XML 스키마를 이용한 암호화된 XML 문서 유효성 검증

홍성표* · 이 준**

The Validity Verification of Encrypted XML Document using the XML Schema

Seong-pyo Hong* · Joon Lee**

이 논문은 2002년도 조선대학교 학술 연구비를 지원 받았음

요 약

XML은 문서의 데이터 포맷 표현을 향상시키는데 중점을 두고 만들어졌기 때문에 문서 변조 및 데이터 삭제 등의 공격에 취약한 문제점을 가지고 있다. 이러한 문제점에 대한 해결책으로 XML Signature, XML Encryption, XML 접근 제어와 같은 다양한 해결책이 제시되었지만 XML 암호화로 인한 구조적인 XML 유효성 위반 문제 및 DTD 공격에 대한 해결책 부재 등의 문제점이 해결되지 않고 있다.

본 논문에서는 유효성과 암호화를 동시에 만족시켜줄 수 있는 방법으로 XML 스키마를 이용하는 방법을 제안하였다. XML 스키마는 정형 XML 문서에 대해서도 지원이 가능하며, XML 문서에 대한 메타 정보를 담고 있으므로 따로 DTD를 필요로 하지 않는다. 또한 각각의 XML 문서에 대하여 동적인 생성이 가능하며 자체 유효성 검사 규칙을 가지고 있으므로 DTD 기반 XML 문서의 암호화에 대한 확장성이 뛰어난 장점을 가지고 있다.

ABSTRACT

XML has weakness problems on document modulation and elimination of data Because of the XML gives priority to present data format, XML signature, XML encryption, or XML access control is provided to overcome those weakness problems. However, structured XML efficiency contravention problem occurred from XML encryption and absence of protection from DTD attack are still remains unsolved.

In this paper, we suggests the XML schema that satisfies both validity and encryption. The DTD is unnecessary because XML schema supports Well-Formed XML documents and include meta information. Also XML schema has possibility to generate each XML document dynamically and because of self efficiency investigator rule, it has an advantage on extendability of DTD based encryption of XML documents.

키워드

Security, Digital Signature, XML Schema, XML Security

*조선대학교 대학원 컴퓨터공학과

**조선대학교 전자정보공과대학 컴퓨터공학부

접수일자 : 2003. 4. 17

I. 서 론

XML 기술의 유용함이 인식되기 시작하면서 다양한 분야에서 XML 기술을 적용하고 있다. 그러나, XML 문서는 타인에 의해 쉽게 조작되거나 오용될 수 있는 문제점을 가지고 있기 때문에 XML 제반기술의 발달과 함께 XML상의 보안을 제공해주는 대표적인 기술인 XML Encryption과 XML Signature 관련 기술 또한 연구가 빠르게 진행되고 있다.

XML Encryption에서 XML 문서를 효과적으로 암호화하기 위해서는 기본적으로 XML 문서의 유효성을 유지시켜 주어야 한다. 그러나, 어떤 XML 문서도 암호화 후에는 정형 XML 문서가 된다. 이는 암호화에 관련된 태그를 암호화 이전에 작성된 XML 문서의 기반이 되는 DTD에서 지원해주지 못하기 때문이다. 즉, XML 문서의 유효성을 유지시키면서 암호화를 수행하기 위해서는 DTD를 기반으로 한 XML 문서의 경우 DTD 자체가 새롭게 정의 되어야하는 해결되기 어려운 단점을 갖는다. 일부 태그가 암호화로 대체되면 전체 DTD가 새롭게 바뀌어야만 유효한 XML 문서로 검증될 수 있다. 뿐만 아니라, DTD는 확장성이 떨어지며, 데이터로서 XML을 제대로 기술하기 어렵고 네임스페이스를 제대로 지원하지 못하는 등 여러 가지 제한 사항을 가지고 있어 DTD에 기반한 XML 문서의 암호화가 유효성을 유지하는데 많은 어려움이 따른다.[1][2][4]

본 논문에서는 유효성과 암호화를 동시에 만족시켜줄 수 있는 방법으로 XML 스키마를 이용하는 방법을 제안한다. XML 스키마는 정형 XML 문서에 대해서도 지원이 가능하며, XML 문서에 대한 메타 정보를 담고 있으므로 따로 DTD를 필요로 하지 않는다.

