메타레벨 XML 보안 기법을 이용한 처방전 보안 시스템 구현

김형균* · 김용호** · 이상범** · 배용근**
*동강대학 컴퓨터인터넷계열
**조선대학교 컴퓨터공학과

Implementation of the Prescription Secure System using a Meta Level XML Security Methods

Hyeong gyun Kim*, Yong-Ho Kim**,Sang Beom Lee**, Bae-Yong Guen**
*Dept. of Computer & Internet, DongKang College
**Dept. of Computer , Chosun University
E-mail : multikim87@hanmail.net

요 약

본 논문에서는 메타레벨의 XML 보안 기법을 이용한 처방전 보안 시스템을 제안하였다. XML/EDI의 암호화를 위하여 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD에 전자 서명을 첨부하는 방법을 사용함으로써 보다 안전한 처방전 전송 시스템을 구축하고자 한다. 처방전 DTD는 처방전의 각 구성요소에 따라 처방전 정보, 환자 정보, 의료기관 정보, 처방내역 정보, 조제내역 정보 엘리먼트를 정의하고 그 하위에 정보 전송에 따른 정보를 관리하기 위한 하위 엘리먼트를 정의하였다. 안전한 처방전 전송을 위하여 DTD파일을 읽어 들이면서 파싱을 하고 여기서 추출되는 엘리먼트나 속성, 엔티티들을 해시테이블에 저장한다. 파싱이 종료되면 해시 테이블을 읽어 들여서 메시지 다이제스트를 수행하고 이를 개인키와 합성하여 전자 서명을 생성한다.

키워드

XML, Security, Prescription

Ⅰ. 서 론

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 정책은 제시되어 있지 않다.

2000년 7월 의약분업의 실시로 인해 의료기관의 입장에서는 종이처방전 발행과 관리에 따른 비용이 발생하며, 수기로 된 종이처방전을 발행하였을 경우 처방전 발행, 진료기록, 진료비청구자료 작성이라는 작업이 분리되므로 인건비 부담이 증가하게 된다. 약국에서도 처방전 자료의 재입력과 건강보험청구 심사자료 작성의 이중 작업이 생기며, 의료 이용자는 의료기관과 약국을 동시에 방문해야 하고 처방에서 조제에 이르는 시간이 증대되어 시간자원이 낭비될 수 있다. 또한 처방전이 분실되는 경우 조제 지연 및 조제를 포기하는 등 오히려 건강이 악화될 가능성도 있다. 또한 의사의 수기처방전 또는 훼손된 처방전의 판단착오로 약사의 오독으로 인해 잘못된 약을 조제하여 환자의 건강이 문제가 될 수도 있다.

따라서, 본 논문에서는 메타레벨의 XML 보안 기법을 이용한 처방전 보안 시스템을 제안하고, XML/EDI의 암호화를 위하여 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD에 전자 서명을 첨부하는 방법을 사용함으로써 보다 안전한 처방전 전송 시스템을 구축하고자 한다.

II. DTD 암호화에 기반한 XML데이터 교환 기법 제안

DTD에서 정의되어 있는 엘리먼트들은 기본적으로 XML의 정보교환을 위한 중요한 지침이 된다. DTD 내용은 공유를 위해 배포하지만, 공개된 엘리먼트 정보는 좋은 공격 단서가 되며 DTD 파일의 보존이 요구된다. 이를 위해 DTD 파일을 암호화된 형태로 관리하도록 한다. DTD 파일을 소유자의 공개키로 암호화한 상태로 보존하고, 요청자의 접근 정도에 따라 XML 데이터 처리를 위해 임시로 복호화된 템플릿을 사용하는 방법이다. 이 방법은 암호화 기법과 접근 제어 기법이 복합된 형태로 사용자의 인증 과정을 거친 후 DTD의 복호화 처리를 수행한다. 암호화된 DTD 파일은 DTD 엘리먼트 변조 및 DTD 파일 삭제에 따른 XML 문서 접근 거부와 같은 공격으로부터 안전하다. DTD 파일의 보호 정책에 기반한 XML 문서처리는 아래와 같은 오토마타로 기술될 수 있다.

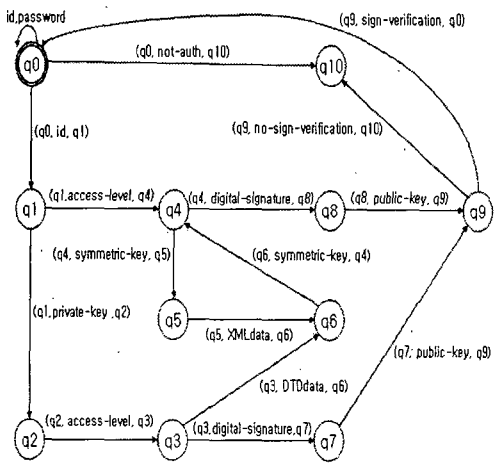

그림 1. DTD 암호화에 기반한 XML 데이터 교환 시스템 흐름도

전이 규칙은 〈이전 상태, 전이시 필요한 데이터, 다음상태〉로 구성된다. 이 오토마타에 대한 흐름도는 그림 3에 제시하였다.

