XML 문서를 위한 역할 기반 접근 제어

신휴근[0] 이원석 김동규
아주대학교 정보 통신 전문 대학원
(lightroo[0], koes, dkkim)@ajou.ac.kr

Role-based Access Control for XML Documents

Hyu-Keun Shin[0] Won-Seok Lee Dong-Kyoo Kim
Dept. of Information Communication Engineering GSIC AJOU

요 약

인터넷이 대중화 되면서 HTML 기반의 웹 어플리케이션을 통한 정보 공유가 활발해지고 있다. 그러나 HTML이 가지는 한계로 인해 HTML만을 이용하여 정보 보호 서비스를 제공하는 것은 불가능하다. 이를 해결하기 위해 SGML의 복잡한 특성을 단순화 하여 만든 " 언어를 위한 언어" XML (eXtensible Markup Language) 을 이용할 수 있다. 본 논문에서는 계층적 특성을 가지는 XML을 이용하여 다양한 정보 보호 서비스 중에서 접근제어 서비스를 제공하려 한다. 기존의 임의적 접근제어 모델(MAC)과 강제적 접근제어 모델(DAC)이 가지는 단점을 보완하면서 사용자와 객체간의 관계를 유연하게 설정할 수 있는 역할 기반 접근제어(RBAC) 모델을 적용하는 " XML 문서를 위한 접근제어 모델" 을 제안하려고 한다.

1. 서론

텍스트, 이미지, 동영상 등에 대한 정보를 인터넷상에서 서로 공유하기 위한 마크업 언어로 1986년 W3C에 의해 SGML(Standard Generalized Markup Language)이 제정되었다. 이 언어는 요소(element)와 속성(attribute)에 대한 정규적 정의를 작성하는 방식으로 자신만의 태그를 규정할 수 있도록 하여 특정 언어를 정의하기 위한 언어 위의 언어이다. 이와 같은 SGML의 특성을 활용하여 몇 개의 언어적인 약속을 DTD(Document type definition)로 정의하고 그 DTD를 클라이언트의 브라우저에서 자체적으로 내장하고 있는 상태로 웹 문서를 처리하는 HTML이 웹 서비스를 제공하기 위한 가장 기본적인 언어로 활용되고 있다. 그러나 이와 같은 단순함으로 인터넷을 대중화 시킨 HTML은 태그가 한정되어 있고 HTML 문서 내의 내용에 대한 계층적 표현의 한계로 인해 HTML 기반 웹 어플리케이션의 클라이언트와 서버가 주고 받는 프로토콜에 정보 보호 서비스를 위한 추가적인 처리 과정을 삽입하는 것은 불가능하다.

HTML 기반 웹 어플리케이션이 가지는 이런 단점을 극복하기 위해 XML(eXtensible Markup Language)이 등장하였다. XML은 문서의 내용에 맞게 태그를 정의할 수 있고 SGML이 가지는 복잡한 특성을 단순화한 메타언어로서의 특성을 가지고 있어서 정보 보호 서비스를 위한 작업 요소로 활용하는데 용이하다.

기업 등의 사무조직 내에서 사용자에 따라 접근 가능한 정보의 수준이 다른 경우가 존재한다. 이는 군사 조직에서 계급에 따라 참조할 수 있는 기밀문서의 종류가 다른 것과 같은 문맥이다. 이와 같이 사용자에 따라 구분된 서비스를 제공하기 위한 방법으로 접근제어 모델이 존재하는데, 임의적 접근제어(MAC) 모델이나 강제적 접근제어(DAC)모델의 경우 제어를 해야 하는 사용자 또는 객체의 수가 늘어날 경우 비효율적인 면이 존재하므로 이를 해결하기 위해 역할기반 접근제어(RBAC) 모델이 사용되고 있다. 이 외에도 역할기반 접근제어 모델을 이용할 경우 다양한 보안 정책을 적용할 수 있고 접근제어 규칙을 정의하는 관리자 에게 편리함을 제공할 수 있는 장점이 있다.

