인터넷 쇼핑몰에서 암호화된 XML/EDI를 위한 DTD 전자서명에 관한 연구

홍성표* · 김형균* · 이 준**

A Study on the DTD Digital Signature for Cryptographic XML/EDI in an Internet Shopping Mall

Seong-pyo Hong* · Hyeong-gyun Kim* · Joon Lee*

이 논문은 2001년도 조선대학교 학술 연구비를 지원 받았음

요 약

XML의 등장으로 기존의 EDI를 전자상거래 환경에 맞게 발전시킨 기술이 XML/EDI이다. 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 인터넷 쇼핑몰에서 암호화된 XML/EDI를 위하여 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD에 전자서명을 첨부하는 방법을 제안하였다. 전자서명 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 전자서명을 생성하는 방법으로 해결하였다.

ABSTRACT

Technology that develop existent EDI according to electronic commerce environment by XML's entrance on the stage is XML/EDI. The 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 for XML/EDI that is encoded in internet shopping mall in this research, proposed method to attach digital signature to DTD. 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

Security, Digital Signature, XML, DTD, Internet shopping mall

*조선대학교 대학원 컴퓨터공학과

**조선대학교 전자정보공과대학 컴퓨터공학부

접수일자 : 2003. 2. 17

I. 서 론

XML/EDI는 최근 HTML 이후 인터넷 기술 확산을 한 단계 끌어올려 줄 것으로 기대를 모으고 있다. 이것은 활발한 응용개발이 이루어지고 있는 XML 기술을 EDI 메시지에 적용함으로서 여러가지 전통적인 EDI 시스템의 문제점을 해결하고자 하는 차세대 EDI 연구[1] 중의 하나이기 때문이다.

인터넷 쇼핑몰에서 XML/EDI 문서가 타인에 의해 쉽게 조작되거나 오용되면 문서에 대한 신뢰성이 떨어져 그 이용이 제한될 것이다. 그러므로 적절한 수준의 보안 및 통제체제가 없으면 EDI를 통한 업무처리가 신뢰성을 얻을 수 없고, 법적으로 심각한 문제가 발생할 수 있다. 따라서 XML 보안 문제를 해결하기 위해 많은 연구[2, 3]가 이루어지고 있다.

DTD는 XML을 표현하기 위한 메타 컨텐츠를 가지고 있는 파일로서, 문서내의 데이터에 대한 의미의 구별, 문서의 유효성 검증을 목적으로 한다. 그러므로 DTD에 대해서도 XML 자체의 보안에 상응하는 보안정책이 요구된다. 그러나 하나의 XML 문서는 오직 하나의 DTD를 기반으로 작성되어야 하고 엘리먼트 선언의 확장성이 떨어지는 등의 많은 DTD의 제약사항으로 인해 효과적인 DTD 보안정책은 제시되어 있지 않다.

본 논문에서는 인터넷 쇼핑몰에서 XML/EDI의 암호화를 위하여 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD에 전자서명을 첨부하는 방법을 제안하였다.

II. XML/EDI

1. XML/EDI의 요소 기술과 트랜잭션 모델

XML/EDI는 기존의 EDI를 통하여 이루어지던 업무거래를 필요한 구성요소만 추출하여 XML DTD로 정의한 후 교환함으로써 전통적인 DEI에서 처리할 수 있는 업무의 한계를 벗어나 업무거래 전반에 걸친 통합적 데이터 교환 방식 및 시스템 프레임워크를 말한다.

XML/EDI는 XML과 EDI 이외에 추가적으로 Template, Agent, 저장소(Repository)의 요소를 포함한 5가지 기술의 융합으로 구성된다. 이들의 관계를 그림 1에 요약하였다.