그림 1에서 제시한 XML데이터 교환 시스템 흐름도를 위한 오토마타의 정의는 다음과 같다.

흐름도는 다음과 같은 순서로 수행된다.

첫째, (id, password)를 입력받고 요청자의 인증을 확인한다.

둘째, DTD를 복호화하고 XML 문서에 대해서는 접근 권한을 부여한다.

셋째, DTD에 접근 권한을 부여한 후 XML 문서를 복호화하여 데이터를 처리한다.

넷째, 처리된 XML 문서는 다시 암호화 되며, 각각의 DTD와 XML 문서는 서명을 첨부한다.

마지막으로 서명된 DTD와 XML 문서가 함께 전송되어 요청자에게 전송되면 서명 검증 절차를 거친 후 적절한 데이터 처리를 수행한다. 이 과정의 중간에서 잘못된 결과로 인해 q10의 상태로 전이되는 부분은 모두 다 클라이언트에서 일어난다. 클라이언트와 관계된 상태는 q0, q9, q10 이며, 서버와 관계된 상태는 q1~q8 까지이다.

q0 : 인증 q1 : 권한부여 q2 : 공개키로 암호화된 DTD q3 : 개인키로 복호화된 DTD
q4 : 암호화된 XML 문서 q5 : 복호화된 XML 문서 q6 : XML 데이타 처리
q7 : 전자 서명이 첨부된 DTD q8 : 전자 서명이 첨부된 XML 문서
q9 : 전자 서명 검증 q10 : 종료
id, password : 사용자의 id 와 패스워드
public-key : 제공자의 공개키
private-key : 제공자의 개인키
access-level : 접근 권한 수준
symmetric-key : XML 문서 암호화에 사용된 세션키
digital- signature : 전자 서명
DTDdata : DTD 데이터
sign-verification : 전자 서명 검증 결과- 서명확인
no-sign-verification : 전자 서명 검증 결과- 오류
not - auth : 접근 권한 부여 거부

K = { q0, q1, q2, q3, q4, q5, q6, q7, q8, q9, q10, q11 }
Σ = { id, password, public-key , private-key , access-level, symmetric key, digital-signature, DTDdata, XMLdata, sign-verification, no-sign-verification}
s = F = q0
Δ = {(q0, (id,password), q0), (q0, id, q1), (q0, not-auth, q10), (q1,private-key ,q2), (q1,access-level, q4), (q2, access-level, q3), (q3, DTDdata, q6), (q3, digital-signature, q7),(q4, symmetric-key, q5),(q4, digital-signature, q8), (q5, XMLdata, q6), (q6, symmetric-key, q4), (q7, public-key, q9), (q8, public-key, q9), (q9, no-sign-verification, q10), (q9, sign-verification, q0)}

III. 처방전 보안 시스템 구현

1. 처방전 DTD 설계

처방전 DTD는 처방전의 각 구성요소에 따라 처방전 정보, 환자 정보, 의료기관 정보, 처방내역 정보, 조제내역 정보 엘리먼트를 정의하고 그 하위에 정보 전송에 따른 정보를 관리하기 위한 하위 엘리먼트를 정의하였다.

대표 엘리먼트들을 구성하는 각각의 엘리먼트에 대하여 특성표를 작성하여 엘리먼트의 반복 횟수에 따른 특징을 구분하고, 그림 4와 같이 계층 구조도를 작성하여 대표 엘리먼트와 하위 엘리먼트의 계층성을 파악하여 DTD를 설계하여, 설계된 DTD를 기반으로 XML 파일을 구성하였다. 그리고 엘리먼트들 사이에는 선택적 연산자를

이용하여 필요한 사항만 수시로 입력할 수 있도록 하였다.

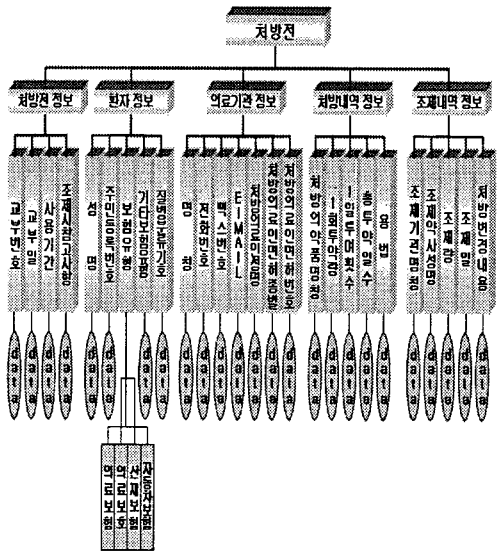

그림 2. 처방전 엘리먼트 구조

2. 시스템 구성

DTD 전자 서명 및 유효성 유지를 위한 XML 스키마 생성기를 포함한 XML 암호화 및 복호화 애플리케이션 시스템의 구성은 그림 3과 같다.

