다중 사용자 환경의 XML 문서를 위한 접근제어모델 설계

심효영° 반용호 김종훈
동아대학교 정보보호실험실
{dungsili°, gaussian, jhpark}@donga.ac.kr

Design of Access Control Model for XML Documents in Multi-user Environment

HyoYoung Sim° YongHo Ban JongHun Kim
Information Secure Lab, Dong-A University

요 약

현재 다양한 분야에서 XML을 이용한 웹 서비스와 애플리케이션이 활용되고 있다. XML 관련 웹 서비스를 실제 환경에서 적용하기 위해서는 XML 데이터와 관련서비스들에 대한 보안 메커니즘이 필요하다. 본 논문에서는 XML 문서의 보안성 확보를 위한 접근제어 모델을 제안한다. 제안된 모델에서는 실시간 동시 작업이 이루어지는 서비스 환경에 적합한 모델구현을 위해서 역할기반 접근제어의 개념을 이용하며, 중요 정보에 대한 암호화 과정을 통해 XML 문서 및 데이터에 대한 안전성을 보장한다.

1. 서 론

XML의 표준이 등장한 이후로 이를 활용하기 위한 관련 표준들이 꾸준히 개발되고 있다. XML과 XML 관련 기술들에 대한 연구를 바탕으로 기업 및 기관 등 다양한 분야에서 XML을 활용한 서비스와 애플리케이션이 개발되고 있다. 이처럼 XML의 활용이 증가함에 따라 XML 데이터가 실제 환경에서 안전하게 사용 되도록 하는 보안 모델들도 제안되고 있다. XML에 대한 보안 방식의 연구 초기에는 기존의 보안 기술들을 활용하였다. 즉 기존의 문서와 컨텐츠와 마찬가지로 암호화 과정 및 안전한 채널을 사용하여 XML 데이터에 대한 보안 모델을 구축하였다. 그러나 이와 같은 방식은 XML을 위해 제안된 보안 메커니즘이 아니며, 따라서 XML 문서의 구조를 잘 반영하지 못한다.[3] 이 때문에 최근 연구되고 있는 XML 위한 보안 메커니즘으로 XML 암호화[1], XML 서명[2], XML 접근제어[3-5] 등이 있다.

본 논문에서는 XML 문서를 위한 접근제어 모델을 설계한다. XML 문서를 위한 접근제어 방식은 현재 실시간 동시 작업 환경에서 많이 사용되는 역할기반 접근제어 모델[7]을 기반으로 한다. 또한 관리자의 정보나 사용자의 패스워드 등과 같은 중요 정보들은 XML 암호화[1] 과정을 통해 XML 문서 및 데이터에 대한 안전성을 보장 한다

본 논문의 구성은 다음과 같다. 2장에서는 실시간 동시 작업 환경에서 많이 이용되는 역할기반 접근제어 시스템에 대해 간략하게 소개하고, 본 논문에서 이용하고자하는 주요 기능을 재 정의한다. 3장에서는 다중 사용자 환경에서 사용되는 XML 문서를 위한 확장된 역할기반 접근제어 모델을 제시하고 특징을 설명한다. 4장에서는 결론 및 향후 과제를 제시한다.

2. 실시간 동시 작업 환경에 적용 가능한 역할기반 접근 제어

소유자 및 관리자가 자율적으로 정보객체에 권한을 부여하는 임의기반접근제어 모델(Discretionary Access Control)[9]과 사전에 정의된 규칙을 통해 객체에 대한 접근을 엄격히 규제하는 강제적 접근제어(Mandatory Access Control)[9]와는 달리 역할기반 접근제어 모델(Role-Based Access Control)[6]은 역할에 따라 접근 권한을 부여한다. 역할에 따른 권한의 부여는 권한 관리를 단순화 시켜주고, 시스템 따른 보안 정책 구현에 효과적이다. 일반적인 역할기반 접근제어 모델은 사용자의 역할에 따른 계층구조는 정의되지만, 각 역할에 해당하는 작업과 세부작업에 대해서는 정의되어 있지 않다. 실시간 동시 작업 환경에 적용을 위해 작업이 정의된 역할기반 접근제어 모델[7]은 <그림1>과 같은 프로세스를 가진다.

