XML 스키마를 위한 접근제어 모델 설계†

김은희*, 문호성*, 신문선*, 류근호*
*충북대학교 데이터베이스연구실
e-mail:ehkim@dblab.chungbuk.ac.kr

Design of Access Control Model for XML Schema

Eun Hee Kim*, Ho Sung Moon*, Moon Sun Shin*,
Keun Ho Ryu*
*Database Laboratory, Chungbuk National University

요약

최근 많은 웹 기반 서비스나 애플리케이션들이 XML 형태로 지원되면서 XML 데이터의 보안에 대해서 많은 연구가 이루어지고 있다. 기존의 XML 보안은 암호, 서명, 접근제어의 형태로 이루어지고 있으며 그 중에서 접근제어는 DTD기반과 문서기반으로 분류되어 임의적 접근제어 모델을 적용한 연구가 진행되어 왔다. 그러나 DTD의 대안으로서 객체지향개념을 수용하는 XML 스키마의 사용이 증가되고 있어 이를 위한 보안요구사항과 접근제어정책이 추가로 필요하게 되었다. XML문서의 데이터보호를 위해서 기존의 DTD기반과 문서기반 접근제어정책을 수용하면서 스키마 기반의 접근제어정책을 지원하기 위해서 이 논문에서는 역할기반접근제어 모델을 적용한 XML 스키마 기반의 접근제어 모델을 제안한다.

1. 서론

최근 많은 웹 기반 서비스들과 애플리케이션들이 XML형태로 지원되면서 XML 데이터의 보안에 대해서 많은 연구가 이루어지고 있다[3,4]. XML 데이터의 보안에 대한 연구는 크게 암호화, 서명, 접근제어로 나누어지며 특히 접근제어와 관련하여 논의하고자 한다. 기존의 XML데이터에 대한 접근제어는 DTD기반과 문서기반으로 분류되어 임의적 접근제어 모델을 적용한 연구가 진행되어 왔다[1,2]. 위의 두 정책들은 DTD 와 문서 관계에 대해서만 유용하며 잘 정형화된 문서나 유효한 문서에서 적용할 수 있다. 그러나 최근 XML 스키마에 대한 보안 요구사항이 대두되어 이 논문에서는 스키마와 문서 관계에서의 접근제어 정책을 분석하며, 사용자와 관련된 역할 개념을 확장한 역할기반 접근제어 모델을 적용한 접근제어 모델을 설계한다.

제안된 모델은 스키마와 문서관계, DTD와 문서관계 모두에 적용될 수 있다. 논문의 구성은 2장에서는 관련연구로서 기존에 연구된 XML 접근제어 기술과 역할기반 접근제어 모델에 대해서 간략히 설명하고, 3장에서는 XML 스키마 보호 요구사항에 대해서 분석하며, 4장에서 접근제어 정책에 대해서 기술하고 5장에서는 역할기반 접근제어 모델을 적용한 새로운 모델을 제안하며 6장에서 결론을 맺는다.

2. 관련연구

2.1 기존 XML 접근제어

기존의 XML데이터에 대한 접근제어로는 DTD기반과 문서기반으로 크게 분류되어 임의적 접근제어 모델을 적용한 연구가 진행되어 왔다[1,2]. DTD 기반 정책에서 인증은 XML 소스의 DTD와 관련 있고 DTD 대 인스턴트 전달 관계 때문에 DTD 인스턴트를 전달한다. 그리고 문서 기반 정책에서 인증은 XML 문서와 직접적으로 관련이 있으며, 각 문

† 이 연구는 한국과학재단 RRC(청주대 정보통신연구센터)의 지원으로 수행되었음

서는 보호를 위한 가장 적당한 인증 정의에 의해서 분리되어 다루어지게 되므로 문서내용에 대한 서로 다른 보호 수준을 제공할 수 있도록 서로 다른 단위 레벨을 정의할 수 있다. 위의 두 정책들은 DTD 와 문서 관계에 대해서만 유용하며 잘 정형화된 문서나 유효한 문서에서 유용하게 적용할 수 있다.