II. XML 보안 기술

XML은 전자상거래에 관련된 데이터 교환이 인터넷상에서 쉽고 원활하게 이루어질 수 있도록 하는 어플리케이션에 적합하다. 인터넷은 불특정 다수를 위한 네트워크로 보안상의 취약점을 지니고 있으며, XML은 문서의 데이터 포맷 표현을 향상시키는 데에 중점을 두고 만들어진 것이기 때문에 문서 변조 및 데이터 삭제 등의 공격에 노출되어 있다. 인터넷 상에서 XML의 비중이 높아짐에 따라 XML 보안은 과거 웹 보안의 일부분에서 독립하여 새로운 분야로 분류되었다.[3][5]

1. XML 암호화 기법

XSS1999[3]와 Imamura2000[1] 및 Brandt2000[2] 등에서 제시한 XML 암호화 기법은 기존의 암호화 기법을 XML에 적용시킨 방법으로, XML 문서 전체의 암호화 기법으로 시작하였으며, 속도 문제의 단점이 지적되어 현재는 엘리먼트 단위로 암호화를 수행하는 향상된 기법이 제안되었다.

Imamura2000은 엘리먼트 암호화를 위한 엘리먼트를 정의하고 있다. 이 정의된 엘리먼트들을 기반으로 하여 XMl 문서에서 암호화가 요구되는 엘리먼트에 대해 암호화를 수행한다. 이 방법은 불필요한 암호화 연산을 하지 않으므로 속도 및 비용면에서 효과적인 반면, DTD 선언(!DOCTYPE...>)이 포함된 XML 문서, 즉 유효한 문서를 처리해주지 못한다. 이는 암호화 과정에서 암호화를 위한 엘리먼트가 문서에 새롭게 추가되지만, 암호화 이전 문서의 DTD에서는 이를 지원하지 않으며, XML 문서는 하나의 DTD를 기반으로 작성되므로 기존 DTD와 새롭게 작성된 DTD를 동시에 인식할 수 없기 때문이다.[6][7]

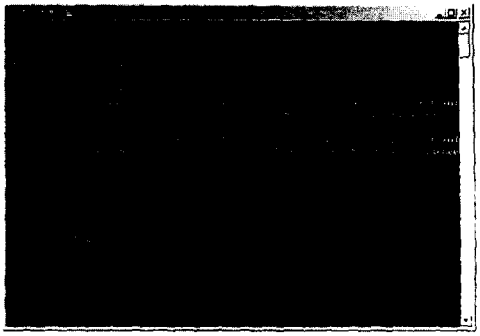
한편, Brandt2000은 여러 계층에 대한 암호화 방식을 제안하였다. 첫째, 암호화하고자 하는 엘리먼트를 secure 엘리먼트로 대체하고, 데이터도 암호화한다. 이 방법은 효과적인 암호화는 가능하지만 모든 암호화 정보가 <secure> 태그로만 설정됨으로써 동일한 태그로 설정된 데이터의 충돌 문제가 발생할 수 있다. 이를 위한 개선 방법으로 태그는 그대로 두고 데이터만 암호화하는 방법을 제안하였다. 둘째, 엘리먼트는 그대로 두고 데이터만 암호화하는 방법이다. 이것은 DTD 내의 엘리먼트 선언에서 불리언 타입의 보안 속성을 설정하여, "참"일 경우 데이터를 암호화하는 방법이다. 이 방법은 데이터만 암호화가 가능한 장점이 있으

나, DTD 속성에는 불리언 타입이 정의되어 있지 않으므로 DTD 문법을 위반하는 문제점이 있다.

셋째, XML 스타일 시트를 이용하는 방법이다. 스타일 시트가 XML 문서와 분리되어 있는 특성을 이용한 것으로, 기존 문서를 보존하는 상태에서 스타일 시트 형식의 시큐리티 시트를 이용하여 암호화된 형태로 만드는 방법이다. 이 방법은 XML 문서 및 DTD와 XML 스키마까지도 암호화가 가능하다고 한다. 그러나 현재 검증된 결과가 없고 오히려 암호화를 위해 특정 내용을 분리시키는 컴포넌트(component)없이는 암호화가 불가능하며, 암호화 수행 후 DTD를 새로 작성해야 하지만 이를 지원하지 못하는 단점이 있다.[2][7][8]

결론적으로, Imamura2000과 Brandt2000 모두 정형(well-formed) XML 문서에 대해서는 암호 기능을 지원하나, XML 문서의 유효성 유지 및 암호 기능을 동시에 만족시키기 위해서는 해결해야 할 문제점을 많이 가지고 있다. 그림 1은 암호화에 대한 예를 보여주고 있다. (가)는 암호화 이전의 XML 문서이며, (나)에서는 <SSN>과 <Tel_num> 태그의 데이터가 암호화된 Imamura2000의 예이다. (다)는 Brandt2000에서 제시된 방법에 기반하여 수행된 XML 엘리먼트 암호화를 수행한 예로, DTD내에 정의된 속성에 기반하여 태그의 변경 없이 데이터만 암호화된 결과를 보이고 있다.

