모델의 사용목적 계층구조 관리 방식으로 사용목적을 관리할 경우, 위에서 언급한 사용목적의 특성 그리고 계층구조의 특성인 최상위 노드를 제외한 모든 노드들은 부모 노드를 가져야 한다는 제약 사항으로 인하여 사용목적의 표현력 부족과 사용목적의 삽입·삭제시 사용목적 관리의 미흡함이라는 문제점이 발생한다.

2.2 접근제어측면

사용목적기반 접근제어와 히포크라테스 XML 데이타베이스 모델의 접근제어 메커니즘을 보면 다음과 같은 상황에서 문제점이 발생한다.

태스크 프로세스상에서 필요한 제공자의 정보에 대한 최소의 접근권한을 요구할 할 경우 최소로 필요한 사용권한보다 상위의 사용권한을 사용하게 되면 필요이상의 사용권한을 허용하게 된다. 즉, 최소권한의 원칙을 위배되는 문제점이 발생한다.

본 논문에서는 위에서 언급한 사용목적 관리시 발생하는 사용목적 표현력의 부족, 삽입·삭제시 사용목적 관리의 미흡함 그리고 접근제어시 발생하는 최소권한의 원칙 위배의 문제점을 각각 3-타입의 사용목적 분류화와 Pu-ARBAC모델을 제시함으로써 해결하려고 한다.

3. 사용목적 분류화를 통한 보안 접근제어 기법

3.1 사용목적 분류화

본 절에서는 사용목적을 대상으로 상위 사용목적이 하위 사용목적을 내포하는 특성인 상속적 구조, 비즈니스 프로세스상 시간의 순차적순서에 따라 사용가능한 특성인 시간적 구조 그리고 상속적, 시간적 구조 이외의 사용목적을 독립적 구조로 3가지 타입으로 분류화한다.

정의 1) 사용목적 트리(Purpose Tree)를 PT라 하고, Pu는 PT 의 모든 사용목적들 중 어느 한 사용목적(Purpose)이라 하며, 그리고 P는 개인정보에 관한 권한(Permission)의 집합이라 하자. 이때 P_i는 집합 P 중 한 원소가 되며, $Pu_i=\{P_1,P_2, \dots, P_n\}$ 이다.

정의 2) 모든 사용목적(Purposes)들은 3-타입 중 하나로 분류화 되어지며, 3-타입의 분류화는 다음과 같다.

가) Inheritance Purpose(타입 I) : 상속적 구조의 사용목적

$\forall i$, purpose $Pu_i \in$ type I $\Rightarrow Pu_i \in$ set of inheritance purpose

나) Stream Purpose(타입 S) : 시간적 구조의 사용목적

$\forall i$, purpose $Pu_i \in$ type S $\Rightarrow Pu_i \in$ set of stream purpose

다) Alone purpose(타입 A) : 독립적 구조의 사용목적

$\forall i$,purpose $Pu_i \in$ type A $\Rightarrow Pu_i \notin$ set of inheritance purpose $\wedge Pu_i \notin$ set of stream purpose

으로 분류화하며,

$\forall i$, purpose $Pu_i \in$ type A and $Pu_i \in$ type S $\Rightarrow Pu_i \in$ set of inheritance purpose $\wedge Pu_i \in$ set of stream purpose

이 존재 가능하다.

정의 3) PT를 사용목적 트리(Purpose Tree)라 하고, Pu는 PT 의 모든 사용목적들 중 어느 한 사용목적(Purpose)이라 할 때, 사용목적 Pu는 타입에 따라 다음과 같은 규칙을 따른다.

타입 I : - 상위 사용목적은 하위사용목적을 내포한다.

타입 S : - 상위 사용목적을 활성화하기 위한 조건으로 하위 사용목적이 조건(시간적인 조건)이 만족 되어져야 하며, 하위 사용목적들은 AND, OR 관계로 이루어져야 한다.

타입 A : - 타입 I 와 타입 S 이외의 모든 사용목적들은 타입 A로 구별되어 진다.