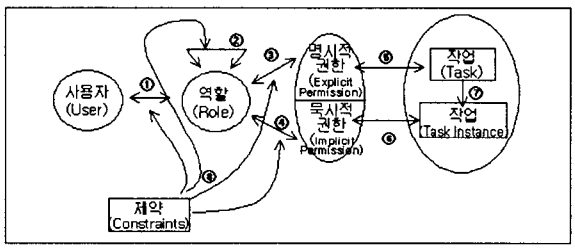

그림1. 실시간 동시작업을 위한 역할기반 접근제어 모델 구조

<그림1>과 같은 역할기반 접근제어 모델의 처리과정은 ①~⑧과 같다. 각 단계는 다음과 같이 정의된다.

① 사용자 할당 - 각 사용자에게 역할을 부여
② 역할 계층 구조 - 개별 역할의 권한에 따른 계층구조
③ 명시적 권한부여할당 - 명시적 권한을 역할에 부여
④ 묵시적 권한부여할당 - 묵시적 권한을 역할에 부여
⑤ 명시적 권한부여 - 작업에 권한 부여
⑥ 묵시적 권한부여 - 세부작업에 권한 부여
⑦ 세부작업 할당 - 작업과 작업 세부과정을 연계
⑧ 권한부여 할당의 제약 - 접근제어 시 필요한 제약조건

3. XML 문서를 위한 확장된 역할기반 접근제어 모델

3.1 사용자(User) 정의

본 모델에서 사용자 정보는 XML 문서로 표현된다. 이들 사용자 정보는 각 클라이언트가 시스템에 접근을 요청할 때 요구되며, 다음과 같이 형식적으로 정의할 수 있다.

u = tuple(id:v_1, password:v_2, roles:(r_1,r_2,…,r_n), 부가정보)

표1. 사용자에 대한 형식적 정의

<표1>에서 정의된 것처럼 사용자 정보는 아이디(id)와 패스워드(password), 역할들(roles)을 요소로 가지고, 사용자의 이름, 나이, 주소와 같은 부가정보들이 추가될 수 있다. 사용자의 아

이디는 사용자의 식별을 위해 반드시 필요하며 각 사용자 마다 유일하다. 패스워드도 사용자의 신분을 증명하기 위해 반드시 필요하다. 형식적 정의에서 "Roles"은 사용자의 역할들을 나타내며, 사용자마다 한개 이상의 역할이 부여된다. 사용자에 대한 나머지 부가 정보는 선택사항으로서 필요에 따라 유동적으로 조직할 수 있다.

<표1>과 같은 사용자에 대한 형식적 정의는 다음과 같은 XML 스키마로 표현할 수 있다.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
   <xs:element name="User">
      <xs:complexType>
         <xs:all>
            <xs:element name="UserID" type="xs:string"/>
            <xs:element name="password" type="xs:string"/>
            <xs:element name="role" type="xs:string"/>
            <xs:element name="name" type="xs:string"/>
            <xs:element name="age" type="xs:nonNegativeInteger"/>
            <xs:element name="address" type="xs:string"/>
         </xs:all>
      </xs:complexType>
   </xs:element>
</xs:schema>
```

그림2. 사용자 정보에 대한 XML 스키마

<그림2>의 스키마 형식을 기반으로 표현된 사용자 정보에 대한 XML 문서는 같다.