2.2 역할기반 접근 제어 모델

역할기반 접근 제어 모델[8]은 전통적인 접근 제어 모델인 임의적 접근 제어 모델과 강제적 접근 제어 모델의 대안으로서 최근 여러 분야에서 접근 제어 모델로서 적용되고 있다. 역할기반 접근 제어 모델의 장점은 실세계 조직체의 역할을 기반으로 하기 때문에 실세계를 모델링 하기가 쉽고, 접근 제어 정책을 기술하기가 용이하며 분산된 사용자들을 위해서 원격 사용자들의 역할 또한 모두 수용할 수 있기 때문에 원격 사용자의 홈 사이트에서도 적용 가능하다.

3. XML 스키마 접근제어를 위한 보안 요구사항

XML 접근제어를 위한 보호는 전통적인 데이터베이스에서의 데이터 보호와 관련하여 새로운 보안 요구사항을 필요로 한다. 새로운 보안 요구사항들은 XML 문서 구조와 주어진 소스에 존재하는 DTDs, valid, well-formed, Schema, 문서들로부터 유도된다. 이 논문에서는 기존의 DTD 기반 보안 요구사항에서 기술된 항목들 중에서 유사한 부분은 그대로 수용하며 스키마에 관련된 항목들을 분석한다. XML 스키마 접근 제어를 위한 보안 요구사항들은 다음과 같이 나타낼 수 있다[6,7].

3.1 미세한 인증 단위

인증은 서로 다른 단위 레벨에서 보호 객체와 관련이 있다. 스키마와 관련하여 보호 객체 단위는 다음과 같이 식별할 수 있다.

- 스키마 : 스키마와 스키마를 위한 스키마를 포함.
- 타입 : 복잡한 타입과 단순한 타입을 모두 포함.
- 엘리먼트(서브엘리먼트) : 엘리먼트와 그 엘리먼트에 포함된 모든 엘리먼트를 포함.
- 속성 : 엘리먼트내의 모든 속성을 포함.

3.2 인증 상속

XML 스키마는 객체지향 개념을 가지고 있기 때문에 객체 지향의 특징인 상속 개념을 도입하여 인증을 상속 할 수 가 있다.

3.3 유효한 문서와 잘 정형화된 문서

스키마를 적용한 문서의 유효성은 스키마와 문서 사이의 관계와 스키마와 DTD의 관계에 따라서 제한을 할 수 있다.

- 스키마와 문서의 관계 : 스키마에서는 문서의 구조와 내용을 기술하며 스키마 내부에서 타깃 네임스페이스를 기술하여 해당 네임스페이스와 문서상에서 사용된 네임스페이스가 일치하는지에 따라서 문서에 대한 유효성을 검증한다.

4. 역할기반 접근제어를 적용한 XML스키마 접근제어 모델 설계

4.1 XML 스키마를 위한 접근제어 정책

이 절에서는 앞 절에서 설명한 보안 요구사항들을 기반으로 하여 XML스키마를 위한 접근제어 정책을 기술한다.

XML 스키마 기반의 접근제어 정책에서 인증은 XML스키마와 관련이 있고, 스키마 대 인스턴트 전달 관계 때문에 스키마의 인스턴트를 전달한다. 또한 스키마의 유효한 문서 인스턴트의 내용에 대한 서로 다른 보호 수준을 제공할 수 있게 스키마 내부에서 다른 타깃 네임스페이스를 정의할 수 있다. 또한 이런 접근 제어 정책들은 스키마 명세서를 통해서 정의를 할 수 있다. 스키마 명세서는 다음과 같은 형태로 나타낸다.

schema-spec.[element-spec].
[set-of-attribute].[target-namespace]

여기서, *schema-spec*은 스키마 전체를 의미하고 있으며 XML 문서 식별자 또는 기호 * 이다. * 기호는 소스에서 모든 문서를 표기하는데 사용된다.

*[element-spec]*은 schema-spec에 의해서 표기된 문서를 위한 엘리먼트 명세서이다. schema-spec=* 면 element-spec는 소스에서 임의의 어떤 문서를 위한 엘리먼트를 명시할 수 있으며 선택사항이다.