이들 분류기준은 실제 비지니스 프로세스(business process)상에서 사용목적이 사용됨을 기반으로 하며, 이들 사용목적들 간에는 삽입·삭제의 행위 과정에 있어서 상이하게 다른 기준이 적용된다. 그로 인해 서로 다른 방식의 삽입·삭제의 행위가 발생된다. 삽입·삭제 행위시 본 논문에서는 너비우선 탐색을 가정하며, 정의 3의 규칙을 따라야 한다.

정의 4) Pu는 PT 의 모든 사용목적들 중 어느 한 사용목적(Purpose)이라 하자. 이때 Pu_t는 집합 PT 중 시간적 특성을 지닌 사용목적이며, Pu_t 은 $Pu_1 \rightarrow Pu_2 \rightarrow \dots \rightarrow Pu_n$ 와 같은 시간적(타입 S) 특성을 지닌다.

본 논문에서는 사용목적의 삽입·삭제 행위시 따라야 할 규칙(정의3)과 이들 3가지 특성으로 분류화되어진 사용목적(타입 I, 타입 S, 타입 A)들이 현실에 존재하는 모든 사용목적들을 표현 가능하다.

그림 1은 정보제공자가 제공한 사용목적에 부합하는 권한을 사용목적 트리에 같이 표기한 예이다.

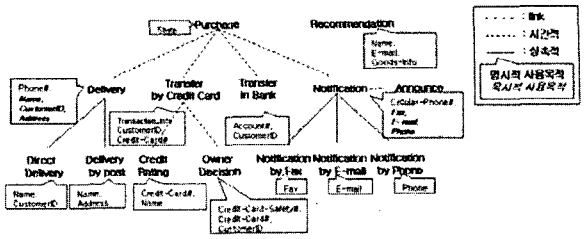

그림 1. 사용목적 트리-권한 부여의 예

3-타입의 분류화에 따른 각각의 특성에 따라 각기 다른 알고리즘에 의해 관리되는 사용목적을 보였으며, 이 예를 통하여 사용목적 표현과 삽입·삭제시 사용목적 관리의 문제점이 해결됨을 보였다.

3.2 사용목적 분류화를 통한 보안 접근제어 모델

본 절에서는 - 사용목적- 분류화를 통한 보안 접근제어 모델로써 Pu-ARBAC을 제시한다. 본 모델은 기존의 ARBAC(Administrative Role Based Access Control)을 기반으로 하고 있으며, 그 중 개인정보에 대한 권한을 그 대상으로 한다.

사용목적은 개인정보에 대한 권한부여의 단위이며, 본 논문의 접근제어 과정에서는 역할을 통하여 부여된 권한을 이용해 특정 태스크 프로세싱(task processing) 수행 중 필요시 되는 개인의 프라이버시와 관련된 정보를 제공하기 위한 조건이자 권한의 단위이다. 그림 2는 환경을 예를 들어 설명한다.

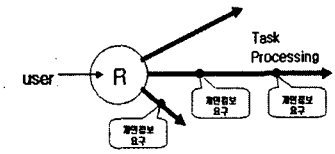

그림 2. Pu-ARBAC 환경의 예

인터넷을 통하여 책을 판매하는 기업이 나이별로 책 선호도를 조사 후 회원들에게 이메일을 사용하여 책을 추천하는 태스크를 수행하는 예를 들면, 여기서 R은 사용자가 얻을 수 있는 역할(role)된다. 또한 역할을 활성화한다는 말은 그에 해당하는 권한을 얻는 것이며, 이때 얻게 되는 권한은 시스템 자원 즉, 나이별로 책 선호도를 분석할 수 있는 분석툴 또는 그 후 고객들에게 책을 소개할 경우 사용되는 이메일 서비스 등을 사용할 수 있는 권한을 말한다. 사용자는 이러한 시스템 자원을 이용하여 일을 수행 중 개인정보를 필요로 하며, 이때 개인정보에 대한 요청시 개인정보에 대한 접근제어가 필요하다. Pu-ARBAC은 이러한 상황에서 기존보다 향상된 최소권한의 원칙을 따르는 접근제어를 한다.

