XML 문서 보호를 위한 접근제어 메커니즘 연구

반용호° 심효영 김종훈
동아대학교 컴퓨터공학과
{gaussian°, dungsili, jhkim}@donga.ac.kr

Research of Access Control Mechanism for XML Document Protection

YongHo Ban° HyoYoung Sim JongHun Kim
Dept. of Computer engineering, Dong-A University

요 약

본 논문에서는 최근 그 필요성이 크게 인식되고 있는 XML 문서에 대한 보호 방안을 접근제어 기법을 적용하여 해결하고자 한다. 일반적인 자원 또는 HTML 문서에 적용되는 접근 방법과 달리 XML 문서가 가지는 구조적 특성을 충분히 활용하여 XML 문서의 각 엘리먼트 레벨까지 소유주의 보호 권한(protection privilege)을 만족하면서, 적절한 사용권한을 가진 사용자에게 해당 XML 문서에 대한 접근과 변경을 수행하는 메커니즘을 제안한다.

1. 서 론

XML(eXtensible Markup Language)[1]은 인터넷상에서 교환되는 구조화된 문서 표현방법으로, 인터넷상에서 구조적으로 정보와 컨텐츠를 기술하기 위한 표준으로 자리 잡았다. 또한 이들 XML 문서는 둘 또는 셋 이상의 이 기종 시스템과 분산 시스템에서 공유될 수 있도록 만들어진 데이터 구조를 이루고 있다. 현재 IT 커뮤니티는 하나의 구조에서 또 다른 구조로 변형이 가능한 공통 메타언어가 XML 이라는 데 동의하고 있다. 의심할 여지없이 XML 은 뛰어난 기술의 한 형태이다. 그러나 XML 이 실제 응용 프로그램에 적용되었을 때 적절한 안전성은 보장될 수 있을까? 이러한 질문은 민감한 데이터가 여러 그룹의 사용자가 공유하여 사용하는 정보 시스템에서는 매우 중요한 고려사항이다. 이들에게 있어서 보안 문제는 시스템 설계에서 가장 먼저 고려해야 할 핵심요소이기 때문이다. 본 논문에서는 XML 데이터에 연관된 보안 문제에 관해 언급하고 웹 기반시스템에서의 XML의 보안 정책을 강화하기 위한 방법을 살펴본다. 일반적인 자원 또는 HTML 문서에 적용되는 접근 방법과 달리 XML 문서가 가지는 구조적 특성을 충분히 활용하여 XML 문서의 각 엘리먼트 레벨까지 소유주의 보호 권한(protection privilege)을 만족하면서, 적절한 사용권한을 가진 사용자에게 해당 XML 문서에 대한 접근 및 변경을 수행하는 메커니즘을 제안한다.

본 논문의 나머지 부분은 다음과 같이 구성된다. 2절에서는 XML 문서에 대한 보호를 위해 제안된 이전의 연구를 살펴본다. 3절에서는 XML 문서의 보호를 위해 Certificate와 접근 제어가 동시에 적용된 접근제어 메커니즘을 소개한다. 4절에서는 접근제어 정책 실현을 위한 XACML 언어를 정의하고, 마지막으로 결론 및 향후 연구방향을 제시한다.

2. 관련연구

XML을 기반으로 하는 응용 애플리케이션의 증가와 함께 XML에 적용 가능한 다양한 보안 기술이 제안 및 개발되고 있다.[2][3] [4] 특히, 최근에는 XML 문서 자체에 대한 전자서명[2]이나 암호화[3] 등에서 확장되어 XML 문서에 대한 접근제어 방법론 및 접근제어 기법들에 대한 연구가 진행되고 있다.[5][6][8][9][10][11][13] 이런 제안 중 몇몇은 상당한 주목을 받고 있는 접근방법도 있지만 아직까지는 실용화 단계까지는 도달하지 못한 것으로 보여 진다. 이전에 제안된 기법들 중 특히 주목할 만한 제안들은 XML 문서에 접근제어 방법을 적용하여 문서의 작은 단위까지도 필요에 따라 접근제어를 위한 권한부여를 할 수 있다는 점이다. 초기에 제안된 권한부여 모델은 접근 요청을 승인하거나 거부하는 시스템으로만 여겨졌다. XML 문서를 위한 접근제어 모델들 중, [7]에 의한 최근 연구는 *sub-subject override policy*와 같은 유연하고 다중 접근통제 정책을 지원하는 능력이 있는 일반적인 프레임워크 제공을 목표로 하고 있다. 하지만 이런 모델 대부분은 접근 요청을 승인하거나 거부하는 시스템으로 보여진다.

