제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003. 5)

DTD 전자서명을 이용한 XML 문서 보호

홍성표* , 이철승*, 이종은*, 문정환*, 이 준**
*조선대학교 대학원 컴퓨터공학과
**조선대학교 전자정보공과대학 컴퓨터공학부
e-mail:hony1128@hotmail.com

The Protection of XML Documents Using the DTD Digital Signature

Seong-pyo Hong* , Cheol Seung Lee*, Jong Eun Lee*, Jung Hwan Moon*, Joon Lee**
*Dept. of Computer Engineering, Graduate School, Chosun University
**School of Computer Engineering, Chosun University

요 약

전자상거래에 관련된 데이터 교환이 인터넷 상에서 쉽고 원활하게 이루어질 수 있도록 하는 어플리케이션에 적합한 언어로 평가받고 있는 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 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 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD에 전자 서명을 첨부하는 방법을 제안하였다. 먼저 DTD파일을 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.

1. 서론

XML(eXtensible Markup Language) 기술의 유용함이 인식되기 시작하면서 다양한 분야에서 XML 기술을 적용하고 있다. 그러나, XML 문서는 타인에 의해 쉽게 조작되거나 오용될 수 있는 문제점을 가지고 있기 때문에 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 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 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 정책[4, 6]은 제시되어 있지 않다.

본 논문에서는 DTD 공격에 대한 해결책으로 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD 에도 전자 서명을 첨부함으로써 DTD 문서에 대하여 신뢰성을 부여하는 방법을 제안하였다.

2. XML 보안 기술

XML 기술의 급속한 성장과 서비스의 확산으로 XML 문서 보안의 중요성이 크게 대두되고 있고, 범용적인 네트워크 보안 기술과 함께 XML 기반의 전자상거래 보안 또한 중요하게 여겨지고 있다.

현재 XML 보안 기술[1, 5]은 사용자 인증 및 데이터의 기밀성, 사용자 키관리, 접근제어 부분에 대해서 논의되고 있으며, 다른 정보보호 분야에 대한 연구도 계속 진행되고 있다. 그림 1은 Infrastructure 부분과 Application 부분으로 나뉜 계층별 XML 보안 기술을 나타낸다.

2.1 XML 디지털 서명

디지털 서명은 전자화된 문서의 메시지 내용이 수정 및 변조되지 않았음을 보장하는 동시에 메시지의

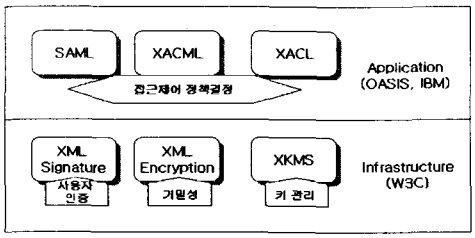

그림 1. 계층별 XML 보안 기술

주체인 사용자들의 신원을 제 3자에게 확인할 수 있게끔 하는 인증방식을 말한다. W3C에서 표준으로 권고된 XML 디지털 서명 기술[2, 8]은 기존의 디지털 서명을 XML을 이용하여 표현한 것으로, 기존의 디지털 서명과 같이 전체 문서에 대해서도 서명을 할 수 있고, 또 XML Transform 기술을 이용하여 서명이 필요한 문서의 일부분에 대해서도 서명 할 수 있어, 기존 문서의 재사용성을 높일 수 있다. 표 1은 XML 디지털 서명에 관련된 태그 집합들을 보여준다.

<표 1> XML 디지털 서명 태그 집합들

```
<Signature ID?>
<SidnedInfo>
<CanonicalizationMethod/>
<SignatureMethod/>
(<Reference URI?>
(<Transforms>)?
<DigestMethod> <DigestValue>
</Reference>)+
</SignedInfo>
<SignatureValue>
(<KeyInfo>)?
(<Object ID?>)*
</Signature>
```

XML 디지털 서명에는 여러 가지 Transform 알고리즘들이 적용되는데, 이는 선택적인 부분의 서명과 문서포맷의 변환 및 서명할 문서의 무결성 등을 보장하기 위해 사용된다.

