XML의 주체 기반 암호화를 이용한 콘텐츠 패키지의 접근 제어

Access Control of Content Package by Using XML Subject-based Encryption

조광문
목포대학교 전자상거래학 전공
Kwang-Moon Cho(ckmoon@mokpo.ac.kr)

요약

XML 문서가 웹 문서의 표준으로 자리 잡음에 따라 많은 정보들이 XML 문서 형식으로 표현되면서 XML 문서의 보안에 관한 요구도 커지고 있다. 현재까지의 XML 보안에 관한 연구는 암호화와 전자 서명 같은 통신상의 보안에 관한 연구가 중심이 되었으나 XML 문서가 방대해지고 복잡해짐에 따라 XML 문서에 대한 통신상의 보안뿐 아니라 관리적인 보안이 필요하게 되었다. 하지만 XML 문서의 암호화는 단순한 통신상의 보안만을 제공할 뿐 관리적 보안 요소인 다양한 사용자와 다양한 접근 권한 정책을 반영하지 못하고 있다.

본 논문에서는 XML 문서의 보안을 위해 주체별 권한 정책을 반영한 접근 제어를 보장하는 주체 기반 XML 문서의 암호화 기법을 제안한다. 접근 제어를 보장하는 암호화를 수행함으로써 다양한 사용자의 다양한 권한 정책을 반영할 수 있다.

■ 중심어 : | 주체 기반 암호화 | 콘텐츠 패키지 | 접근 제어 |

Abstract

As a large quantity of information is represented in XML format on the web, there are increasing demands for XML security. Until now research on XML security has been focused on the security of data network using digital signature and encryption technology. As XML data become extensive and complex, however, XML security comes to involve not only network security but also managerial security. But XML encryption support only simple network security. So it cannot support multiple users and multiple access control policy.

In this paper, we propose an integration method of encryption and access control policy for securing XML documents. This methodology can support multiple authorization of multiple users with integrating access control.

■ keyword : | Subject-based Encryption | Content Package | Access Control |

* 이 논문은 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(R05-2004-000-10867-0)

접수번호 : #051114-004
접수일자 : 2005년 11월 14일
심사완료일 : 2005년 12월 13일
교신저자 : 조광문, e-mail : ckmoon@mokpo.ac.kr

I. 서 론

XML은 웹 환경에서 데이터를 표현하기 위한 마크업 언어이다. 이러한 XM은 SGML에서의 복잡성을 제거하고, HTML에서의 고정된 태그의 한계에서 벗어나 사용자가 문서 구조를 정의할 수 있다[1][2]. 이와 같은 장점 때문에 W3C에서는 XML을 웹 데이터의 표준으로 제정했다. XML의 표준화 이후 많은 데이터가 XML로 표현되기 시작했고, 현재는 웹 상에 정부나 기업 등의 다양한 XML 데이터가 존재하고 있다. 웹 상에 존재하는 XML 문서의 정보는 네트워크를 통해 분산되고 공유되므로 XML 문서 정보의 유출을 막기 위한 기밀성 보장이 매우 중요한 보안의 요구 사항으로 자리잡게 되었다. 기밀성의 보장은 많은 응용에서 중요한 부분이다[3].

본 논문은 암호화와 접근 제어를 통합함으로써 전송 계층 상의 보안뿐만 아니라 사용자의 차별적 접근을 허용하는 관리상의 보안 요구 사항을 만족시키고자 한다. 암호화에 접근 제어 정책을 반영하는 방법은 문서에 모든 권한을 반영하여 주체에 따른 접근 권한에 따라 같은 주체에게 허용된 문서의 부분들을 하나의 키로 암호화한다. 이렇게 주체 기반 암호화를 수행하게 되면 기존의 노드 단위 암호화로 발생했던 문제점인 키의 생성과 암호화 회수를 단축할 수 있다. 또한 권한의 평가가 사용자가 요청한 후에 이루어지는 것이 아니고 암호화 수행 과정에서 이루어지므로 기존 접근 제어의 복잡하고 반복적으로 수행되었던 권한 평가의 비용을 줄일 수 있다.

II. 관련 연구

XML 문서의 보안은 암호화, 전자 서명, 키 관리, 접근 제어 등에 관해 연구되고 있다. XML의 보안은 통신상의 보안 관점의 암호화뿐만 아니라 관리적 보안인 접근 제어도 함께 이루어져야 한다.

XML 문서의 암호화에 관하여 먼저 살펴본 후, XML 문서의 접근 제어에 대하여 분석한다.