```
<?xml version="1.0" ?>
- <User id="s01">
   <userID>S9833761</userID>
   <password>xxxx</password>
   <role>Student</role>
   <name>Hyo Young, Sim</name>
   <age>25</age>
   <address>Geumjeong-gu BUSAN</address>
  </User>
```

그림3 사용자 정보에 대한 XML 문서의 예

3.2 XML 객체 정의

본 접근제어 모델의 보호 객체는 XML 문서이다. 접근제어 정책을 통해 보호되는 XML 문서는 XML 저장소에 저장된다. XML 저장소에 저장된 데이터들의 효과적인 처리를 위해 [8]에서 논의된 방식과 같이 XPath[10] 과 SQL와 같은 질의 구문을 사용할 수 있을 것이다. XML 객체를 저장하기 위한 XML 저장소에 대한 구체적인 설계는 본 논문의 주제와 벗어나므로 여기서는 생략하기로 한다.

3.3 명시적 권한부여와 묵시적 권한부여 정의

실시간 동시작업을 위한 역할기반 접근제어 모델 구조에서 작업에 부여되는 허가를 명시적 권한부여라고 한다. 또한 세부작업에 부여되는 허가를 묵시적 권한부여라고 한다. 이들 권한부여 방식은 작업순서에 따라 사용자에게 권한을 부여할 수 있다. 즉 사용자가 작업을 요청하면, 묵시적이고 명시적인 권한들이 사용자의 역할에 할당되었는지 여부를 판단하고 작업 관리자가 단계적으로 허가와 거부를 할당된다.

다음 <표2>는 사용자의 작업과 역할에 따른 XML 스키마의 권한부여 범위를 나타내는 접근제어 리스트이다.

U105	학생	자기정보 변경	자기 정보 읽기/쓰기		스키마 일부
		수강신청	수강목록 읽기	학생정보 읽기/쓰기	
U104	교수	자기정보 변경	자기정보 읽기	쓰기	스키마 일부
		강의관리	강의정보 읽기,쓰기,삭제	학생정보읽기	
...	...	...	...		
U001	관리자	자기정보 변경	자기정보 읽기/쓰기		스키마 전체
		사용자 관리	사용자 정보 읽기, 쓰기, 삭제		
		작업 추가	작업 및 작업 인스턴스 읽기, 쓰기, 삭제		

표2. 실시간 동시 작업 기반 접근제어 리스트

<표2>에서 표현된 접근제어 리스트에 대한 XML 스키마의 예는 <그림4>와 같다.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" >
   <xs:group name="Student">
      <xs:sequence>
         <xs:element name="UserID" type="xs:ID"/>
         <xs:element name="Role" maxOccurs="unbounded"/>
         <xs:element name="Task">
            <xs:complexType>
               <xs:sequence>
                  <xs:element name="TInstnace" maxOccurs="unbounded"/>
               </xs:sequence>
            </xs:complexType>
         </xs:element>
      </xs:sequence>
   </xs:group>
   <xs:group name="Professor">
      <xs:sequence>
         <xs:element name="UserID" type="xs:ID"/>
         <xs:element name="Role" maxOccurs="unbounded"/>
         <xs:element name="Task">
            <xs:complexType>
               <xs:sequence>
                  <xs:element name="TInstnace" maxOccurs="unbounded"/>
               </xs:sequence>
            </xs:complexType>
         </xs:element>
      </xs:sequence>
   </xs:group>
   <xs:group name="manager">
      <xs:sequence>
         <xs:element name="UserID" type="xs:ID"/>
         <xs:element name="Role" maxOccurs="unbounded"/>
         <xs:element name="Task">
            <xs:complexType>
               <xs:sequence>
                  <xs:element name="TInstnace" maxOccurs="unbounded"/>
               </xs:sequence>
            </xs:complexType>
         </xs:element>
      </xs:sequence>
   </xs:group>
</xs:schema>
```

그림 4. 접근제어리스트에 대한 스키마 예

이들 XML문서에 대한 접근제어 처리과정은 간략히 표현하면 <그림5>과 같다.