Damiani 등은 XML 문서와 스키마 정의에 대한 접근 제어 모델을 제안했다.[6] 비록, 접근제어 메커니즘과 함께 주어진 XML 문서에서의 의미는 유사하지만, 그것은 XML 문서의 읽기를 위한 의미에 보다 많은 중점을 두었다. 이들 제안에서는 XPath[14] 식을 이용하여 권한부여 객체를 식별하고 서버의 접근 결정을 유도할 수 있도록 하였다. 유사한 프레임워크가 [12]에서 제안되었으며, 엘리먼트의 암호화와 암호화된 키를 사용자에 전송하여 원격 수행이 가능하도록 확장되었다.

[11]에서는 안전한 서버에 의존하지 않고 기존의 여러 애플리케이션을 이용하여 접근제어를 수행하기 위한 방법을 제시했다. 접근제어를 수행할 서버를 따로 두지 않으므로 서버 측의 부하를 줄이고 사용자 접근 요청이 있을 때, 접근에 필요한 정보를 따로 요구하는 조건부 접근제어 모델을 제시했다. 사용자가 특정 자원에 대한 접근 요구 시 별도의 정보를 요구하는 방식은 본 논문과 유사하나 본 논문에서 제안된 모델에서는 권한 결정을 위한 서버가 존재하는 것이 차이점이다.

[12]는 임의 접근 정책이 정의될 수 있는 모델을 제안했다. 그런 정책은 주체가 추가적인 동작이나 자격을 만족이 제공되어야 데이터에 대한 접근을 허용한다(즉, 주체의 동작이 로그인 되거나, 패스워드가 제공되어야 한다) 이런 규정(조건)은 비록 그것들이 신뢰 할 수 있는 보안 프로세서의 프레임워크 내에서 동작한다고 가정하고 있지만, 본 논문에서 고려하는 접근제어의 개념과 유사하다. 본 논문에서 제안된 목표는 사용자의 권한 정보를 가진 데이터를 이용하여 해당 문서에 대한 접근을 만드는 것으로 요약된다. 또한 본 논문에서는 제안되는 접근제어 메커니즘은 읽기 기능

에 한정되지 않고, 최종적으로 사용자가 요구하는 문서에 대한 읽기뿐만 아니라, 쓰기, 생성, 삭제 기능 또한 다룰 수 있도록 확장될 것이다.

3. XML 문서 보호를 위한 접근제어 메커니즘

접근제어 메커니즘의 개발을 위해서는 권한부여 규칙(Authorization Rule)이 명확히 규정되고, 접근제어가 적용될 주체(subject)와 객체(object)에 대한 정의가 필요하다.

3.1 전체적인 메커니즘의 개요

주체(subject)

주체는 XML 문서에 접근하고자 하는 사용자를 의미하며, 각 사용자는 사전에 사용자 정보 파일에 등록되어 있다고 가정한다. 등록된 사용자는 SLS(Subject List Sheet)에 추가된다. 주체는 각각의 사용자를 식별하는 ID와 인증서를 보유한다. 논의의 단순화를 위해서 인증서는 속성인증서가 아닌 일반적인 인증서라고 가정하고, 인증서에 포함된 정보 중에서 인증서의 발행자에 의해 사전에 결정되는 인증서의 DN(CN=반용호(BAN YONG HO), OU=ISD, OU=personal, O=Dong-A, C=kr) 또는 인증서의 등급을 사용한다. 주체의 접근 요구는 다음과 같은 정보 집합을 접근제어 서버에 제출함으로 이루어진다. 제출된 정보는 접근제어 서버에 의해 인증서의 유효성과 권한을 검색하여 확장된 형태로 권한부여 서버에게 전달하게 된다.

Request_Sub(ID of Sub, Certificate of Sub, XML Document)

그림 1. 주체의 접근 요구를 위한 초기 정보의 구성

그림 1에서 "ID of Sub"는 사용자를 식별하기 위한 사전에 등록된 ID를 의미한다. "Certificate of Sub"는 사용자가 인증서 발행 서버로부터 발급 받은 인증서를 의미한다. "XML Document"는 사용자가 접근하고자 하는 XML 문서를 의미한다.