2.2 서명문서 생성

XML 디지털 서명문서의 생성에는 크게 두 가지 생성 절차가 있는데, 첫 번째는 Reference 생성이고, 두 번째는 서명 생성이다. Reference 생성은 사용자 문서에 여러 가지 Transform을 적용하고, Transform 된 문서에 대해 해쉬값을 계산한다.

서명 생성은 위에서 생성한 Reference 부분을 포함한 서명정보 부분, 즉 SignedInfo 엘리먼트 영역을 사용자의 개인키를 이용해 서명값을 계산하는 과정이다. 여기서 서명전에 서명할 부분에 대한 무결성을 위해 Canonicalization을 수행한다. 그림 2는 XML 서명문서 생성과정을 나타낸다.

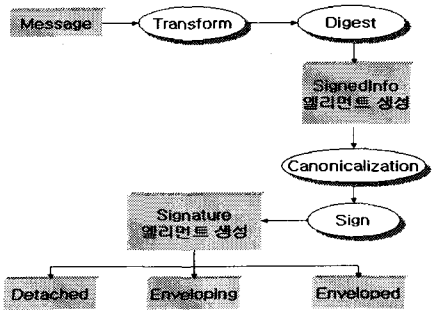

그림 2. XML 서명문서 생성

생성된 서명 문서는 enveloped, enveloping, detached 세 가지 형태로 구분된다. 서명될 문서 안에 Signature 엘리먼트가 포함되어 있으면 enveloped 서명이고, 서명될 문서가 Signature 엘리먼트 안에 포함되어 있으면 enveloping 서명이며, Signature 엘리먼트와 서명될 문서가 한 XML 문서 안에 없으면, detached 서명 형태이다.

2.3 서명문서 검증

XML 디지털 서명 문서의 검증[6] 역시 Reference 검증과 서명 검증 두 부분으로 나뉘어지는데 두 가지 검증 절차는 다음과 같다.

Reference 검증절차는 수신된 서명 문서의 SignInfo 엘리먼트를 추출하여 이 부분에 대한 무결성을 위해 Canonicalization을 수행하고, Reference 생성과정과 동일하게 사용자 문서에 여러 가지 Transform을 적용한 다음 해쉬값을 계산한다. 여기서, 사용자 문서는 Reference 엘리먼트의 URL에서 얻을 수 있다. 이렇게 검증시 계산한 해쉬값과 서명문에 포함된 해쉬값을 비교하여 그 값들이 동일할 경우 Reference 검증은 성공하게 된다.

서명 검증 절차는 사용자의 공개키에 해당하는 정보를 얻는다. 이 공개키로 서명값을 검증하게 된다. 검증 결과가 유효하다면 수신 받은 디지털 서명문서는 유효하다고 판단한다. 그림 3은 XML 서명문서 검증 과정을 나타낸 것이다.

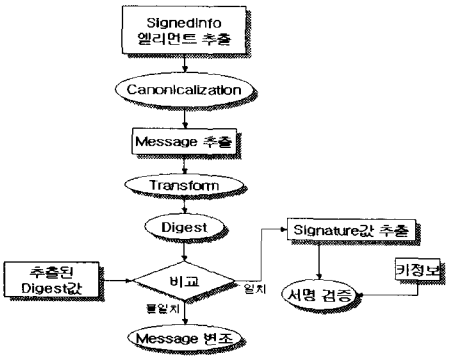

그림 3. XML 서명문서 검증

4. DTD 보안의 문제점

XML 문서는 DTD 또는 XML 스키마에 기반을 두어 작성된다. 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.[7]

DTD에 대한 가장 기본적인 공격은 DTD 파일을 삭제하거나 임의로 파괴하여 XML 문서에 대해 유효성 여부의 검증을 어렵게 하는 것이다. 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.

