DTD 전자서명을 이용한 XML문서의 보안성 향상

박도준* 민혜란* · 이준*
*조선대학교 컴퓨터공학과

Security Elevation of XML Document Using DTD Digital Signature

Dou Joon Park*, Hye Lan Min*, Joon Lee*
*Dept of Computer Eng. Chosun University
E-mail : hr7sun@hanmail.net

요 약

DTD는 XML 문서에 표현될 자료의 의미를 정의한 메타 데이터라고 할 수 있다. 따라서 DTD 정보가 손상될 경우 이 정보를 기반으로 한 XML 문서의 보안은 심각한 문제점을 가지게 된다.

본 연구에서는 XML 문서의 송수신 과정에서 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD 에도 전자 서명을 첨부하는 방법을 제안하였다. 먼저 DTD파일을 끝까지 읽으면서 파싱을 하고 여기서 추출되는 엘리먼트나 속성, 엔티티들을 해시테이블에 저장한다. 파싱이 종료되면 해시 테이블을 읽어 들여서 메시지 다이제스트를 수행한다. 수행 후 이를 개인 키와 합성하여 전자 서명을 생성한다. 전자 서명 시 메시지 다이제스트 과정에서 바뀐 순서에 대해서는 검사하지 못하기 때문에 전혀 다른 다이제스트 값을 생성하는 문제가 발생되는데, 이것은 표준화된 구조와 문서에 대한 트리 구조를 구현할 수 있는 DOM을 이용하여 DTD의 전자 서명을 생성하는 방법으로 해결하였다.

ABSTRACT

Can speak that DTD is meta data that define meaning of expressed data on XML document. Therefore, in case DTD information is damaged this information to base security of XML document dangerous. Not that attach digital signature on XML document at send-receive process of XML document in this research, proposed method to attach digital signature to DTD. As reading DTD file to end first, do parsing, and store abstracted element or attribute entitys in hash table. Read hash table and achieve message digest if parsing is ended. Compose and create digital signature with individual key after achievement. When sign digital, problem that create entirely other digest cost because do not examine about order that change at message digest process is happened. This solved by method to create DTD's digital signature using DOM that can embody tree structure for standard structure and document.

키워드
XML, DTD, Digital Signature, Security

Ⅰ. 서 론

인터넷의 급속한 발전과 보급으로 웹 문서의 새로운 양식인 XML이 등장하게 되었다. 최근에는 이를 이용하여 인터넷에서 다양한 활용 사례들이 나타나고 있으며, 특히 XML/EDI (Electronic Data Interchange)를 이용한 전자상거래 환경 구축이 이루어지고 있다.

XML화된 EDI 문서가 타인에 의해 쉽게 조작되거나 오용되면 문서에 대한 신뢰성이 떨어져 그 이용이 제한될 것이다. 그러므로 적절한 수준의 보안 및 통제 체제가 없으면 EDI를 통한 업무처리가 신뢰성을 얻을 수 없고, 법적으로 심각한 문제가 발생할 수 있다. 따라서 XML 보안 문제를 해결하기 위해 많은 연구가 이루어졌으며, 대표적인 XML 보안 기법으로는 XML 전자서명, XML 암호화 기법, XML 접근 제어 기법 등이 있다. 이러한 기법들을 통해서 XML 문서에 대한

보안 수준이 향상되었지만 XML 문서에 대해 완벽한 보안을 지원하는 것은 아니다.

XML문서 보안에 대한 근본 문제는 XML의 구조 자체에 있다. XML 문서는 XML 문서 원본과 문서 내에서 표현하는 여러 정보를 포함한 DTD의 쌍으로 구성된다. DTD는 XML을 표현하기 위한 메타 컨텐트를 가지고 있는 파일로서, 문서 내의 데이터에 대한 의미의 구별, 문서의 유효성 검증을 목적으로 한다. 그러므로 DTD에 대해서도 XML 자체의 보안에 상응하는 보안 정책이 요구된다. 그러나 하나의 XML 문서는 오직 하나의 DTD를 기반으로 작성되어야 하고 엘리먼트 선언의 확장성이 떨어지는 등의 많은 DTD의 제약 사항으로 인해 효과적인 DTD 보안 정책은 제시되어 있지 않다.

본 논문에서는 XML 문서의 송수신 과정에서 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD 에도 전자 서명을 첨부하는 방법을 제안하여 XML 문서의 보안성을 향상시키고자 하였다. 전자 서명 시 메시지 다이제스트 과정에서 바뀐 순서에 대해서는 검사하지 못하기 때문에 전혀 다른 다이제스트 값을 생성하는 문제가 발생되는데, 이것은 표준화된 구조와 문서에 대한 트리구조를 구현할 수 있는 DOM을 이용하여 DTD의 전자 서명을 생성하는 방법으로 해결하였다.