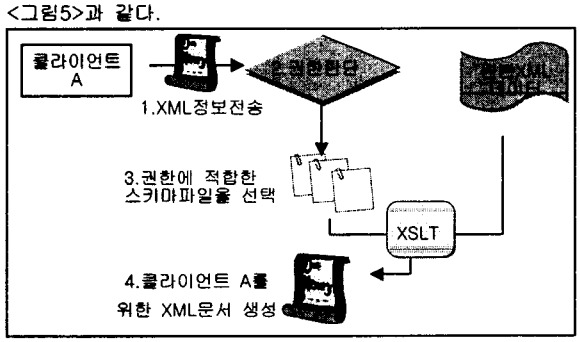

그림 5. XML 문서 처리과정

3.4 XML 암호화의 정의

접근제어방식을 이용한 XML 문서의 보안 모델은 XML 데이터에 대한 불법적인 접근을 효율적으로 제어할 수 있다. 그러나 시스템 관리자와 같이 특수한 권한을 가지는 사용자들의 정보나 시스템 자체가 공격당하는 경우, 접근제어 방식은 안전하다고 할 수 없다. 악의적인 사용자들의 공격에 대해 데이터를 보호하기 위해는 암호화 과정이 필요하다.

여기서는 XML 문서를 위한 보안 모델을 제안하므로, XML 문서를 위한 암호화 방식인 XML 암호화(XML Encryption)[2]을 활용한다. 즉 XML 암호화 방식을 통해 기밀성이 유지되어야 할 XML 문서, 요소, 속성, 컨텐츠 등이 암호화될 수 있다. 암호화된 XML 데이터는 XML 저장소에 따로 저장된다.

3.5 XML 접근제어 모델의 설계

앞에서 설명한 정의를 바탕으로 XML 문서를 위한 안전한 접근제어 모델을 <그림6>와 같이 정의할 수 있다.

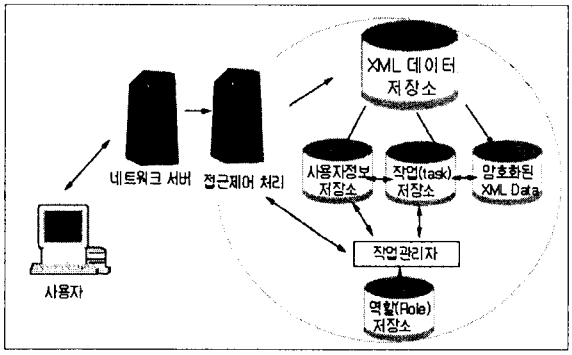

그림6. 실시간 동시 작업 환경을 위한 XML 접근제어모델

제안된 모델에서 사용자는 시스템에 접근하기 위하여 하나 이상의 역할을 부여받는다. 사용자 정보는 서버로 전송되고, 전송된 정보는 XML 데이터 저장소에 저장된다.

XML 데이터 저장소에 저장된 정보 중에서 작업을 수행하기 위해 필요한 사용자 정보는 사용자 저장소에, 작업과 세부작업에 관련된 정보는 작업 저장소에 따로 복사되어 저장된다.

특히 기밀성이 보장되어야 할 중요 정보에 대한 처리를 위해 문서, 요소, 컨텐츠 등을 암호화하여 암호화 데이터를 위한 XML 저장소에 보관한다.

사용자의 역할에 대한 정의와 역할 계층구조는 역할 저장소에 저장된다. 역할에 대한 계층구조는 XML 트리의 형태로 정의될 수 있다. 사용자의 역할에 대한 계층구조는 <그림7>와 같이 정의될 수 있고, XML 트리 구조에서 권한 중복을 막기 위해 상위계층의 역할은 하위 계층의 역할로 전파된다.