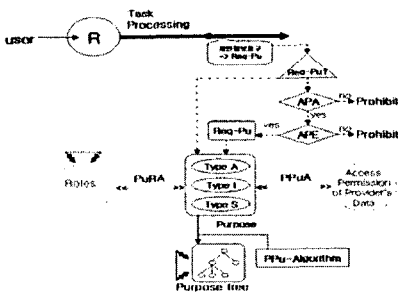

그림 3. Pu-ARBAC 모델

Pu-ARBAC 모델은 사용목적-역할 관리(Purpose-Role Administration)와 권한-사용목적 관리 (Permission- Purpose Administration)의 구성요소로 되어있으며 ARBAC을 따르고 있다. 사용목적 획득과정은 다음과 같다.

- Req-Pu는 태스크 프로세싱상에 관리자의 의해 미리 정해진 사용목적(권한) 이며, Req-Pu↑는 사용목적트리를 참조하여 사용목적 Req-Pu의 상위 사용목적들의 집합을 얻는다.
- APA은 <ap, cr>의 2-튜플로 이루어져 있다. cr은 <r, C>의 2-튜플을 가지며, C는 역할 속성과 시스템 속성를 말한다. 여기서 APA은 사용자가 요구하는 사용목적 Pu가 활성화 가능하면 yes를 반환하며, 그렇지 않으며 no를 반환한다.
- APE(Access Purpose Existence)은 Req-Pu↑에 Pu이 있으면 yes 그렇지 않으면 no를 반환한다.
- 최종적으로 yes가 반환되면 최초에 정해진 태스크를 진행하는데 필요한 최소의 사용목적(권한) Req-Pu를 선택하여 PPu-Algorithm(사용목적 권한 획득 알고리즘)을 이용하여 권한을 획득하게 된다.

다음 그림 4는 사용목적 권한 획득 알고리즘과 시간적 성격의 사용목적에 대한 메타 데이타를 저장하고 있는 Purpose action table 이다.

```
request_purpose(ID)                                    ID : 입력(사용목적ID)
                                                       type : 사용목적 구조
Begin                                                  rights : 권한
  If(search node(ID))
    {
      If (type == "None") then return rights;
      else If (type == "Pu_Link") then go parent's node and return rights;
      else if (type == "Pu_Inheritance_Last") then return rights;
      else if (type == "Pu_Inheritance") then return rights;
      else if (type == "Pu_Precondition_Last") then return rights;
      else if (type == "Pu_Precondition")
        {
          if (comparing condition value with Purpose action table => satisfaction) then return rights;
        }
      else fail;
    }
  else fail;
End
```

(a) PPu-Algorithm(사용목적 권한 획득 알고리즘)

Purpose (id)	수행여부 (yes/no)
Analysis Data Collection :	no yes :

(b) Purpose action table

그림 4. 사용목적 권한 획득 알고리즘

4. 비교 분석 및 평가

본 절에서는 사용목적의 분류화와 이를 이용한 접근제어인 Pu-ARBAC을 기존의 모델과 실험을 통하여 다음과 같은 비교 분석한다.

표 1은 기존모델과 제안모델에 대해서 사용목적 관점에서 비교 분석한 것이다.

표 1. 비교 분석 - 사용목적 관점

O : Appropriate, Δ : Partially Appropriate, X : No Consideration

평가기준 \ 모델		제안 모델	Hippocratic Databases	Hippocratic XML Databases	Purpose Based Access Control
기존모델의 문제점	데이터수집 후 보안관리	O	O	O	O
	사용목적관리	O	X	X	X
	Pu1(기존) ∩ Pu0(삽입) = some	O	O	X	X
	Pu1(기존) ∩ Pu0(삽입) = none	O	O	X	X
	Pu1(기존) = Pu0(삽입)	O	O	X	X

표 2는 4가지 모델에 대해서 접근제어 관점에서의 실험을 통하여 비교 분석한 것이다.