II. XML 전자서명

보안에 대한 요구사항 중 기밀성, 무결성, 인증에 관련된 사항은 암호화 방법을 이용하여 해결이 가능하다. 그러나 부인 봉쇄에 대해서는 전자서명(digital signature)을 이용한다. 전자 서명이란 상대방에게 송신자의 신뢰성을 증명해주는 방법이다. 즉 임의의 공격으로 인한 문서 위조를 방지하기 위한 기법으로, 상대방에게 전자적으로 작성된 서명이 첨부된 형태의 문서를 전송하여 수신자로 하여금 확인 가능하게 한다.

XML 전자 서명은 XML문서의 해시 값을 계산하고 이것을 서명자의 개인키로 암호화한 결과를 서명 값으로 활용한다.

그림 1은 전자 서명이 삽입된 XML문서를 보여주고 있다. <sign>요소의 내용이 원 문서에 대하여 삽입된 전자 서명이다.

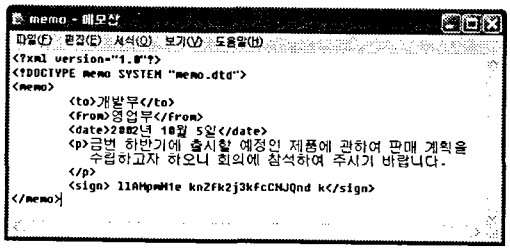

그림 1. 전자서명이 삽입된 XML문서

XML 전자 서명의 중요한 고려사항은 공백 문자 처리, 속성 기본 값, 문자 인코딩이 다른 XML 문서에 대해서도 논리적으로 내용이 동일하다면 같은 서명 값을 생성해야 한다는 점이다. 이에 대한 해결 방안으로 정규형 XML과 DOMHash 기법이 있다.

정규형 XML은 XML문서를 논리적으로 동일한 형태로 인식할 수 있는 규칙을 제정한 것으로, 앞에서 언급한 예외 부분을 특정 규칙에 따라 처리하여 논리적으로 동일한 형태의 XML 문서로 변환시키는 방법이다.

DOMHash를 이용한 서명 생성 방법은 XML 파싱에 이용되는 구조 중 하나인 DOM 구조에 기반을 두어 해시 값을 생성하는 방법으로, 기본적으로 유니코드의 일종인 UTF-16으로 인코딩을 지원하여 정규형 XML의 문자 인코딩 단점을 극복하였고, 정규형 XML 생성 과정의 필요없이 표준 DOM API를 이용하여 해시 값을 계산하는 방법을 정확하게 정의할 수 있는 장점을 지니고 있다.

III. DTD 보안의 문제점

XML 문서는 DTD 또는 XML 스키마에 기반을 두어 작성된다. 그림 2는 DTD 기반 하에 작성된 XML문서를 보여주고 있다.

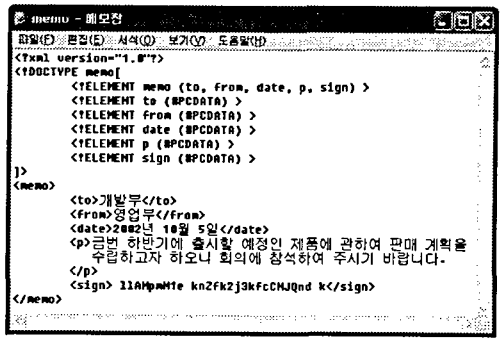

그림 2. DTD 기반 XML 문서

XML 문서의 데이터를 표현하는 메타 데이터 집합인 DTD는 여러 계층에서 공유되고 있다. 그런데 이러한 DTD의 공유 및 메타 컨텐트 관리 측면에서 DTD의 보안 기법은 매우 중요함에도 불구하고, 현재의 연구는 XML 문서의 데이터 암호화에 초점이 맞추어져 있다.

W3C(World Wide Web Consortium)에서는 DTD의 보안에 대한 필요성을 인식하고 있지만 현재의 XML 명세에 따르면 DTD에 대하여 암호화 기법이 적용될 경우 DTD 구문법을 위반하게 되고, 동시에 XML 명세에도 맞지 않기 때문에 적절한 해결책이 제시되지 않고 있다.