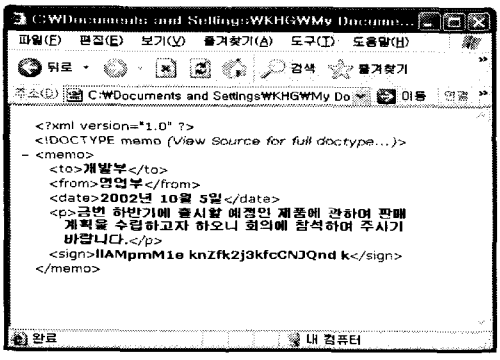

그림 4. 정상적으로 DTD 선언을 포함한 XML 문서

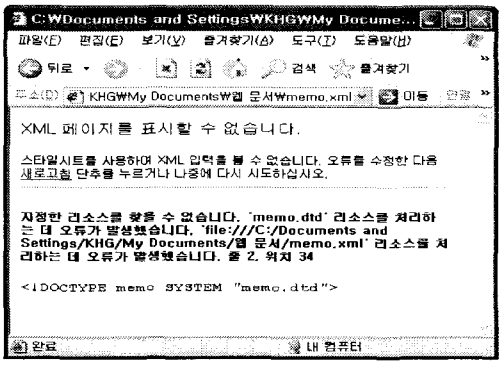

그림 5. 공격에 의해 DTD가 삭제된 XML 문서

그림 4는 정상적인 DTD 선언을 포함한 XML 문서인 경우이고, 그림 5는 공격에 의해 DTD가 삭제되어 정상적인 실행을 하지 못한 경우이다.

5. 설계 및 구현

XML 문서의 데이터를 표현하는 메타 데이터 집합인 DTD는 여러 계층에서 공유되고 있기 때문에 DTD의 공유 및 메타 컨텐츠 관리 측면에서 DTD의 보안이 매우 중요함에도 불구하고, 현재의 연구는 XML 문서의 데이터 암호화에만 초점이 맞추어져 있기 때문에 DTD 파일을 삭제하거나 임의로 파괴하여 XML 문서에 대해 유효성 여부의 검증을 어렵게 하고있다.

본 논문에서는 DTD 공격에 대한 해결책으로 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD 에도 전자 서명을 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 전자 서명을 생성하는 방법을 제안한다. DOM은 구조에 대하여 표준화가 되어 있으며 문서 전체에 대

한 트리구조를 구현할 수 있다는 점에서 문서 구조의 정규화에 유리한 장점을 가지고 있다.

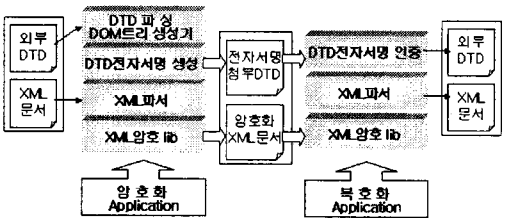

그림 6. DTD 전자서명을 이용한 XML 암호화 과정

그림 7은 DTD 파일을 읽어서 전자 서명을 생성하는 플로 차트다. 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 전자 서명을 생성한다.

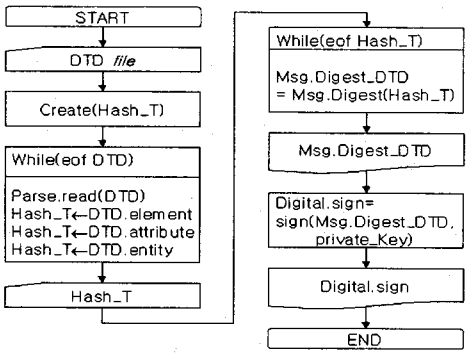

그림 7. DTD 전자서명 Flowchart

6. 결 론

XML은 전자상거래에 관련된 데이터 교환이 인터넷 상에서 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. 이러한 문제점에 대한 해결책으로 XML 전자서명, 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 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 문서를 분석할 때마다 문서의 유효성을 확인하기 위한 시간을 소비하여 속도를 저하시키는 문제를 극복할 수 있는 방안에 대한 것이다.

참고문헌

[1] 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.

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

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

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

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

[6] 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.

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

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