본 논문은 XML 기반 웹 어플리케이션의 구현에 있어서 역할 기반 접근제어 모델을 적용하여 사용자에게 차별화된 서비스를 제공하기 위한 모델을 제안하고자 한다.

2. 관련 연구

2.1 DOM (Document Object Model)

XML 문서에는 데이터에 대한 정보뿐만 아니라 태그에 대한 정보도 포함하고 있으므로 그를 이용해 알맞은 정보를 추출해내는데 많은 어려움이 있다. 본 논문에서 제안하는 모델은 XML 문서에서 데이터를 획득하기 위한 방법으로 XML 문서를 파싱하여 트리 기반의 계층적 구조로 변환시켜주는 DOM을 활용하고 있다. DOM API는 XML 구조와 정보로의 접근을 용이하게 하고 그것의 조작을 가능하게 하는 인터페이스를 제공한다. [1]

2.2 XPath

XML 문서가 포함하고 있는 특정 데이터의 위치를 표현하는 방법이 XPath이다. XPath는 논리적인 트리로 XML 문서를 다룬다. 이와 같은 XPath를 이용하여 XML 내에 포함된 엘리먼트의 위치경로를 표현할 수 있을 뿐만 아니라 특정한 계산을 수행할 수 있는데 이는 XML 문서가 포함하고 있는 엘리먼트 단위로 접근제어를 하는 것을 가능하게 한다. [1]

2.3 RBAC(Role-based Access Control)

역할 기반 접근제어 모델은 임의적 접근제어 모델과 강제적 접근제어 모델이 가지는 구조에 추가적으로 사용자와 객체의 중간에 역할(Role)이라는 새로운 개념을 포함시킨 접근제어 모델을 의미한다. 기존 접근제어 모델의 경우 특정 사용자와 객체간의 관계를 직접적으로 설정해 주는 방식인데 이는 기존에 있는 객체의 구조가 변경되는 경우 그 객체와 관련된 모든 사용자와의 관계를 리스트에서 삭제해 주어야 하는 등의 비효율적인 면이 존재한다. 이에 반해 역할 기반 접근제어 모델은 이를 해결하기 위해 특정 사용자를 관련된 모든 객체와 직접적으로 연관시키기 보다는 그와 관련된 객체들과 관계를 맺고 있는 역할과의 관계를 설정함으로써 접근제어를 관리하는데 있어서 많은 이점이 존재한다. [2]

3. RBAC을 이용한 접근 제어 모델 제안

본 논문에서 제안하는 모델을 설명하기 위해 다음과 같은 실례를 제시한다.

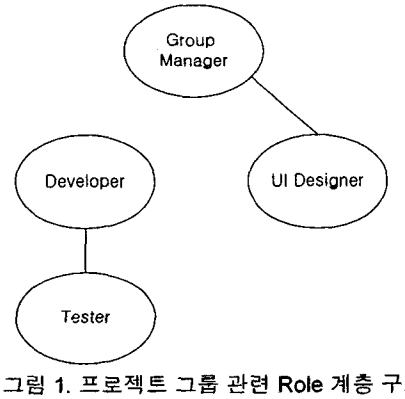

그림 1. 프로젝트 그룹 관련 Role 계층 구조

[그림 1]은 기업 내의 프로젝트 그룹과 관련하여 존재하는 Role들의 계층적 구조를 나타내고 있다. DTD를 이용한 엘리먼트 타입의 정의를 통해 XML 문서 내에 [그림 1]과 같은 계층적 구조를 표현하는 것이 가능하다. 이와 같은 Role 계층 구조를 포함할 수 있는 RBAC 관련 DTD 문서와 XML 문서에 대한 설계는 다음과 같다.