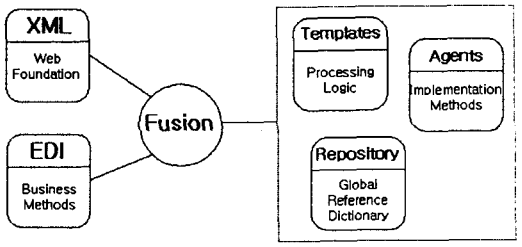

그림 1. XNL/EDI의 요소 기술
Fig. 1 Elements of XML/EDI

XML/EDI 사용모델[4]은 Star, Hybrid, Ad hoc, Web 모델의 4가지로 구분할 수 있다. 그림 2는 XML/EDI의 요소와 사용 가능한 모델을 기초로 하여 제시한 통합 XML/EDI 트랜잭션 모델이다.

XML/EDI 트랜잭션 모델에서는 문서를 교환할 수 있는 웹서버와 글로벌 저장소(Global Repository)의 역할을 하는 웹서버 그리고 데이터베이스 서버가 필요하다.

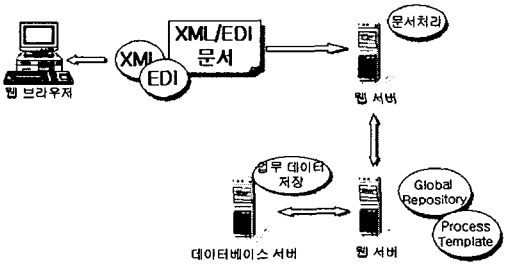

그림 2. 통합 XML/EDI 트랜잭션 모델
Fig. 2 Integrated XML/EDI Transaction Model

2. XML을 이용한 구현의 장점

인터넷 쇼핑몰 구현에 XML을 사용함으로서

큰 장점[6, 8]은 다음과 같다.

① HTML로는 표현할 수 없었던 문서의 구조를 임의의 DTD를 선언하고 태그를 정의함으로써 문서를 표현할 수 있다 - DTD나 스키마를 통해 문서의 구조를 선언함으로써 HTML로는 다 나타낼 수 없었던 문서의 논리적 구조를 표현할 수 있다.

② 인터넷에서 곧바로 사용 가능하다. - HTML이 인터넷 보급과 함께 빠르게 발전했던 것과 같이 인터넷에서 사용 가능함으로 XML의 빠른 발전이 가능하다.

③ SGML보다 구현이 쉽다 - SGML의 subset 이므로 SGML보다는 덜 복잡하다.

④ 내용과 표현이 분리되어 있다 - 마크업은 문서의 구조 및 내용을 나타내기 위해 사용되고 표현을 위해서는 CSS나 XSL을 사용한다.

⑤ 기계뿐만 아니라 사람도 이해할 수 있는 언어이다. - HTML의 마크업 언어는 브라우저가 이해하기는 쉬웠으나 사람이 이해하기에는 그 구문을 외웠어야 했지만, XML은 태그 이름을 내용으로 나타내기에 적당한 것을 사용하게 되면 사람이 이해하기에 훨씬 쉽다.

⑥ 문서의 내용에 접근이 가능하다 - 내용과 표현이 구분되어 구조적인 접근을 통해 내용에 접근이 가능하다.

⑦ XML 태그들은 검색을 효율적으로 할 수 있게 해준다. - HTML의 검색은 태그가 특별히 나타내주는 정보가 없기 때문에 전문(Full text) 검색을 해야한다. 그러나 XML의 태그들은 문서의 구조적 정보나 내용의 정보를 담고 있기 때문에 특정 태그의 내용에서 원하는 단어가 발견된다면 찾고 있는 내용을 갖는 문서라는 것을 알 수 있다.

⑧ 재활용이 가능하다 - XML로 만들어진 문서 중에서 필요한 태그와 그 내용들을 추려서 새로운 문서를 만드는 것이 가능하다. 이 또한 XML의 태그가 문서의 구조나 내용에 대한 정보를 담을 수 있기 때문이다.

III. XML 전자서명

보안에 대한 요구사항 중 기밀성, 무결성, 인증에 관련된 사항은 암호화 방법을 이용하여 해결이 가능하다. 그러나 부인봉쇄에 대해서는 전자서명을 이용한다.[5] 전자서명이란 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 전자서명은 XML문서의 해시 값을 계산하고 이것을 서명자의 개인키로 암호화한 결과를 서명 값으로 활용한다.