1. DTD 파괴

이 공격은 DTD 파일을 삭제하거나 임의로 파괴하여 XML 문서에 대해 유효성 여부의 검증을 어렵게 한다. XML 문서는 DTD에 기반을 두어 작성되며 이 규칙을 지킨 문서만이 브라우징이 가능하게 되어있다. 정보 교환 측면에서 볼 때 DTD가 없는 정형 XML 문서는 정상적인 데이터의 의미를 인지하기 어렵기 때문에 애플리케이션 상에서 데이터 처리가 어렵다. 즉 DTD 선언을 포함하고 선언된 DTD 기반에서 작성된 XML 문서는 유효성이 검증되어야 브라우징을 비롯한 데이터 처리가 가능하다.

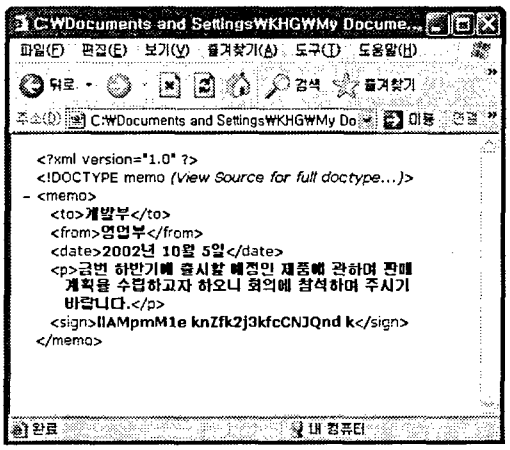

그림 3. 정상적으로 DTD선언을 포함한 XML문서

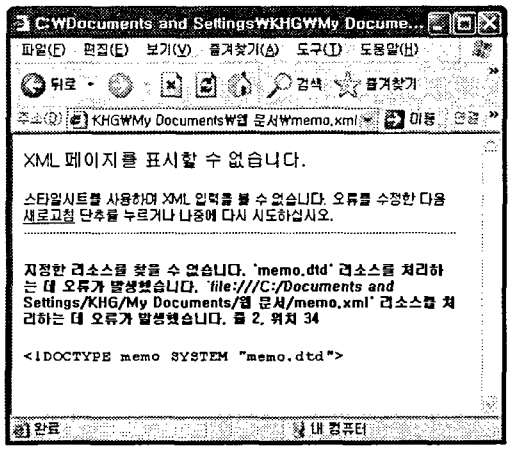

그림 4. 공격에 의해 DTD가 삭제된 XML문서

2. DTD 변조

DTD 파괴보다 한 차원 높은 수준의 공격으로 DTD 파일 내에 정의된 요소 정의 데이터를 조작함으로써 요소에 기반을 둔 암호화 기법을 무력화시킨다.

암호화에 필요한 요소나 속성을 선언한 DTD가 변조되면 XML문서의 암호화 요소 또는 속성 값은 존재하지 않게 되므로 작업을 수행하지 않게 되며 결과적으로 암호화 작업은 일어나지 않는다. 복호화의 경우 암호화 작업이 일어나지 않은 문서에 대해서는 필요가 없으며, 암호화된 문서에 대해서도 복호화할 태그를 찾을 수 없으므로 복호화 또한 수행되지 않는다. 이 경우 안전하게 전송되어야 하는 데이터가 암호화되지 않은 상태로 전송될 가능성이 커지며, 결국 신상 정보와 같은 높은 보안 수준이 요구되는 데이터의 보안 수준은 심각한 문제점을 갖게 된다.

IV. DTD 전자 서명을 이용한 XML 암호화 시스템 구현

XML 문서의 보안성 향상을 위하여 XML 문서의 송수신 과정에서 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD 에도 전자 서명을 첨부한다. 원본 DTD 문서의 메시지 다이제스트 값을 첨부함으로써 DTD 문서에 대하여 신뢰성을 부여한다. 애플리케이션에서 XML 문서 처리 전에 서명 값을 검증함으로써 정보 유출 등의 문제를 극복할 수 있다. 문제점은 DTD 내에 존재하는 엘리먼트 선언들의 순서문제이다. 전자 서명 시, 메시지 다이제스트 과정에서 바뀐 순서에 대해서는 검사하지 못하기 때문에 논리적으로 같더라도 전혀 다른 다이제스트 값을 생성하기 때문이다. 이 문제는 XML 전자 서명에서 나타난 것과 동일한 것으로 XML 정규화를 DTD에 적용시키는 정규 DTD 생성 등이 해결책으로 제시될 수 있다. 그러나 이는 DTD 파서가 따로 요구되며 DTD의 정규화를 위해 또 다른 구문법의 정의가 요구되는 등 많은 시간과 노력이 소요된다. 따라서 본 논문에서는 DOM을 이용하여 DTD의 전자서명을 생성하는 방법을 제안한다.