1. W3C XML Encryption

W3C의 XML 암호화[4]는 다양한 단위의 암호화를 제공한다. 다음은 XML의 암호화 단위를 나타낸다.

- XML 문서 전체
- XML 문서에 포함된 단일 엘리먼트(와 그들의 하위 엘리먼트와 애트리뷰트)
- XML 문서에 포함된 엘리먼트의 값(과 그들의 하위 노드의 일부 또는 전체 노드)
- XML 문서 외부의 이진 값

XML 암호화는 XML 문서 전체뿐만 아니라 엘리먼트나 애트리뷰트, 문서의 엘리먼트와 애트리뷰트의 집합 단위도 제공함으로써 다양한 단위의 암호화를 제공한다.

또한 XML 암호화는 다양한 사용자를 위한 암호화 방법을 몇 가지 제공한다. 가장 간단한 방법은 모든 사용자에게 XML 문서의 동일한 부분을 볼 수 있도록 허용하는 것이다. 이 경우 값은 한번만 암호화되고, 그 키는 각각의 사용자를 위해 다시 암호화된다. 다양한 사용자를 위한 암호화의 다른 방법은 이미 암호화된 값을 다시 암호화하는 방법이 있다. 이 방법은 모든 사용자에게 제공되는 문서의 내용이 동일하지 않은 경우에 사용한다.

[그림 1]은 슈퍼 암호화를 그림으로 나타낸 것이다. 사용자 A와 사용자 B의 권한이 다른 경우에 암호화된 문서에 또 다른 암호화를 수행하여 사용자에 따라 문서를 처리할 수 있는 범위가 달라진다.

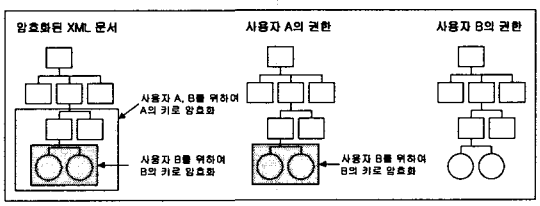

그림 1. 슈퍼 암호화

2. XML 문서의 접근 제어

XML 문서의 접근 제어는 기존의 웹 기반 문서들의 접근 제어 모델과는 다른 많은 특징이 반영되어야 한다. 기존의 웹 기반의 접근 제어 모델들은 파일 단위나 파일

의 부분에 권한을 기술하는 것이 가능하다. 그러나 이런 방법은 XML 문서의 큰 특징인 정보의 의미에 따른 처리를 위한 정보의 의미에 기반한 접근과 엘리먼트와 같은 아주 작은 단위의 접근이 불가능하다. 그러므로 XML 문서의 접근 제어 모델은 문서의 집합이나 하나의 엘리먼트 등의 다양한 레벨에서의 접근 제어를 지원해야 한다[5].

XML DOM 트리는 XML 문서의 엘리먼트에 접근할 수 있는 API를 제공한다. [5]에서 제안하는 접근 제어 모델은 이러한 DOM 트리를 이용하여 XML 문서와 DTD의 엘리먼트에 접근 권한을 설정하고, 설정된 접근 권한 정보에 의해 사용자의 XML 문서 접근을 제어한다. 이 모델의 접근 권한 정보는 다음과 같은 다섯 가지 구성요소를 사용하여 명시하고 있다.

- subject : 사용자 이름 또는 IP 주소 또는 컴퓨터 이름
- object : xPath 1.0
- action : read
- sign : +/-
- type : LDH, RDH, L, R, LD, RD, LS, RS

subject는 XML 문서에 접근하는 주체이다. 이들의 주체는 사용자의 그룹과 패턴을 지원한다. object는 XML 문서의 엘리먼트이며, 이는 xPath를 이용하여 구별할 수 있다. action은 인가된 주체가 수행할 수 있는 연산이고, sign은 권한의 허가 혹은 거부에 대한 표현이다. type은 권한의 속성 값이다. 권한의 전파 여부를 결정하는 R(recursive)과 L(local), 권한 충돌 시 우선순위를 결정하는 H(hard)와 S(soft), 그리고 DTD를 의미하는 D의 조합으로 type 값이 구성된다.

[그림 2]는 XML 문서의 접근 제어 수행 과정을 보여준다. 이 접근 제어 과정을 통해 사용자는 XML 문서 중에서 자신이 볼 수 있는 권한이 있는 부분만을 접근하게 되므로, 비인증된 사용자로부터 데이터의 기밀성을 보장할 수 있다.