그림 3은 전자서명이 삽입된 XML문서를 보여주고 있다. <sign>요소의 내용이 원 문서에 대하여 삽입된 전자서명이다.

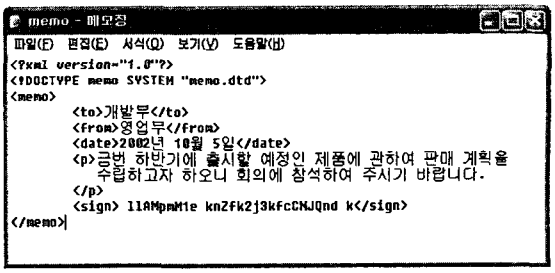

그림 3. 전자서명이 삽입된 XML 문서
Fig. 3 XML document that digital signature is inserted

XML 전자서명의 중요한 고려사항은 공백문자 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.

IV. DTD 보안의 문제점

XML 문서는 DTD 또는 XML 스키마에 기반을 두어 작성된다. 그림 4는 DTD 기반 하에 작

성된 XML문서를 보여주고 있다.

XML 문서의 데이터를 표현하는 메타 데이터 집합인 DTD는 여러 계층에서 공유되고 있다. 그런데 이러한 DTD의 공유 및 메타 컨텐트 관리 측면에서 DTD의 보안기법은 매우 중요함에도 불구하고, 현재의 연구는 XML 문서의 데이터 암호화에 초점이 맞추어져 있다.[7]

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. 정보교환 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.

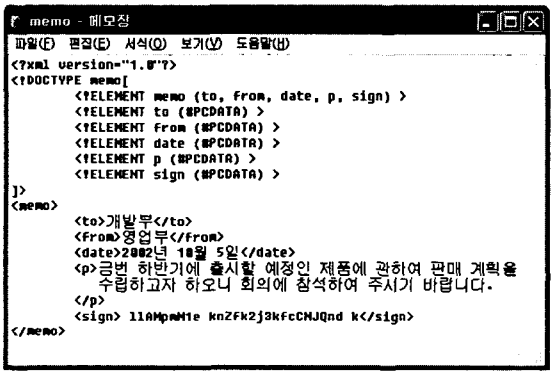

그림 4. DTD 기반의 XML 문서
Fig. 4 XML document of DTD base

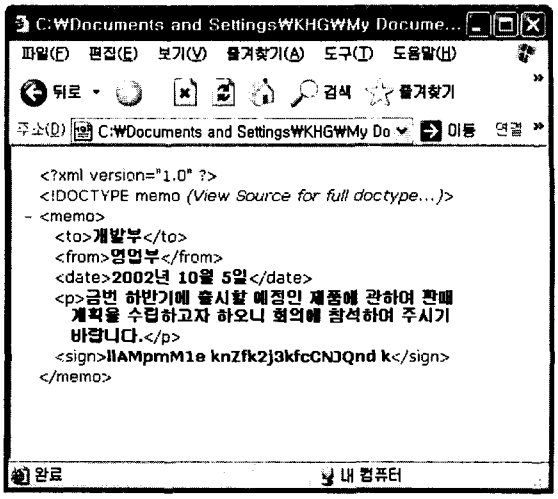

그림 5. 정상적으로 DTD선언을 포함한 XML 문서
Fig. 5 Normally XML document including DTD declaration

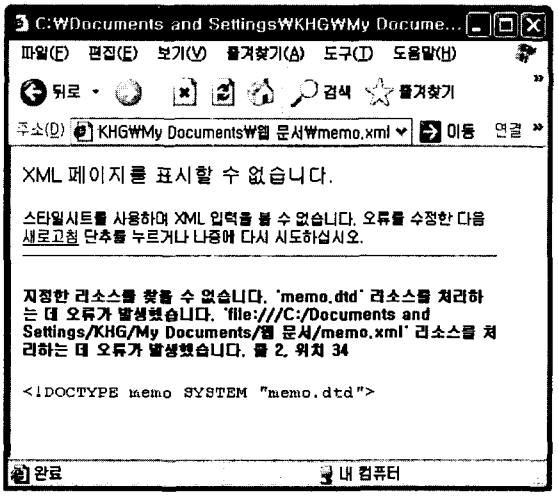

그림 6. 공격에 의해 DTD가 삭제된 XML 문서
Fig. 6 XML document that DTD is deleted by attack

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 신상정보와 같은 높은 보안 수준이 요구되는 데이터의 보안 수준은 심각한 문제점을 갖게 된다.

