XML 메시지 암호화 전송 방법 구현†

장의진, 고 훈, 신용태
숭실대학교 컴퓨터학과
e-mail : fiatlux@cherry.ssu.ac.kr

An Implementation of XML Message Encryption Transfer Method

Uijin Jang, Hoon Ko, Yongtae Shin
Dept. of Computing, Soongsil University

요 약

인터넷 기술의 비약적인 발전으로 상품 및 서비스 구매나 발주 광고 활동 등 인터넷을 기반으로 행하는 전자상거래가 활발해지면서 대량의 전자문서를 관리하는 효율적인 정보서비스가 요구되어 왔다. 이에 따라 서로 다른 기종간의 효율적인 문서정보 교환을 위한 여러 표준화 작업들이 이루어져 왔는데, 그 중 인터넷 상에서 구조화된 전자문서를 표현하고 처리하기 위한 표준으로 W3C 에서 XML 이 발표되었다. 그러나 전자상거래의 활성화로 XML 문서의 전송 중 개인정보 유출에 대한 위협이 있을 수 있는데, 본 논문에서는 특정 부분에 대한 암호화를 지원할 수 있는 XML 의 구조적 특징을 이용한 XML 메시지 암호화 전송 기법을 구현하였다.

1. 서론

인터넷 사용자의 급격한 증가로 인해 인터넷상에서의 개인정보 유출 및 정보 유용에 따른 피해가 문제점으로 대두되고 있다. 이에 따라 최근 각 연구소와 학교에서는 개인정보보호를 위한 연구가 활발히 진행중이다. 특히 전자상거래가 활성화 되면서 이런 개인정보 보호에 많은 관심이 집중되고 있다.

이에 본 연구에서는 인터넷 상에서 전송되는 개인의 정보 유출을 방지할 수 있는 전송 시스템을 구현하고자 한다. 여기서 차세대 전자문서 교환의 표준화로 인정 받고 있는 XML(eXtensible Markup Language)을 이용하여 열악한 네트워크 환경을 효율적으로 이용할 수 있게 해주는 멀티캐스트를 기반으로 한 XML 메시지 암호화에 초점을 두어 연구하였다.

2 장에서는 본 연구의 기반이 되는 XML 과 그에 따르는 암호화 기법에 대해 살펴 보겠다. 3 장에서는 XML 메시지 암호화 기법을 이용하여 제안하는 시스템에 대해 구체적으로 논하고, 4 장에서는 결론 및 향후 연구 방향을 제시한다.

2. 관련 기술

2.1. XML

XML(eXtensible Markup Language)은 1996 년 W3C(World Wide Web Consortium)의 후원으로 형성된 XML Working Group 의해 개발된 것으로, 문서를 세분화하고 그 문서들의 일부를 구분하는 의미론적인 태그(tag)를 정의하는 규약의 집합이다. [1]

기존의 SGML(Standard Generalized Markup Language)은 유연성이 많고 시스템이나 플랫폼에 독립적으로 운용되는 등 많은 장점을 갖는 반면 사용이 어렵고 DTD(Document Type Definition) 생성이나 이해가 쉽지 않은 등 시스템을 개발하는데 많은 어려움이 있다. 또한 HTML(Hypertext Markup Language)은 이식성이 뛰어나고 사용이 편리하나, 고정된 태그 집합만을 사용하여, 확장성, 구조성, 데이터의 검사기능에 있어서 한계를 가지고 있다. 이렇듯 SGML 에서의 복잡성을 제거하고, HTML 에서 사용자가 문서 구조를 정의하여 사용할 수 있도록 SGML 과 HTML 의 단점들을 상호 보완하여 문서의 표준화와 대중화에 적합한 형태로 새롭게 정의하고 간결화 시킨 기술 언어가 XML 이라고 할 수 있다.

2.2. XML Encryption

인터넷 상에서 데이터를 전송할 때 대부분 IPSec(IP

Security)과 SSL(Secure Sockets Layer)과 같은 표준 암호화 프로토콜을 사용한다. 그러나, XML 문서 내에서 특성 요소(element)만을 암호화하여 정해진 사용자 외에는 그 내용을 볼 수 없도록 하는 암호화 기법에는 만족스럽지 못하다. 이에 대한 개발이 W3C 의 XML Encryption WG 에서 이루어지고 있다[2].

```
<Invoice>
  <Bookorder>... </Bookorder>
  <Payment>... </Payment>
  <CardInfo>
    <Name>Uijin Jang </Name>
    <Expiration>08/2001 </Expiration>
    <Number>1234 5678 </Number>
  </CardInfo>
</Invoice>
```