*[set-of-attribute]*는 속성들의 집합으로 식별하여 선택적으로 할 수 있으며 명세서에서 함께 발생하지는 않는다.

*[target-namespace]*은 schema-spec에 의해서 표기된 네임스페이스에 대한 것으로서 선택적으로 할 수 있으며 target-namespace=*이면 스키마 내에 있는 임의의 네임스페이스를 명시할 수 있다.

(예1.) 표1의 고객관리에 관한 스키마에 대해서 고려

해 보자.

다음은 스키마 명세서의 예제이다.

schema : 스키마 전체를 의미

schema.id.name : 스키마에서 id 와 name 엘리먼트를 명시

schema.{xmlns:xmlschema} : 스키마에서 xmlschema 네임스페이스를 적용한 부분을 명시

표 1. 스키마 예제

```
<xsd:schema
xmlns:xsd="http://www.w3.org/2000/10/xmlschema">
<xsd:element name="id" type="xsd:string"/>
<xsd:element name = "name"  type="xsd:string"/>
<xsd:element name = "sex"  type="xsd:string"/>
<xsd:element name = "job"  type="xsd:string"/>
<xsd:element name = "address"  type="xsd:string"/>
</xsd:schema>
```

XML 스키마에 대해서도 엘리먼트에 대해서 접근 제어 정책을 설정을 해 놓으면 서브엘리먼트나 속성 그리고 데이터타입등에 대한 접근제어는 부득이 설정을 하지 않아도 된다. 예를 들어, "주소{시, 군, 리, 반, 우편번호}"로 구성된 주소 엘리먼트에 대해서 접근제어를 설정을 해 놓았다면 서브엘리먼트인 {시, 군, 리, 반, 우편번호}에 대한 접근제어도 자동적으로 상속을 받기 때문이다. 이것은 스키마 전체에 대해서도 적용이 될 수 있다.

4.2 역할 기반 접근 제어 모델 적용

접근 제어 모델로서 역할 기반 접근 제어를 사용하는 가장 큰 이점은 1) 역할들을 계층 형태로 표현이 가능하며, 2) 역할들이 서로 다른 권한을 가지고 동일한 사용자에 대해서 서로 다른 세션을 허용할 수 있으며, 3) 권한들은 사용자가 아닌 역할을 가지고 저장이 된다는 점이다. 그리고 역할 기반 접근 제어 모델은 홈 사이트뿐만 아니라 원격 사이트에서도 역할을 그대로 수용할 수 있다는 장점을 가지고 있다. 즉 예를 들면 홈 사이트에서 역할이 대학원생이라면 원격사이트에서 그 사용자에게 할당된 역할도 대학원생이 된다. 이러한 점에서 역할 기반 접근 제어 모델은 분산환경에서도 적합하다고 할 수 있다. 따라서 역할 기반 접근 제어를 적용한 XML 스키마를 위한 접근 제어 모델을 설계한다.

XML 스키마를 위한 역할 기반 접근제어 모델을 적용한 아키텍처는 아래 그림 1에서처럼 나타낼 수 있다. 제안된 모델의 구성요소는 다음과 같다.

U : 사용자 집합(또는 자동화된 에이전트)

R : 역할 집합(역할 계층을 포함하고 있다)

P : 권한 집합(read, write, execute, append)

S : 세션 집합

C : 제약사항 (예외사항 처리)

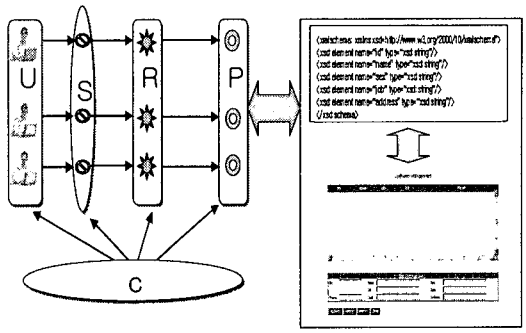

그림 1 스키마를 위한 RBAC 모델

(예2). 그림 1을 적용한 예제.