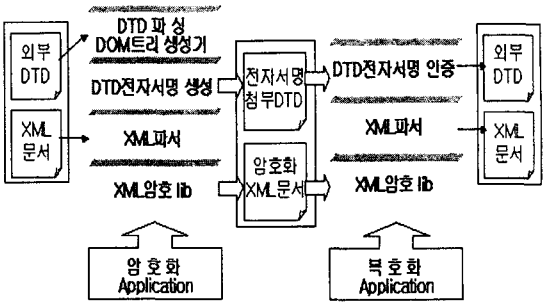

그림 7. DTD 전자서명을 이용한 XML 암호화 과정
Fig. 7 XML encryption process that use DTD digital signature

V. DTD 전자서명을 이용한 XML 암호화 설계

인터넷 쇼핑몰의 보안성 향상을 위하여 XML/EDI 과정에서 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD 에도 전자서명을 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. 전자서명시, 메시지 다이제스트 과정에서 바뀐 순서에 대해서는 검사하지 못하기 때문에 논리적으로 같더라도 전혀 다른 다이제스트 값을 생성하기 때문이다. 이 문제는 XML 전자서명에서 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.

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 8은 DTD 파일을 읽어서 전자서명을 생성하는 플로 차트이다. 먼저 DTD파일을 읽어 들이고 DTD 파일의 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 전자서명을 생성한다.

본 논문에서는 DTD 전자서명 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.

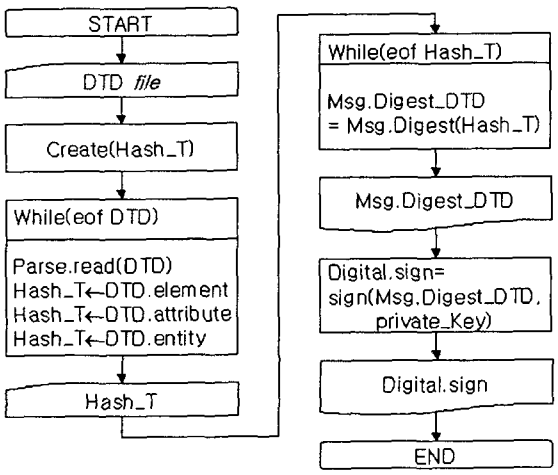

그림 8. DTD 전자서명 flowchart
Fig. 8 DTD digital signature flowchart

VI. 결 론

XML에 대한 역기능으로 많은 정보가 노출됨으로써 인터넷 쇼핑몰과 같은 안전한 정보 교환이 요구되는 환경하에서 많은 정보 범죄를 야기할 수 있는 문제점을 드러내었다. 이러한 문제점에 대한 해결책으로 XML 전자서명, XML 암호화 기법, XML 접근제어와 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, 인터넷 쇼핑몰에서 XML/EDI에서 DTD 전자서명을 이용한 XML 보안기능을 제안하였다. 기존의 XML 엘리먼트 암호화기법과 DTD 전자서명의 관점에 중점을 두었으며 XML 접근제어 관점에서는 DTD 접근제어의 적용 가능성을 제시하였다. 따라서 기존의 시스템에서 발생할 수 있는 DTD의 파괴와 같은 문제점을 접근권한 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 보안기능을 지원하는 방법 등에 관한 연구가 필요하다.

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.

저자소개

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

김형균(Hyeng-Gyun Kim)

1998년 2월 조선대학교 산업대학원 전자계산전공(공학석사)
2000년 3월 현재 조선대학교 일반대학원 컴퓨터 공학과 박사과정
※관심분야: 멀티미디어, 영상처리, 영상통신

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