객체(object)

객체는 사용 권한을 가진 주체에 의해 검색되는 문서 XML 문서를 말한다.

권한부여 정보의 확장(Extension Authorization Info)

Subject가 제출한 정보는 접근 권한부여 서버에서 다음과 같은 확장이 일어난다.

Request_Sub(ID of Sub, Certificate of Sub's Level , Target Document, ACS, ACCESS)

그림 2. 권한부여를 위해 확장된 권한 정보

확장된 권한 정보는 ID of Sub, Certificate of Sub's Level , Target Document, ACS, ACCESS로 구성된다. 그림 2에서 보이는 바와 같이 Certificate of Sub's Level은 사용자가 제출한 인증서에서 추출한 등급 또는 DN 정보에 의해 결정된 사용자의 권한 등급을 의미한다. ACS(Access Control Sheet)는 사용자의 등급에 따라 Target Document에 대한 정보를 재구성하기 위한 정보를 나타내고, ACCESS는 Target 문서에 대한 접근 허용 또는 접근 거부를 표시하기 위한 정보로 grant|deny 중 한 가지가 선택된다.

3.2 권한부여 규칙(Authorization Rule)

권한 부여 규칙은 XML 문서형태의 권한부여 규칙 명세(Authorization Rule Sheet)에 작성된다. 본 논문에서 정의된 권한부여 규칙 명세는 대상 문서의 타입에 관계없이 동일한 의미를 가진다. 권한부여 규칙 명세는 앞에서 설명된 권한부여를 위해 확장된 정보 집합과 유사하다. 다음 그림에서 권한부여 규칙이 명시된 예를 보여주고 있다

```
<Base Authorization Policy>
<Rule 1>
<BAP BasePolicy = "+" BaseSubjectFile="SubjectList. XML>
<Rule 2>
<rule access = "grant" object="sample01" subject = "gauss">
<Rule 3>
<rule access = "deny" object="contract[@name]" subject = "gauss">
<Rule 4>
<rule access = "grant" object="products/price" subject = "BYH">
</Base Authorization Policy>
```

그림 3. 권한부여 규칙

그림의 첫 번째 엘리먼트는 기본정책의 적용여부를 결정한다. 만약 특정 사용자 A가 X라는 문서에 대한 어떠한 다른 정책도 설정되지 않았다면 이는 A가 X에 접근할 수 있음을 의미한다. 반대로 BasePolicy가 "-"로 설정되어 있다면 A는 X라는 문서에 접근할 수 없게 된다. 그림의 규칙1은 SubjectList에 등록된 모든 사용자가 모든 문서에 접근할 수 있음을 나타낸다. 규칙2는 gauss라는 사용자가 sample01이라는 문서에 접근할 수 있음을 나타낸다. 규칙3에서는 gauss라는 사용자가 contract 문서의 name 필드를 볼 수 없음을 나타낸다. 규칙4는 BYH라는 사용자가 products문서의 price 필드를 검색할 수 있도록 한다.

권한부여 규칙은 그림 3에 보이는 것뿐만 아니라, 필요에 따라 정책관리자에 의해 추가 될 수도 있으며 이전에 설정된 규칙 또한 삭제 될 수 있다.

XML 문서에 대한 접근이 허용된 사용자는 권한별로 문서에 대한 읽기, 쓰기, 새로운 문서의 생성 및 삭제 작업을 수행 할 수 있다. 문서에 대한 쓰기, 생성, 삭제 작업은 해당 사용자가 제출한 초기 정보를 바탕으로 접근제어 서버 측에서 권한부여 서버 측으로 확장된 정보가 전달되어 문서에 대한 권한과 사용자에게 부여된 권한이 일치할 때 가능하게 된다. 표 2는 사용자에게 부여되는 동작 및 각 동작에 대한 의미를 나타낸다.