[그림 1] 암호화 되기 전의 XML 문서 예

[그림 1]과 [그림 2]는 XML Encryption 에 대한 간단한 예이다. [그림 1]은 암호화 되기 전의 XML 문서이며, 암호화를 원하는 요소는 <Cardinfo>이다.

```
<Invoice>
  <Bookorder>... </Bookorder>
  <Payment>... </Payment>
  <EncryptedData>
DDAKBgNVBAsTA1RSTDECTAcGA1UEAxMQSGlyb3N
oaSBNYXJ1eWFtYTAeFw05OTEyMTcwMDM3MzRa
Fw0wMDAzMTYwMDM3MzRaMEQxCzAJBgNVBAYTA
kpQMQwwCgY DVQQKEwNJQk0xDDAKBgNV==
  </EncryptedData>
</Invoice>
```

[그림 2] 암호화 된 후의 XML 문서 예

Encryption 프로세싱을 마치면 [그림 2]와 같이 원하는 요소만 암호화가 된다.

```
<EncryptionInfo
xmlns="http://www.w3c.org/2000/10/xmlenc" (Id=)?>
 (EncryptionMethod (Algorithm=))   :암호화 알고리즘
 (EncryptionPropertyList)?         :메타-정보
 <ReferenceList>
  (Reference (URI=)? (Xpath=)?)+   :암호화된 데이터 참조
 </ReferenceList>
 (KeyInfo
xmlns=http://www.w3c.org/2000/09/xmldsig#")
                                   :암호화 키
</EncryptionInfo>
```

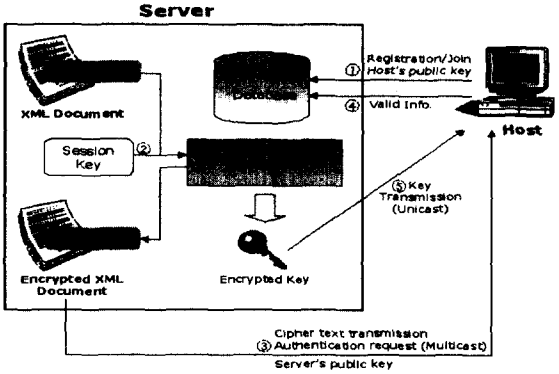
[그림 3] <EncryptionInfo>요소 구문 개요

이러한 암호화 및 복호에 필요한 암호화 알고리즘 및 키잉 정보는 <EncryptionInfo>요소에서 찾을 수 있다. [그림 3]은 <EncryptionInfo>요소의 구문을 나타낸다[3].

3. XML 메시지 암호화 전송 기법

3.1. 시스템 설계

[그림 4]에서는 본 시스템의 전체적인 흐름을 명시하고 있다. 우선 호스트와 서버는 각각 자신의 공개키와 비밀 키를 생성한다.



[그림 4] 시스템 구조

① 호스트는 서버에 개인 정보를 등록하고, 생성된 그룹에 가입하게 된다. 이때 호스트는 이미 생성된 자신의 공개 키를 서버에게 전송한다.
② 서버는 세션 키를 생성한다. 세션 키를 사용하여 전송할 XML 메시지를 암호화한다.
③ 서버는 가입된 호스트에게 암호화된 메시지와 자신의 공개 키를 전송하고, 세션 키 전송을 위해 해당 호스트에 대한 정보를 요구한다.
④ 간단한 인증을 위해 요청을 받은 호스트는 서버에게 그에 상응한 응답을 해준다.
⑤ 응답을 받은 서버는 데이터베이스에 저장되어 있는 개인정보와 비교 후, 이상이 없으면 해당 호스트의 공개 키와 자신의 비밀 키를 이용해 암호화한 세션 키를 전송한다.

이렇게 키를 수신한 호스트는 서버의 공개 키와 자신의 비밀 키를 이용하여 암호화된 세션 키를 복호한다. 복호 된 세션 키를 이용하여 해당 메시지의 암호화된 요소를 복호 할 수 있게 된다.

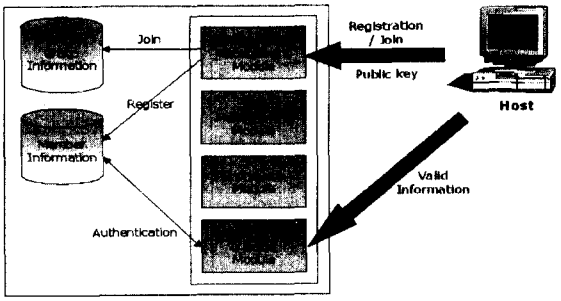
3.2. 서버의 역할

서버는 [그림 5]에서 볼 수 있듯이 메시지 암호화, 키 관리, 그룹 관리, 메시지 및 키 전송의 네 가지 기능을 수행한다.

1) XML 메시지 암호화

XML 문서의 구조적 특징을 이용해 보안이 필요한 부분만을 선택하여 암호화 하는 방식을 사용한다. 송신자가 XML 메시지를 작성하면 메시지 암호화 모듈은 우선 해당 메시지가 유효한(well-formed) XML 문서 구조를 가졌는지에 대해 검사를 한다. 그 후 메시지 내 요소(element)들 중 암호화될 요소들을 검출하고, 해당 요소들을 비밀키 암호 알고리즘을 사용하여 암호화한다. 이 때 사용되는 비밀키는 해당 그룹에 대한 세션 키가 된다. 이렇게 암호화된 요소는 다시 XML 메시지 내의 해당 요소와 대체되기 위해 인코딩 된다. 암호화된 내용을 복호 할 때 필요한 정보들은 암호화

된 내용과 같이 추가된다. 이 과정을 통해 XML 메시지 암호화가 이루어진다.