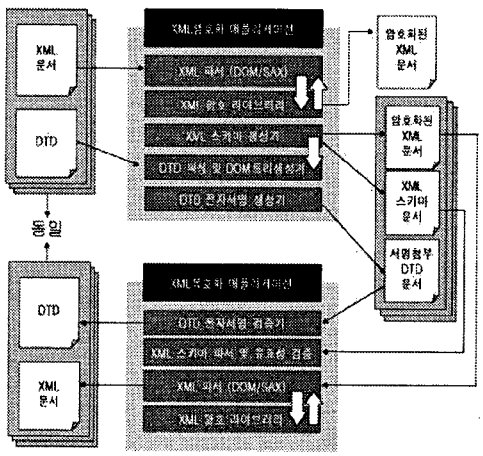

그림 3. XML 암호화 및 복호화 애플리케이션 구성도

기존의 라이브러리에 기반하여 본 논문에서 추가하는 부분인 DTD 전자 서명 및 XML 문서 유효성 보존 부분을 자바로 구현하였다. 애플리케이션 구현은 JDK 1.3을 이용하였으며 XML 파서는 IBM-Apache에서 개발한 Xerces3.1 과 Xalan2.0.0, 그리고 Sun Microsy st ems의 JAXP 1.1을 이용하였다. 한편, XML 스키마에 관해서는 ORACLE의 XMLSchema 1.0.1을 참조하였다. 마지막으로, 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.

Ⅳ. 결 론

본 논문에서는 메타레벨 XML 보안기법을 기반으로 한 처방전 보안시스템을 제안하고, XML/EDI의 암호화를 위하여 XML 문서에만 전자서명을 첨부하는 것이 아니라, 처방전 DTD에 전자 서명을 첨부하는 방법을 사용함으로써 보다 안전한 처방전 전달 시스템을 구축하였다.

본 논문에서 제안한 방법은 기존의 XML 엘리먼트 암호화 기법과 XML 전자 서명의 관점에 중점을 두었으며 XML 접근 제어 관점에서는 DTD 접근 제어의 적용 가능성을 제시하였다. XML 문서의 암호화를 통해 얻을 수 있는 가장 큰 효과는 XML 명세가 갖고 있는 한계인 데이터의 내용과 표현의 분리에만 치중하여 보안상의 헛점을 가지고 있던 단점을 극복할 수 있게 되었다는 점이다. 그러나 유효한 XML문서를 제대로 지원하지 못하는 문제를 가지고 있었다. 이러한 문제를 해결하고자 본 논문에서 제시한 방법은 다음과 같은 특징을 가지고 있다. 첫째, 유효성을 고려한 XML 문서의 암호화 및 복호화 처리를 가능하게 하여 웹 상에서의 XML문서 교환시 브라우저에서 발생할 수 있는 DTD에 기반한 원활한 정보 공유를 지원할 수 있다는 점이다. 기존 연구의 한계인 정형 XML 문서에만 적용할 수 있었던 XML 엘리먼트 암호화를 유효한 XML 문서에까지 적용할 수 있는 장점을 갖는다. 둘째, 기존의 XML 전자서명 기법에서도 문서의 유효성 유지 기능을 지원하고, 동시에 DTD에 전자서명을 부여하는 방법을 지원함으로써 XML문서의 무결성을 DTD에까지 확장 가능하게 하였다. 결과적으로 XML 데이터 교환에 대한 신뢰성이 높아지는 효과를 얻을 수 있다. 마지막으로 DTD의 접근 제어 측면을 고려해보면 기존의 시스템에서 발생할 수 있는 DTD의 파괴와 같은 문제점을 접근 권한 부여 기법을 이용하여 보완함으로써 보다 강력한 보안 기능의 지원이 가능하다는 점이다. 또한, XML 접근 제어 측면에서 본다면 DTD 접근 제어를 가능하게 하였다. 그러나 유효성 유지를 위해 XML 스키마를 생성하는 등의 복잡한 작업이 수행되어야 하며, 자바로 구현되어 다른 언어로 구현된 시스템과 비교했을 때 느린 속도를 극복하기 어려운 단점이 있다. 또한 XML 명세의 제약으로 인해 애플리케이션으로만 해결할 수 밖에 없는 한

계점을 지니고 있다. 추후 연구과제로 느린 속도 문제를 극복할 수 있는 방안과, 실험 결과 미해결 상태로 남아 있었던 스타일 시트에서 보안 기능을 지원하는 방법 등이 있다. 또한, 접근 제어에 관련하여 XML 스키마에 적용할 수 있는 XML 접근 제어 기법 또한 해결해야할 과제일 것이다.

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 - χ: 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.