표 1. 사용자에 의해 실행 가능한 동작 및 의미

읽기(read)	권한부여 정보로부터 검색되어 연결되는 대상 객체(태그, 텍스트, 컨텐츠, 속성타입/값 쌍)를 포함하는 권한부여 결과를 검색
쓰기(write)	권한 부여 요청에 명시된 매개변수를 포함한, 권한 부여 정보에 저장된 정보에 따라 대상 객체의 내용을 수정
생성(create)	권한 부여 요청에 명시된 매개변수를 포함한, 권한 부여 정보에 저장된 정보에 따라 새로운 구조의 문서를 생성
삭제(delete)	권한 부여 정보에 저장된 정보에 따라 대상 문서를 삭제

3.3 제안된 접근제어 메커니즘의 전체적인 구성 및 흐름

제안된 접근제어 메커니즘은 사용자(subject), 접근제어 서버, 권한부여 서버, XML 문서(object)로 구성된다. 권한부여 서버는 권한 부여에 필요한 별도의 권한부여 규칙(Authorization Rule)을 ARS(Authorization Rule Sheet)에 작성하여 저장하고 있다. 사용자는 3.1절에서 언급된 바와 같이 주체의 접근 요구를 위한 초기 정보의 구성하여 접근제어 서버에 제출함으로 이루어진다. 제출된 정보는 접근제어 서버에 의해 인증서의 유효성과 권한을 검색하여 확장된 형태로 권한부여 서버에게 전달하게 된다. 권한부여 서버는 접근제어 서버로부터 전송된 정보를 접

근 제어 규칙과 비교하여 대상 문서에 대한 접근 허용 여부, 읽기, 쓰기, 새로운 문서의 생성 및 삭제를 위한 문서 요청 정보를 생성하여 대상객체에 적용하고, 그 결과를 사용자에게 반환함으로서 사용자의 요청을 처리한다.

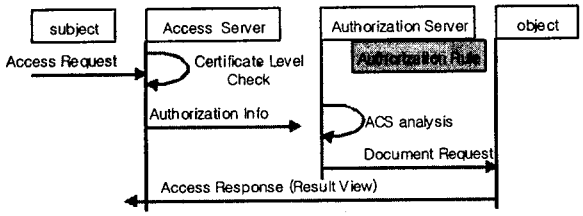

그림 4. 제안된 접근제어 메커니즘의 구성 및 흐름

3.4 XACML

XACML은 앞절에서 설명한 권한부여 모델을 바탕으로 하는 접근제어 언어이다. 여기서는 XACML의 문법과 의미를 간략하게 기술한다. 특히, 식별자 <policy>를 가지는 element를 정의한다. 기본적인 목적은 보안정책 프로그래머가 XML에서 유연성 있는 권한부여 정책을 작성할 수 있도록 하는 것이다. 정책 명세를 XML로 하는 또 다른 장점은 XACML 언어가 정책관리 권한부여 규칙을 쉽게 구현할 수 있다는 것이다. 다시 말해서, 권한부여 정책상에서의 권한부여 규칙 자체는 XACML에서 명시된 것과 같은 메타-규칙(meta-rule)에 의해 정의되어질 수 있다. XACML로 작성된 정책 집합을 대상 문서와 연결하는 방법(여기서는 이런 방법에 대해서는 별도로 명시하지 않는다)은 스키마(또는 DTD)를 정의하는 방법과 각각의 특정의 문서에 대한 정의하는 방법이 존재한다. 전자의 접근방법은 정책 집합이 DTD에 일치하는 유효한 모든 문서를 범위로 한다. 따라서 특정 DTD와 연관된 정책을 연결하기 위한 방법이 필요하다. 후자의 접근방법은 각각의 특정문서에 포함되게 된다. 이 경우에는 연결되는 정책이 <policy> 엘리먼트로 구성되어 정책이 적용될 문서에 하나의 요소로서 포함되게 된다. 본 논문에서 제안된 접근제어 메커니즘은 후자의 방법을 사용하여 정책을 적용한다.

3.5 제안된 메커니즘의 장점 및 특징

제안된 접근제어 방식은 접근 제어를 수행하기 전에 사용자에게 발급된 인증서의 권한정보를 분석하여 해당 사용자의 권한에 따라 서버 측에서 확장된 권한 정보를 재구성하여 Target Document를 관리하는 실행 모듈에게 해당 문서를 재구성 하여 반환하도록 하는 방법을 사용하였다. 따라서 기존에 제안된 다른 접근 방법에 비해 사용자의 권한을 부여하기 위해 추가적인 접근 제어 규칙이 요구되지 않으며, 또한 사용자가 요청한 문서에 대한 원본을 그대로 제공하는 것이 아니라, 결정된 권한에 일치하는 *ACS(Access Control Sheet)* 정보에 의해 재구성된 문서가 제공되므로 보다 안정된 접근제어 서비스가 가능하다.