(가) 원본 XML 문서



(나) 엘리먼트 단위의 XML 암호화 기법

(다) 엘리먼트 속성에 기반한 XML 데이터 암호화 기법

그림 1. XML 암호화 기법

Fig. 1 The techniques of XML encryption

2. XML 유효성 유지 문제

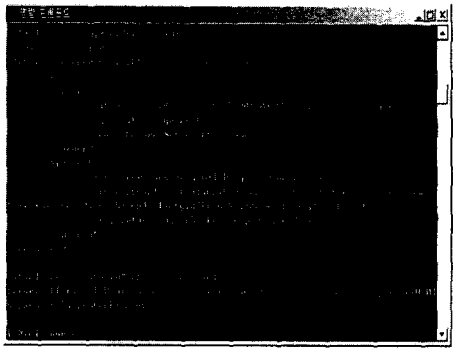
XML 문서는 기본적으로 DTD에 기반하여 작성된 문서이다. 따라서 궁극적으로 안전한 XML 문서의 데이터 교환이 이루어지기 위해서는 유효한 XML 문서에 대한 보안이 필연적으로 요구된다.[9][10]

현재 Imamura2000은 정형 XML 문서에 대해서만 암호화 기능을 지원하고 있다. 이는 자체 정의한 암호화 작업 이전에 작성되어 있는 원문 XML에 기반이 되는 DTD에는 정의되어 있지 않기 때문이다. 따라서 안전한 송수신 문제까지는 해결할 수 있으나, 그 이후의 데이터에 대한 유효성 문제는 검증하기 어려운 한계를 가지고 있다.

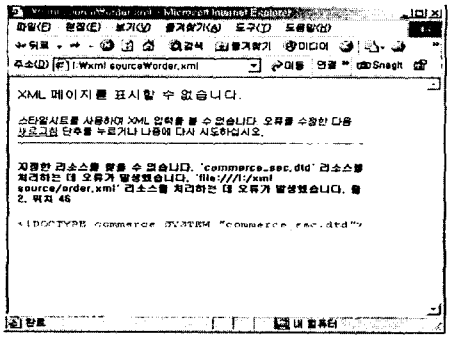
XML 문서와 DTD의 원 상태를 유지하면서 시큐리티 시트를 이용하여 보안성을 지원하는 Brandt2000은 내용과 표현을 분리한다는 측면을 이용한 장점이 있으나, 실제로는 올바른 데이터의

암호화 및 복호화 단계까지는 지원하지 못함이 확인되었다.

XML 보안 기능을 수행할 때 유효성을 고려하였을 경우 나타날 수 있는 현상을 그림 2에서 제시하였다. 그림 2의 (가)는 XML 문서내의 엘리먼트가 암호화된 후 갱신된 XML 문서에 대하여 유효성을 검증하지 못하는 예를 보여주고 있다. (나)는 정형 XML 문서 형태를 만들기 위해 XML 문서내의 DTD 선언에 대하여 암호화 작업을 수행한 후 해당 DTD 선언을 브라우저에서 파싱했을 때의 오류상황을 보여주고 있다. 이러한 유효성 오류는 향후 안전한 XML 문서 교환에 있어 필수적으로 해결해야할 과제이며, 본 논문에서는 이를 XML 스키마를 이용하여 해결하고자 한다.