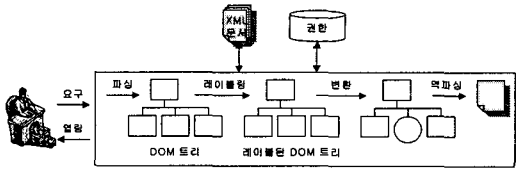

그림 2. XML 문서의 접근 제어 수행 과정

3. 슈퍼 암호화의 문제점

[그림 1]에 나타난 슈퍼 암호화는 몇 가지 한계점을 지니고 있다. B는 자신에게 권한이 있는 모든 정보를 보기 위해서는 반드시 A의 키를 가져야 한다. 하지만 A에게 허용된 권한 중에 B에게 제공해서는 안되는 정보가 존재할 경우 B는 A의 키도 가지므로 이 정보까지 접근이 가능하다. 또한, A는 자신의 키로 복호화를 수행한 경우 복호화되지 않는 부분이 존재하는 것을 알고 비밀 정보가 존재함을 알게 된다. 또한 복호화되지 않는 부분을 볼 수 있는 사용자가 존재하는 것이므로 자신보다 권한이 많은 사용자가 있음을 알게 된다. 사용자 B는 복호화를 수행한 뒤 모든 문서를 자신이 볼 수 있으므로 자신이 이 문서에 대한 최고 권한이 있는 사용자임을 알게 된다. 또한 내부 암호화된 부분이 존재하는 것을 알고 다른 사용자는 내부 암호화된 부분의 내용을 볼 수 없다는 것을 알게 된다. 이처럼 XML 암호화는 다양한 종류의 정보의 유출이 존재한다. 이는 암호화의 수행시 권한과 사용자에 대한 고려를 하지 않았기 때문에 발생하는 문제이다.

또한 XML 문서에 대한 접근 제어에 있어서 전체의 DOM 트리가 메모리 상에 적재되어야 하고, DOM 트리의 모든 노드에 접근 권한을 설정하기 위한 반복적인 트리의 검색으로 많은 메모리가 사용되며, 복잡한 권한의 평가 과정으로 인해 시스템의 성능 저하를 초래할 수 있는 문제점이 있다. 또한, 메모리의 DOM 트리에서 기밀 정보를 포함한 모든 문서 전체를 처리하기 때문에 data diddling 문제가 발생할 수 있고 네트워크를 통해 기밀 정보가 포함된 문서를 전달하므로 packet sniffing과 같은 정보의 유출 문제가 발생할 수 있다.

III. XML 암호화를 통한 접근 제어

1. 사용자 주체 기반 암호화 구조

[그림 3]은 본 논문에서 제안한 사용자 주체 기반 암호화를 통한 XML 접근 제어 구조이다.

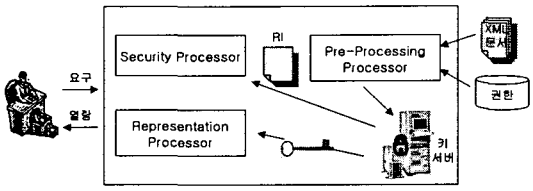

그림 3. 사용자 주체 기반 암호화 기법의 구조

접근 제어는 인증을 거친 사용자가 원하는 자원을 요청하면 시스템은 사용자의 권한을 확인하고 요청한 자료를 제공할 것이지 아닌지를 결정하게 된다.

문서가 생성되면 전처리기(pre-processing processor)에 의해 전처리 과정이 수행된다. 전처리 과정은 XML 문서와 권한 데이터베이스를 이용하여 대체 정보(RI: replacement information)를 생성하고, 문서를 암호화하여 저장하고, 생성된 키를 키 서버(key server)에 전달한다. 사용자는 시스템에 인증을 거친 후 역할을 할당받게 된다. 인증된 사용자가 문서를 요청하면 보안 처리기(security processor)에 의해 대체 정보를 확인하게 된다. 사용자에게 허용된 권한이 존재하면 표현 처리기(representation processor)는 대체 정보와 암호화된 문서 중 권한이 있는 부분에 대하여 키 서버에서 역할에 해당하는 키 집합을 받아 사용자에게 전달할 문서로 재구성한다. 구성된 문서는 사용자에게 전달되고 사용자는 복호화하여 자신에게 권한이 존재하는 문서의 부분만을 볼 수 있게 된다.

2. 디지털 콘텐츠 패키징 방법

디지털 콘텐츠를 패키징하는 것은 결국 콘텐츠를 구성하고 있는 메타데이터를 패키징하는 것이다. 메타데이터를 구성하는 방안을 크게 3가지로 구분할 수 있다.