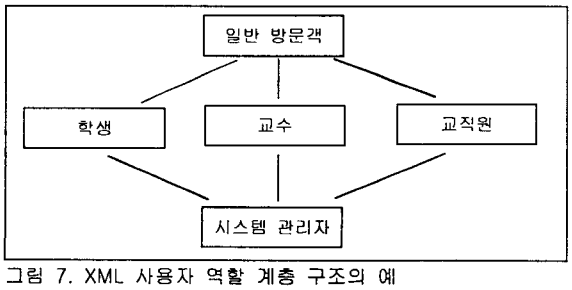

그림 7. XML 사용자 역할 계층 구조의 예

3.6 실시간 동시 작업의 적용

<그림4>에서 살펴본 바와 같이 제안된 접근제어리스트에서는 사용자의 역할과 함께 수행 가능한 작업들을 XML 문서로 정의한다. 작업들은 세부작업으로 표현되며, 이들 세부작업에 대한 정보는 작업 저장소에 저장된다. 작업 저장소에 저장된 세부작업은 작업관리자에 의해 작업 소유자와 작업순서가 결정된다. 이와 같은 과정을 통해 본 모델에서 제시된 접근제어 모델은 여러 사용자가 동시에 작업을 수행하는 실시간 동시 작업 환경에 적용 가능하다.

4. 결론 및 향후과제

제안된 XML 접근제어 모델은 XML 문서를 위한 안전한 보안 메커니즘을 제공한다. 제안된 모델은 확장된 역할기반 접근제어 방식의 적용으로 실시간 동시 작업이 이루어지는 서비스 환경에 적합하다. XML 저장소에 저장된 중요 데이터는 XML 암호 방식을 통해 보안을 보다 강화하고, 이를 통해 XML 데이터 공유를 보다 효율적으로 제공할 수 있다.

향후 연구과제로는 임의의 작업에 따른 세부작업들의 권한부여 과정과 작업의 삭제와 추가와 같은 변화를 접근제어 시스템에 효율적으로 반영하기 위한 방법에 대한 연구가 필요하다. 또한 제안된 접근제어 시스템의 관리를 위한 관리자의 정의와 XML 암호화, XML 서명기술과 통한 접근제어시스템의 강화에 대한 보다 깊이 있는 연구가 필요하다.

참고문헌

[1] W3C, "*XML Signature Syntax and Processing*" ,http://www.w3.org/TR/xmldsig-core/ 2002.

[2] W3C, "*XML Encryption Syntax and Processing*" ,http://www.w3.org/TR/xmlenc-core/ 2002.

[3] Ernesto Damiani, Sabrina De Capitani di Vimercati, Stefano Paraboschi, Pierangela Samarati, "*A fine-grained access control system for XML documents* " ,ACM Computing SurveysACM Trans on Information and System Security, VOL.05 NO.02 pp. 0169 ~ 0202, 2002.

[4]Hao He, Raymond K. Wong "*A Role-Based Access Control Model for XML Repositorie*" Proceedings of the First International Conference on Web Information Systems Engineering (WISE'00) , 2000.

[5]E. Bertino, S. Castano, E. Ferrar, "*securing xml documents with Author-x*" IEEE Internet Computing, Maggio/Giugno , 2001.

[6] Ravi Snadhu, E.J.Coyne, H.L.Feinstein, and C.E.Youman, "*Role-based Access Control Method*", IEEE Computer, vol.29, Feb. 1996.

[7] Savith Kandala and Ravi Sandhu, *"Secure Role-Based Workflow Models."* Database Security XV: Status and Prospects, Kluwer 2002.

[8] Yoshikawa, Amagasa, "*XRel: A path-based approach to storage and retrieval of XML documents using relational database*", ACM Transactions on Internet Technology.,2001.

[9] R.S.Sandhu, P.Samarati, "*Access Control: Principles and Practice*", IEEE Communication Magazine, pp40-48, Sep. 1994

[10] W3C, "*XML Path Language*" ,http://www.w3.org/TR/xpath, 1999