(가) 암호화 수행 후 유효성이 검증되지 않는 XML 문서의 예



(나) DTD 선언 암호화 수행 후 유효성이 검증되지 않는 XML 문서의 예

그림 2. 유효성이 검증되지 않는 XML 문서들

Fig. 2 XML documents that is not verification

III. 암호화된 XML 문서의 유효성 검증

효과적인 XML 문서의 암호화를 위해서는 기본적으로 XML 문서의 유효성을 유지시켜 주어야 한다. 그러나, 어떤 XML 문서도 암호화 후에는 정형 XML 문서가 된다. 이는 암호화에 관련된 태그를 암호화 이전에 작성된 XML 문서에 기반이 되는 DTD에서 지원해주지 못하기 때문이다. 즉, XML 문서의 유효성을 유지시키면서 암호화를 수행하기 위해서는 DTD를 기반으로 한 XML 문서의 경우 DTD 자체가 새롭게 정의 되어야하는 해결되기 어려운 문제가 발생한다.[8][11]

본 논문에서는 유효성과 암호화를 동시에 만족시켜줄 수 있는 방법으로 XML 스키마를 이용하는 방법을 제안한다. XML 스키마는 정형 XML 문서에 대해서도 지원이 가능하며, XML 문서에 대한 메타 정보를 담고 있으므로 따로 DTD를 필요로 하지 않는다. 또한 각각의 XML 문서에 대하여 동적인 생성이 가능하며 자체 유효성 검사 규칙을 가지고 있으므로 DTD 기반 XML 문서의 암호화에 대한 확장성이 뛰어난 장점을 가지고 있다.

암호화된 XML 문서에 XML 스키마를 이용하여 XML 문서의 유효성을 유지하는 과정은 다음과 같다.

① XML 문서를 파싱
- 암호화될 데이터를 찾기 위해 XML 파싱이 필요하다.

② XML 문서내의 데이터를 읽어들여서 암호 화를 수행
- 과정 1에서 파싱된 정보를 이용하여 암호화될 데이터에 대하여 암호화 연산을 수행하여 암호화된 XML 문서를 생성한다.

③ 암호화된 XML 문서를 파싱, 새로운 XML 스키마 작성
- 암호화된 XML 문서는 유효성을 유지하지 못하는 정형(well-formed) 문서이므로 유효성 검증을 위한 XML 스키마를 생성한다.

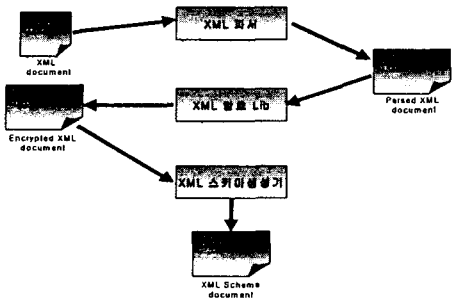


그림 3. XML 스키마 생성
Fig. 3 Creation of XML schema

본 논문에서 XML 문서 유효성 보존 부분은 자바로 구현하였다. XML 파서는 IBM-Apache에서 개발한 Xerces 3.1과 Xalan 2.0.0을 사용하였고, 스키마에 관해서는 ORACLE의 XMLSchema 1.0.1을 참조하였다. 작성된 XML 스키마는 XMLSchema2001의 규칙을 따르게 작성되며, 암호화된 XML의 유효성을 유지시키는 기능을 위해 만들어진 것이다. 따라서, XML 문서가 수신되고 이에 대한 유효성 검증 작업을 마친 후에는 필요가 없다.

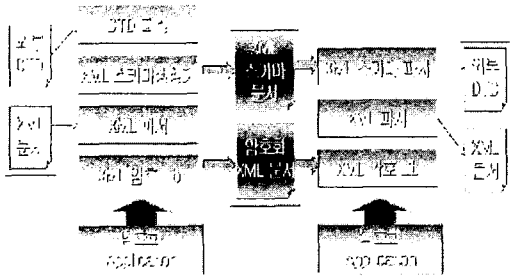


그림 4. XML 스키마를 이용한 유효성 검증
Fig. 4 Validity Verification of XML documents using the XML schema

암호화된 XML 문서에 대한 XML 스키마 생성 이후 최종적으로 갱신된 XML 문서에 대한 유효성 검사결과 DTD에 기반한 XML 문서 암호화 기법에서 발생하는 유효성 위반 문제를 발생하지 않음을 확인하였다. 이 결과를 통해서 암호화된 XML 문서의 브라우징이 가능하며, 네트워크 상의 송수신 후에도 문서에 대해 무결성의 수준이 높아져 사용자와 제공자에게 동시에 신뢰성을 증대시킬 수 있다.