- 모든 참여자의 메타데이터를 하나로 구성(정적 메타데이터)
- 메타데이터를 공통 영역과 특정 영역으로 나누어서 구성(동적 메타데이터)
- 각 참여자의 전체 메타데이터를 계층적으로 첨부(계층 메타데이터)

정적 메타데이터는 디지털 콘텐츠의 유통에 관여한 모든 참여자들의 메타데이터를 하나로 구성하는 방법으로서 정적(static)인 형태를 갖는다. 이 방법은 각 참여자의 가능한 요소(element)를 모두 표현할 수 있고, 모든 요소들을 하나의 구조에 표현함으로써 구조가 단순하여 유통 단계가 간단할 경우에 효과적이다. 그러나 메타데이터의 크기에 따른 낭비가 발생할 수 있고, 유통 환경의 변화에 따른 유연성이 부족하며 복합 콘텐츠, 패키징 서비스에 문제가 있을 수 있다. 또한 모든 참여자의 정보가 노출됨으로써 보안 문제가 발생할 가능성도 있다.

동적 메타데이터는 디지털 콘텐츠의 메타데이터를 공통 영역과 특정 영역으로 구분하여 구성하는 방법으로서 동적(dynamic)인 형태를 갖는다. 이 방법에서는 유통에 관련된 각 참여자의 요소 중 공통 부분과 서로 다른 부분을 나누어 구성함으로써 메타데이터의 크기가 작아질 수 있고, 개방 가능한 데이터와 보안이 필요한 데이터를 분리할 수 있다. 또한 유통 흐름의 추적이 용이하고 유통 환경의 변화에 따른 유연성을 가질 수 있지만, 구현이 복잡해진다.

계층 메타데이터는 유통의 흐름 상에서 각 참여자가 디지털 콘텐츠의 메타데이터를 첨부해 나가는 형식으로 구성하는 방법이다. 이 방법은 유통 단계별로 각 참여자가 정보를 추가함으로써 유통 흐름의 추적이 용이하고 보안에 강점을 갖는다. 유통 환경의 변화에 따른 유연성이 부족하고 각 참여자별로 메타데이터 분석 프로그램이 필요하다.

3. 디지털 콘텐츠 패키지에의 적용

III.1절에서 제시한 과정을 패키지화된 디지털 콘텐츠에 적용할 수 있다. 패키징된 디지털 콘텐츠의 각 구성 콘텐츠에 서로 다른 사용자가 자신만의 권한으로 접근

하여 이용할 수 있는 것이다. [그림 4]는 제안하는 암호화 기법의 수행 과정을 나타낸다.

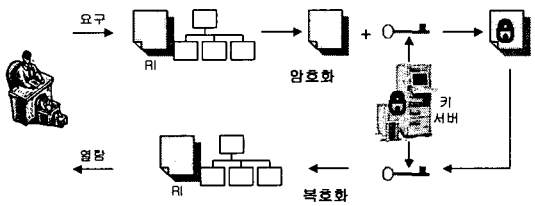

그림 4. 암호화 기법의 수행 과정

사용자는 인증 과정을 거친 후 역할을 할당받아 문서를 요청하게 된다. 시스템은 사용자의 역할을 바탕으로 대체 정보를 확인하게 된다. 대체 정보를 확인하여 사용자의 역할에 해당하는 암호화된 문서의 부분과 키를 제공받아 재구성하여 사용자에게 전달하게 된다. 사용자는 전달받은 문서를 해당 키로 복호화하면 자신에게 접근이 허용되는 문서의 부분만을 볼 수 있게 된다.

전처리 과정의 수행은 다음의 단계로 구성된다.

① 초기 레이블링(initial labeling) 단계 : 접근 권한을 바탕으로 XML 문서의 각 노드에 사용자 주체 각각에 대한 접근 허용, 거부를 표기한다.

② 충돌 해결(conflict resolution) 단계 : 동일 주체에 대해 허용과 거부가 모두 존재하는 경우 충돌 해결 원리에 따라 하나의 접근 권한만을 결정한다.

③ 그룹핑(grouping) 단계 : 레이블을 바탕으로 동일 레이블이 존재하는 노드들의 그룹화를 수행한다.

④ 대체 정보 생성(replacement information creation) 단계 : 그룹화된 노드별로 주체와 객체, 접근 권한, 암호화 아이디 등의 권한 정보를 대체 정보로 생성한다.

⑤ 암호화(encryption) 단계 : 대체 정보를 바탕으로 그룹화된 노드들의 주체의 키로 암호화한다.