3.1 역할 기반 접근 제어 모델을 위한 RBAC DTD 문서

[그림 2]는 Role의 계층적 구조와 Role이 가질 수 있는 여러 엘리먼트에 대한 태그를 정의하고 있다. "Proposed NIST Role-based Access Control" [2]에서 제안하고 있는 RBAC 모델인 Core RBAC, Hierarchical RBAC, Constrained RBAC 등의 종류에 따라 RBAC 관련 컴포넌트들을 표현한 DTD 엘리먼트들의 구조가 바뀌어야 한다.

```
<!ELEMENT ROLE_HIER (Web_app , (Role)*)*>
<!ELEMENT Web_app (Server)>
<!ELEMENT Role (Name , Cardinality? , (SSD_role?)* ,
          (Parent_role?) , (Child_role)*>
<!ELEMENT Server (#PCDATA)>
<!ELEMENT Name (#PCDATA)>
<!ELEMENT Cardinality (#PCDATA)>
<!ELEMENT SSD_role (#PCDATA)>
<!ELEMENT Parent_role (#PCDATA)>
<!ELEMENT Child_role (#PCDATA)>
```

그림 2. RBAC 관련 DTD 문서(RBAC.dtd)

[그림 2]에서 제시한 DTD는 정적 의무분리(Static Separation of Duty) 관계를 가진 Hierarchical RBAC의 특성을 가지고 있다. 정적 의무분리가 가지고 있는 단점으로 인해 동적 의무분리(Dynamic Separation of Duty) 관계를 포함시키기를 권장하고 있지만 일반 웹 어플리케이션의 경우 웹 서버에 접속하는 사용자에 따라 보여주는 컨텐츠가 다른 서비스를 구현하는데 있어서는 세션동안에 접속하는 사용자에 대한 접근 권한이 동적인 면보다는 특정 사용자에게 보여지는 컨텐츠는 사전에 이미 결정되는게 일반적이므로 정적 의무분리를 적용하는 것만으로도 충분하다.

3.2 역할 기반 접근 제어 모델을 위한 RBAC XML 문서

실례로 제시한 프로젝트 그룹의 계층적 특성 및 [그림 2]에서 정의한 RBAC 관련 DTD 문서를 참고하여 [그림 3]과 같은 Role의 계층적 구조를 포함한 XML 문서를 생각해 볼 수 있다.

```
<?xml version="1.0" ?>
<!DOCTYPE Role_HIER SYSTEM "RBAC.dtd">

<ROLE_HIER>
   <Web_app>
     <Server>Linux</Server>
   </Web_app>

   <Role>
     <Name>Group Manager</Name>
     <Cardinality>1</Cardinality>
     <Child_role>Developer</Child_role>
     <Child_role>UI Designer</Child_role>
   </Role>
          .....
</ROLE_HIER>
```

그림 3. DTD에 의해 Role 계층구조를 표현한 XML 문서

3.3 접근제어 시스템의 전체적인 구조

제안하는 모델의 핵심과정인 접근제어 과정을 거치기 전에 컨텐츠 관련 XML 문서를 다루기 쉬운 형태로 변형시킬 필요가 있다. 따라서 DOM API를 이용한 파싱을 통해 트리 기반의 계층적 구조 데이터를 얻어낸다. 이 트리 데이터는 DOM API에 포함된 다양한 인터페이스를 이용하여 쉽게 노드를 추가하고 삭제할 수 있게 된다.

접근제어 처리를 위해 필요한 요소는 다음과 같다.