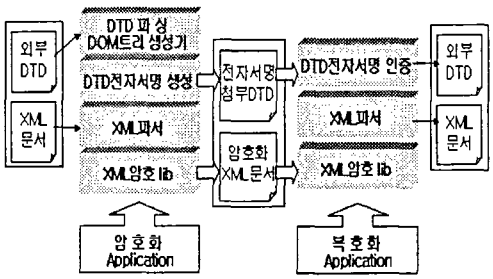

그림 5. DTD전자서명을 이용한 XML암호화시스템

XML 문서를 파싱하는 방법에 DOM과 SAX라는 방법이 있는데, DOM는 XML문서 또는 DTD 문서를 읽어 들여 DOM 트리 구조로 바꾸어서

저장한다.

본 논문에서 DOM구조를 바탕으로 DTD를 파싱하는 방법을 이용하여 해결하려는 이유는 DOM은 구조에 대하여 표준화가 되어 있으며 문서 전체에 대한 트리구조를 구현할 수 있다는 점에서 문서 구조의 정규화에 유리한 장점을 가지고 있기 때문이다.

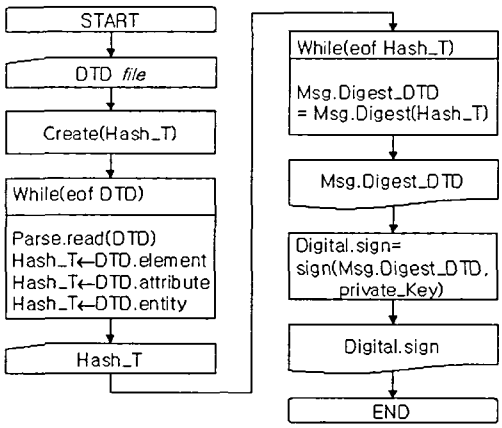

그림 6. DTD 전자서명 flowchart

그림 6은 DTD 파일을 읽어서 전자 서명을 생성하는 플로 차트다. 먼저 DTD파일을 읽어 들이고 DTD 파일의 끝까지 읽으면서 파싱을 하고 여기서 추출되는 엘리먼트나 속성, 엔티티들을 해시 테이블에 저장한다. 파싱이 종료되면 해시 테이블을 읽어 들여서 메시지 다이제스트를 수행한다. 수행 후 이를 개인 키와 합성하여 전자 서명을 생성한다.

본 논문에서는 DTD 전자 서명 및 XML 문서 유효성 보존 부분을 자바로 구현하였다.
애플리케이션 구현은 JDK 1.4를 이용하였으며 XML 파서는 MS-XML Parser 4.0을 이용하였다.

보안에 관련된 툴은 XML에 대해서는 IBM에서 개발한 XSS4J (XML Security Suite for JAVA)를 사용하였고 자바 보안에 관련된 라이브러리로는 Sun Microsystems에서 개발한 JCE 1.2.1을 이용하였다.

V. 결 론

XML 에 대한 역기능으로 많은 정보가 노출됨으로써 전자상거래와 같은 안전한 정보 교환이 요구되는 환경 하에서 효율적이면서도 동시에 많은 정보 범죄를 야기할 수 있는 문제점을 드러내었다. 이러한 문제점에 대한 해결책으로 XML 전자 서명, XML 암호화 기법, 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 연구에서는 이러한 XML 보안의 취약점을 파악하여, XML 문서의 보안성을 향상시킬 수 있는 DTD 전자 서명을 이용한 XML 보안 기능을 제안하였다. 기존의 XML 엘리먼트 암호화 기법과 DTD 전자 서명의 관점에 중점을 두었으며 XML 접근 제어 관점에서는 DTD 접근 제어의 적용 가능성을 제시하였다. 따라서 기존의 시스템에서 발생할 수 있는 DTD의 파괴와 같은 문제점을 접근 권한 부여기법을 이용하여 보완함으로써 보다 향상된 보안 기능의 지원이 가능해졌다.

DTD 전자서명을 이용한 XML 문서의 암호화를 통해 얻을 수 있는 가장 큰 효과로 XML 데이터의 내용과 표현의 분리에만 치중하여 보안상의 문제점을 가지고 있던 단점을 극복할 수 있게 되었다.

향후 연구과제로 느린 속도 문제를 극복할 수 있는 방안과, 스타일 시트에서 보안 기능을 지원하는 방법 등이 있다.

참고문헌

[1] ST I- SECURITY Technologies Inc, "*J/LOCK - Java Cryptography Package*", March , 2000.

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

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

[4] 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.

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

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

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

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