전처리 과정의 수행 후 인증을 거친 사용자가 해당 XML 문서를 요청하게 되면 다음과 같은 과정이 수행된다.

① 대체 정보 확인 단계 : 사용자의 역할을 바탕으로 해당 문서에 접근 권한이 존재하는지 대체 정보를 확인한다.

② 문서의 재구성 단계 : 만약 사용자에게 권한이 존재하면 수정된 대체 정보와 사용자에게 허용되는 암호화된 문서, 이를 복호화할 수 있는 주체의 키 집합을 재구성하여 사용자에게 전달한다.

③ 복호화 단계 : 사용자는 재구성된 문서를 복호화하여 자신에게 접근 권한이 존재하는 문서의 부분만을 접근하게 된다.

Ⅳ. 결 론

최근 멀티미디어와 모바일 환경의 급속한 확산으로 인하여 디지털 콘텐츠에 대한 저작권 침해 소송이 잇따르고, 이에 따라 디지털 콘텐츠 저작권 문제에 관심이 높아지고 있다. 저작권과 더불어 사용자의 사용 권한에 대한 관리와 감시가 필요한 실정이다. 이러한 환경에서 사용자에 기반한 데이터 접근 제어 방법이 필요하게 된다.

이에 본 연구에서는 암호화와 접근 제어를 통합함으로써 전송 계층상의 보안뿐만 아니라 사용자의 차별적 접근을 허용하는 관리상의 보안 요구 사항을 만족시키고자 한다. 암호화에 접근 제어 정책을 반영하는 방법은 문서에 모든 권한을 반영하여 주체에 따른 접근 권한에 따라 같은 주체에게 허용된 문서의 부분들을 하나의 키로 암호화한다. 이렇게 주체 기반 암호화를 수행하게 되면 기존의 노드 단위 암호화로 발생했던 문제점인 키의 생성과 암호화 회수를 단축할 수 있다. 또한 권한의 평가가 사용자가 요청한 후에 이루어지는 것이 아니라 암호화 수행 과정에서 이루어지므로 기존의 접근 제어의 복잡하고 반복적으로 수행되었던 권한 평가의 비용을 줄일 수 있다. 향후 본 논문에서 제안한 내용을 모바일 콘텐츠 유통 프레임워크 상에서 적용 가능한 프로토타입으로 설계하고 구현하고자 한다.

참 고 문 헌

[1] M. Bartel, J. Boyer, B. Fox, B. LaMacchia, and E. Simon, "XML-Signature Syntax and Processing," W3C Recommendation, Feb., 2002.

[2] XML Key Management Specification (XKMS) Version 2.0, W3C Working Draft, Apr., 2003.

[3] 조광문, 전자상거래를 위한 XML 메시지 처리기 설계, 한국콘텐츠학회논문지, 제4권, 제3호, pp.13-19, 2004(9).

[4] T. Imamura, B. Dillaway, and E. Simon, "XML Encryption Syntax and Processing," W3C Recommendation, Dec., 2002.

[5] E.Damiani, S.Vimercati, S.Paraboschi, and P.Samarati, "Securing XML Documents," Proceedings of the 2000 International Conference on Extending Database Technology(EDBT2000), Konstanz, Germany, Mar., 2000.

[6] S. Godik and T. Moses, et el, "eXtensible Access Control Markup Language(XACML) Version 1.0," OASIS Standard, Feb., 2003.

[7] C. Geuer-Pollmann, "XML Pool Encryption," Workshop On Xml Security Proceedings of the 2002 ACM workshop on XML security, Nov., 2002.

[8] E. Bertino and E. Ferrari, "Secure and Selective Dissemination of XML Documents," ACM Transaction on Information and System Security, Vol.5, No.3, pp.290-331, Aug., 2002.

[9] M, Kudo and S. Hada, "XML Document Security based on Provisional Authentication," Proceedings of the 7th ACM Conference on Computer and Communications Security, Nov., 2000.

저 자 소 개

조 광 문(Kwang-Moon Cho) 종신회원

- 1988년 2월: 고려대학교 컴퓨터학과(이학사)
- 1991년 8월: 고려대학교 컴퓨터학과(이학석사)
- 1995년 8월: 고려대학교 컴퓨터학과(이학박사)
- 1995년 9월~2000년 2월: 삼성전자 통신연구소 선임연구원
- 2000년 3월~2005년 2월: 천안대학교 정보통신학부 조교수
- 2005년 3월~현재: 목포대학교 전자상거래학 전공 전임강사

<관심분야> : 전자상거래, 콘텐츠 유통, 모바일 콘텐츠, 데이터베이스, 그리드 컴퓨팅