- ◆ Role 관련 XML 문서 (Role related XML Document) : 웹 어플리케이션과 관련된 Role의 계층적 구조 및 Role의 특성에 대한 정보를 포함하고 있는 문서
- ◆ 사용자 XML 문서 (User XML Document)
  1) 로그인 하는 과정이 포함되어 있는 경우 인증과정이 우선적으로 수행되고 인증 시 사용된 ID에 따라 사용자를 구분해 놓은 XML 문서
  2) 로그인 과정이 포함되어 있지 않고 인터넷에서 일반적으로 XML 문서를 주고 받는 어플리케이션으로 사용자의 ID가 아니라 호스트명 또는 IP를 통해 사용자를 구분해 놓은 XML 문서
- ◆ 관계 설정 XML 문서 (Relation XML Document) : RBAC 모델을 구현하기 위해 필요한 세가지 기본 요소인 사용자(User), 역할(Role), 퍼미션 (객체(Object) + 기능(Operation)) 들의 관계를 명시하고 있는 XML 문서.

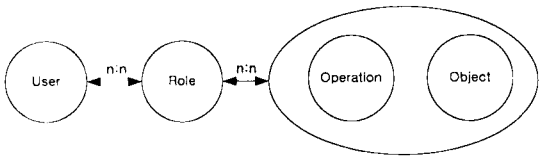

그림 4. RBAC에서 기본 요소들 간의 관계

DOM API를 이용하여 컨텐츠 관련 XML 문서를 파싱하고 얻은 DOM 트리를 앞에서 정의한 세 문서 – Role 계층구조를 표현한 XML 문서, 사용자 정보를 포함하는 XML 문서, 역할 기반 접근제어 컴포넌트들의 관계를 설정한 XML 문서 -를 통해 해당하는 사용자에게 맞는 XML 엘리먼트만을 포함한 XML 문서를 얻어내는 접근 제어 처리(Access Control Process) 과정이 포함된다. 본 논문에서는 접근 제어 처리 과정에 대한 구체적인 구현은 제시하지 않는다.접근 제어 처리기에 의해 나온 DOM 트리는 해당 사용자에게 전송하기 위한 XML 문서로 변형하는 과정이 포함되게 된다. 이와 같은 처리과정은 [그림 5]에서 나타내고 있다.

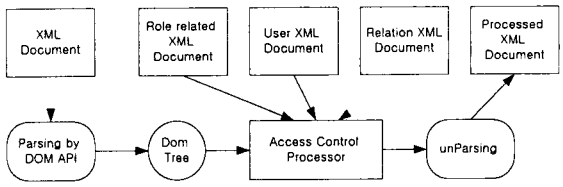

그림 5. 접근제어 시스템의 전체적인 구조

4. 결 론 및 향후 연구과제

본 논문에서는 HTML의 한계를 극복하기 위해 등장한 XML을 위한 역할 기반 접근 제어 모델을 제안하고 있다. 인터넷에서 XML 기반 웹 어플리케이션을 이용하여 서비스를 제공하는 경우 XML이 가지는 계층적인 특성을 이용하여 역할 기반 접근제어 모델을 적용하는 것이 용이하다. 본 논문에서는 일반 웹 어플리케이션을 위한 의무분리 방식으로 정적 의무분리를 제안하고 있지만 좀 더 다양하고 복잡한 서비스를 제공하는 웹 어플리케이션을 위한 경우엔 같은 사용자에게 항상 동일한 서비스를 제공하는 방식이 아닌 세션과 같은 시간 또는 외적인 요인에 따라 다른 서비스를 제공할 수 있는 동적 의무분리 방식을 고려할 필요가 있다.

향후 연구 과제로는 정적 및 동적 의무분리 방식을 적용하여 XML Access Control Processing 를 수행하는 시스템의 프로토타입을 구현해보는 것이다.

5. 참고 문헌

[1] Alexander Nakhimovsky and Tom Myers, "Professional Java XML Programming with Servlets and JSP", 1999

[2] David F. Ferraiolo and Ravi Sandhu, "Proposed NIST Standard for Role-Based Access Control", ACM Transaction on Information and System Security, 2001.08

[3] Ernesto Damiani and Sabrina De Capitani Di Vimercati, "A Fine-Grained Access Control System for XML Documents" ICSA Labs, 1999.12