XML 원본 문서를 관리하는 관리자나 XML 문서에 대한 원소유주의 관점에서는 XML 문서에 접근하는 사용자의 신분을 접근 초기에 제출하는 인증서의 유효성 및 필요에 따라 전자서명을 검증하는 과정을 거침으로서 부인방지의 효과 및 원본 문서에 대한 불법적인 변경을 검증 및 추적할 수 있는 효율성을 가질 수 있다.

5. 결론 및 향후 연구 방향

본 논문에서는 최근 그 필요성이 크게 인식되고 있는 XML 문서에 대한 보호 방안을 접근제어 기법을 적용하여 해결하고자 인증서를 이용하여 사용자의 등급을 부여하고 그에 따른 접근권한을 부여하는 메커니즘을 제안하였다. 본 논문에서 제안된 방식은 일반적인 자원 또는 HTML 문서에 적용되는 접근 방법과 달리 XML 문서가 가지는 구조적 특성을 충분히 활용하여 XML 문서의 각 element 레벨까지 소유주의 보호 권한(protection privilege)을 만족하면서, 적절한 사용권한을 가진 사용자에게 해당 XML 문서에 대한 접근과 변경을 수행하는 방식으로 처리되도록 하였다.

향후 추가적으로 연구되어야 할 부분은 다음과 같이 요약된다. 먼저 권한부여 규칙들에 대한 보다 세밀한 정의가 이루어져야 한다. 또한 각 서버에서 정보 추출 및 정보 재구성에 필요한 XPath[14]및 XACML 언어에 대한 추가적인 연구가 필요하다.

참고문헌

[1] W3C. "Extensible Markup Language (XML) 1.0". World Wide Web Consortium(W3C). http://www.w3c.org/TR/REC-xml (October 2000).

[2] W3C. "XML-Signature Syntax and Processing". W3C Recommendation http://www.w3c.org/TR/xmldsig-core(February 2002)

[3] W3C. "XML Encryption Syntax and Processing". W3C Recommendation. http://www.w3.org/TR/xmlenc-core(December 2002)

[4] C. Ilioudis, G. Pangalos and A. Vakal-i, "Security Model or XML data".Proceedings of the 2nd International Conference on Internet Computing, 2001

[5] www.oasis-open.org. "OASIS eXtensible Access Control Markup Language (XACML) Committee Specification 1.0", November 2002

[6] E. Damiani, S. D. C di Vimercati, S. Paraboschi, P. Samarati. "A fine-grained access control system for XML documents", ACM Transaction on Information and System Security, Vol.05 No.02 169-202, 2002.

[7] E. Damiani, S. D. C di Vimercati, S. Paraboschi, P. Samarati, "Controlling access to xml documents" IEEE Internet Computing 5(6):18-28, November 2001.

[8] Ravi Sandhu, Pierangela Samarati, "Access Control: Principles and Practice", IEEE Communications Magazine. 1994 Feb.

[9] Bertino, Castano, Ferrari, Mesiti. "Controlled Access and Dissemination of XML Document". WIDM 1999.

[10] E. Damiani, S. De Capitani di Vimera-cati, S. Paraboschi and P. Samarati, "Securing XML documents". In proc. of EDBT 2000, Germany. Springer Verlag, in LNCS 1777, 2000

[11] Gerome Miklau and Dna Suciu, "Cryptographically Enforced Conditional Access for XML". Fifth International Workshop on the Web and Databases (WebDB 2002). 2002

[12] M. Kudo and S. Hada. "XML Document Security based on Provisional Authorization",Proceedings of the 7th ACM conference on Computer and communications security. November, 2000.

[13] H. He and R.K. Wong , "A role-based access control model for XML repositories" , Procs. 1st Int. conf. on W-eb Info. Syst. Eng., WISE'00, Hong Kong, 2000.

[14] James Clark, Steve DeRose, "XML Path Language (XPath) Version 1.0" http://www.w3.org/TR/xpath. 1999.11