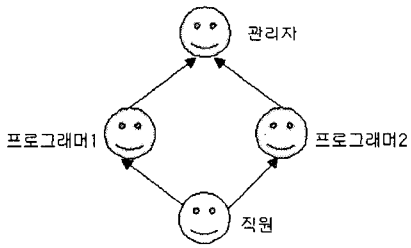

그림 2 역할 계층

표 2 그림1에 대한 사용자, 역할, 권한 예

사용자	역할	권한	비고
U1	관리자	read, write, append	스키마 전체
U2	프로그래머 1	read, write	스키마 일부
U3	프로그래머 2	write	스키마 일부

사용자U1은 관리자로서 스키마 전체에 대해서 read, write, append를 할 수 있고, 사용자U2는 프로그래머 1로서 고객에 대한 정보 변경 시 read, write 할 수가 있지만 스키마 전체에 대한 권한이 아니라 스키마 일부 즉 특정 엘리먼트에 대해서만 read, write 권한을 수행할 수가 있다. 사용자U3도 역할은

프로그래머1과 같은 프로그래머이지만 사용자 U2와는 다르게 스키마 일부에 대해서만 write를 할 수 있다.

회사 내의 주요 고객에 대한 정보는 전체 프로그램 관리자(U1)에 의해서 수행이 되며 프로그래머 1과 2는 스키마의 특정 부분에 대해서만 read, write 권한을 각각 수행 할 수 있기 때문에 상위 계층(즉, 관리자)에서 볼 수 있는 정보에 대해서는 접근을 할 수 가 없게 되므로 정보에 대한 기밀성을 유지 할 수 있다. 두 프로그래머1과 2의 관계에서도 read, write 권한이 수행될 때 프로그래머 2가 가지고 있는 권한으로는 같은 프로그래머일지라도 프로그래머 1이 접근 할 수 있는 정보에 대해서는 접근을 할 수가 없으므로 정보에 대한 기밀성을 유지 할 수 있다.

5. 결론

DTD의 대안으로서 객체지향개념을 수용하는 XML 스키마가 각광을 받고 있으며 이를 위한 보안 요구사항과 접근제어정책이 추가로 필요하게 되었다. XML문서의 데이터보호를 위해서 기존의 DTD 기반과 문서기반 접근제어정책을 수용하면서 스키마 기반의 접근제어정책을 지원하기 위해서 이 논문에서는 역할기반접근제어 모델을 적용하여 XML 스키마 기반의 접근제어 모델을 제안하였다. 먼저 XML 스키마 보호 요구사항을 분석하고 접근제어 정책을 기술하였으며, 기술된 정책에 역할 기반 접근 제어 모델을 적용하였다. 향후 DTD기반이나 문서기반 접근제어정책과 비교 분석하고 실제환경에서 구현하는 연구가 계속될 것이다.

참고문헌

[1]E.Bertino,S.Castano,E.Ferrari,M.Mesiti, Specifying and Enforcing Access Control Policies for XML Document Sources, World Wide Web 3(3), pages:139-151, 2000.

[2]M.Hitchens, V.Varadharajan, RBAC for XML Documents Stores, Third International Conference, ICICS 2001, Xian, China, Proceedings, LNCS 2229, p. 131-143. November 13-16, 2001.

[3]H.He,R.K.Wong, A role-based access control model for XML repositories, Proceedings of the First International Conference on , Volume: 1, pages: 138 -145, 2000.

[4]E.Bertino,S.Castano,E.Ferrari, Securing XML Documents: the Author-X Project Demonstration, SIGMOD Conference, pages:21-31, 2001.

[5]E.Damiani,S.C.Vimercati,S.Paraboschi,P.Samarati, Securing XML Document, Springer-Verlag, EDBT2000, pages 121-135, 2000.

[6]World Wide Web Consortium(W3C), XML Schema Part 1: Structures, May 2001, http://www.w3.org/TR/2001/REC-xmlschema-1-20010502.

[7]World Wide Web Consortium(W3C), XML Schema Requirement, Feb 1999, http://www.w3.org/TR/1999/NOTE-xml-schema-req-19990215.

[8]R.Sandhu,J.Coyne, H.Feinstein, Role based access control models, IEEE computer, vol. 2, pages:38-47, 1996.