표 2. 실험 비교 분석 - 접근제어 관점

O : Appropriate, Δ : Partially Appropriate, X : No Consideration

평가기준 \ 모델		제안 모델	Hippocratic Databases	Hippocratic XML Databases	Purpose Based Access Control
보안관리를 위한 접근제어 기법		• ARBAC을 기반으로 역할과 사용목적을 사용	• DBMS를 기반으로 프라이버시 권한(속성 액세스 통제)과 사용목적을 사용	• XML을 기반으로 프라이버시 권한(관리자 프라이버시권한 속성 액세스 통제,제공자 프라이버시 권한 레벨도 액세스 통제)을 사용	• RBAC을 기반으로 역할과 사용목적을 사용
개인정보 요구(사용목적 요구)시 최소권한의 원칙(least privilege)		• 묵시적, 상속적, 시간적 구조를 고려해 사용자가 활성화시킬 수 있는 사용목적은 조건으로 사용되며, 최종적으로 Task Process에서 제시하는 최소의 사용목적으로 최소의 개인정보(권한)가 제공 • 역할 속성과 시스템 속성의 constraints를 제공	• 요구 사용목적보다 큰 권한을 가지고 있는 사용목적을 활성화 할 경우 불필요한 개인정보(권한)가 제공	• 요구 사용목적의 상위 사용목적을 활성화 할 경우 불필요한 개인정보(권한)가 제공	• 요구 사용목적의 상위 사용목적을 활성화 할 경우 불필요한 개인정보(권한)가 제공 • 역할속성과 시스템 속성 constraints를 제공
기존 모델의 문제점(요구사항) - Task에 필요한 사용목적보다 상위의 사용목적으로 접근 시	접근 허용 문제	Δ	O	O	O
	최소권한의 원칙문제	O	X	X	X

5. 결론

최근 들어 사적인 데이타에 대한 개인의 프라이버시 문제가 큰 이슈로 떠오르고 있으며, 그로 인해 개인정보에 대한 수집 방법과 수집 후 보안관리에 대해 많은 연구가 진행 중에 있다.

본 논문은 기존 연구에 대한 문제점을 제시하였고, 또한 문제의 해결책을 제시하였다. 본 논문에서 제안한 기법의 기여도는 다음과 같다. 첫째, 사용목적의 표현력을 향상 시키기 위해 사용목적을 3가지 구조로 분류화하였으며 둘째로, 각 사용목적 구조에 따른 사용목적의 관리기법을 제시하였다. 셋째로, 이렇게 분류화되어 관리되는 사용목적을 통하여 최소권한의 원칙을 따르는 접근제어 기법을 제시하였다.

본 논문에서 제안한 기법은 최근 중요한 이슈로 떠오르는 개인정보에 대한 프라이버시 보안에 있어서 정보 제공자의 의도를 따르며, 보안관리에 있어서 최소권한의 원칙을 따름으로써 개인정보 제공자의 데이타에 대한 보안을 강화하였다.

본 논문에서 제안한 접근제어 기법은 보통 일반 업무에서 보듯이 태스크상에서 개인정보를 접근하는데 있어 이미 고정화되어 있는 사용목적에 사용자의 업무상 위치나 상황을 조건으로 비교하여 접근 여부를 결정한다. 그러나 상황에 따라서 동적으로 사용목적을 필요로 하는 환경 또한 존재한다. 본 논문은 이러한 환경에 대해 조사가 미흡했고, 또한 그러한 환경에서는 기존의 접근제어 모델들과 차별성이 없다.

본 논문은 한 기업환경에서 개인정보에 대한 프라이버시를 보호하기 위한 기법이다. 그러나 실제로 기업에서 관리하고 있는 개인정보는 한 기업 내에서만 이용되는 것이 아니라 한 기업에서 다른 기업으로 유통되는 경우가 많다. 이러한 경우 개인의 프라이버시 보호에 큰 어려움이 생기며, 이에 대한 제한사항에 대한 연구가 추가적으로 필요하다.

참 고 문 헌

[1] World Wide Web Consortium (W3C). Platform for Privacy Preferences (P3P). Available at www.W3.org/P3P

[2] IBM: Enterprise Privacy Authorization Language (EPAL); Submission request to W3C, http://www.w3.org/Submission/EPAL/, November 2003.

[3] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, Yirong Xu, "Hippocratic Databases", Proceedings of the 28th VLDB Conference, Hong Kong, China, 2002

[4] Ji-Won Byun, Elisa Bertino, Ninghui Li, "Purpose Based Access Control of Complex Data for privacy Protection", SACMAT'05, 2005, Stockholm, Sweden

[5] 이재길, 한욱신, 황규영, "Hippocratic XML Databases: A Model and Access Control Mechanism", 정보과학회논문지: 데이타베이스 제 31 권 제 6호 (2004.12)