IV. 결 론

XML은 인터넷 상에서 데이터 교환이 쉽고 원활하게 이루어질 수 있도록 하는 어플리케이션에 적합한 언어로 평가받고 있다. 그러나 XML은 문서의 데이터 포맷 표현을 향상시키는데 중점을 두고 만들어졌기 때문에 문서 변조 및 데이터 삭제 등의 공격에 취약한 문제점을 가지고 있다. 이를 보완하기 위해 XML 제반기술과 함께 보안에 관련된 기술 또한 연구가 빠르게 진행되고 있다.

XML 문서의 보안기술 중에서 XML 암호화 기법은 가장 활발한 연구가 진행중인 분야이다. 그러나 XML 암호화 기법은 XML 문서를 암호화시 암호화에 관련된 태그가 새롭게 포함됨으로써 유효한 XML 문서로 검증될 수 있도록 하기 위해서는 전체 DTD를 새롭게 변경해야되는 문제 및 DTD 공격에 대한 해결책 부재 등의 문제점이 해결되지 않고 있다.

본 논문에서는 XML 문서의 유효성과 암호화를 동시에 만족시켜줄 수 있는 방법으로 XML 스키마를 이용하는 방법을 제안하였다. XML 스키마는 정형 XML 문서에 대해서도 지원이 가능하며, XML 문서에 대한 메타 정보를 담고 있으므로 따로 DTD를 필요로 하지 않는다. 또한 각각의 XML 문서에 대하여 동적인 생성이 가능하며 자체 유효성 검사 규칙을 가지고 있으므로 DTD 기반 XML 문서의 암호화에 대한 확장성이 뛰어난 장점을 가진다.

향후 연구과제로 문서를 분석할 때마다 문서의 유효성을 확인하기 위한 시간을 소비하여 속도를 저하시키는 문제를 극복할 수 있는 방안에 대한 연구가 필요하다.

참고 문헌

[1] Takeshi Imamura, Hiroshi Maruyama, "Specification of Element-wise XML Encryption", W3C XML-Encryption Workshop, November, 2000.

[2] Paul Brandt, Frederik Bonte, "Towards Secure XML", http://lists.w3.org/Archives/public/xml-encryption/2000Oct/

[3] Alpha, Works, "XML Security Suite", 1999, htttp://www.alphaworks.ibm.com/tech/xmlsecuritysuite

[4] STI- SECURITY Technologies Inc, "J/LOCK - Java Cryptography Package", March, 2000.

[5] Takeshi Imamura, Hiroshi Maruyama, "Specification of Element - wis e XML Encryption", W3C XML-Encryption Workshop, November, 2000.

[6] Michiharu Kudo, Satoshi Hada, "XML Document Security based on Provisional Authorization", Conference on Computer and Communication Society, Athens. Greece, Nov ember, 2000.

[7] E. Damiani, S Vimercati, S. Paraboschi, P. Samarati, "Design and Implementation of an Access Control Process or for XML Documents ", Proceedings of 9th International World Wide Web Conference, Amsterdam, May, 2000.

[8] E. Bertino, M. Braun, S. Castano, E. Ferrari, M. Mesiti, "Aurhor - x: a Java - Bas ed System for XML Data Protection", Proceeding of the 14th IFIP WG 11.3 Working Conference on Database Security, Schoorl. Netherlands, August, 2000.

[9] H. Maruyama, K.Tamur a, N. Uramoto, "XML and Java, Developing Web Applications", Addison Wesley, May, 1999

[10] William J .Pardi, "XML in Action, Web Technology", Microsoft Press, 1999.

[11] Jonathan Knudsen, "Java Cryptography ", O'REILLY, 1998.

저자 소개

홍성표(Seong-pyo Hong)

1997년 2월 광주대학교 전자계산학과 졸업(공학사)

2001년 2월 조선대학교 대학원 컴퓨터공학과 졸업 (공학석사)

2001년 3월 - 현재 조선대학교 대학원 컴퓨터공학과 박사과정

※관심분야 : 시스템 보안, 분산 운영체제, 컴파일러

이 준(Joon Lee)

1979년 2월 조선대학교 전자공학과(공학사)

1981년 2월 조선대학교 대학원 전자공학과(공학석사)

1997년 2월 숭실대학교 대학원 전자계산학과(공학박사)

1982년 3월 - 현재 조선대학교 전자정보공과대학 컴퓨터공학부 교수

※ 관심분야 : 시스템 보안, 분산 운영체제, 프로그래밍 환경