[그림 5] 서버 구조

2) 키 관리

서버는 그룹 생성시 해당 그룹에서 사용할 세션 키를 생성한다. 해당 그룹의 수신자들에게 첫 번째 메시지가 전송될 때 세션키가 분배되며, 이 세션키는 수신자가 서버에 등록할 때 저장된 수신자의 공개키를 사용하여 암호화된다. 멀티캐스트 상에서의 빈번한 가입과 탈퇴에 따른 보안 유지를 위해 세션 키를 업데이트 해주어야 하는데, 새로운 가입자의 발생 혹은 탈퇴의 경우 해당 그룹의 세션 키는 갱신된다. 이러한 키 업데이트는 해당 그룹 내에서 첫 번째 메시지가 전송되기 전까지는 이루어지지 않는다.

3) 그룹 관리

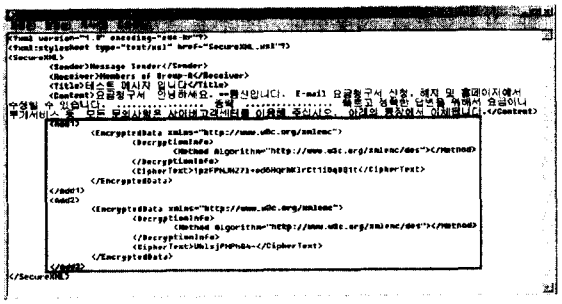
우선 그룹 생성에 필요한 정보(그룹 이름, 그룹주소 등)를 입력하여 그룹을 생성한다. 이 정보는 데이터베이스에 저장되며 클라이언트는 어플리케이션을 통해 그룹 정보를 리스트로 볼 수 있다. 메시지 전송이 끝났거나 더 이상의 그룹 가입자가 없을 경우 해당 그룹을 삭제할 수 있다. 그룹 가입자가 남아 있을 경우, 해당 그룹의 종료를 알리고 데이터베이스에서 해당 정보를 삭제하여 그룹 삭제 프로세스를 마치게 된다.

4) 메시지 및 키 전송

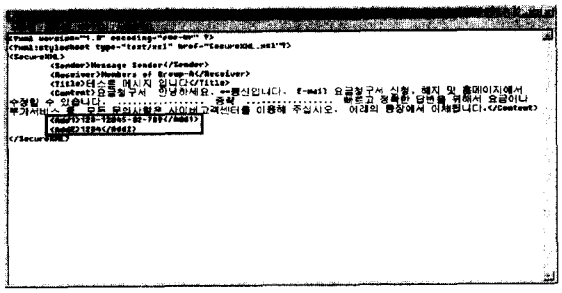
XML 메시지는 멀티캐스트 그룹 주소를 사용하여 전송된다. 그러나 XML 메시지를 암호화할 때 사용한 세션 키는 비밀키로써 안전하게 전송되어야 한다. 본 연구에서는 이를 위해 공개키 암호 방식을 사용하였는데, 수신자의 공개키로써 세션 키를 암호화하여 해당 수신자만이 암호화된 세션 키를 복호 할 수 있다. 이러한 과정에서 많은 키 전송이 이루어지는데, 이는 그룹 통신 초기와 가입자의 발생 및 탈퇴의 경우에만 행해지며 그 이후 세션이 지속되는 동안은 전송 받은 세션 키를 사용하여 통신이 이루어진다.

4. 구현 결과

[그림 6]은 클라이언트에서 복호 되기 전의 XML 메시지 소스이며, 클라이언트에서 복호 과정을 거친 후 [그림 7]과 같이 암호화된 요소들이 복호 되었다.



[그림 6] 암호화된 XML 메시지 소스



[그림 7] 복호된 XML 메시지 소스

5. 분석 및 향후 연구 방향

동일한 데이터를 여러 호스트들에게 전송할 때 멀티캐스트를 사용함으로써 네트워크의 대역 낭비를 방지할 수 있는 장점이 있는 반면 멀티캐스트 주소만 알면 데이터를 수신할 수 있는 문제점에 착안하여 본 논문에서는 XML 문서 구조 중 특정 요소의 암호화 방법을 통해 중요한 데이터를 안전하게 여러 호스트들에게 동시에 전송할 수 있게 하였다. 복호를 위한 키는 해당 그룹 가입자 각각의 개인키로 암호화하여 유니캐스트로 전송함으로써 기존의 멀티캐스트 전송시에 생기는 보안 문제를 해결하였다.

향후에는 메시지 암호화 뿐 아니라 멀티캐스트 정보 보호[4]에 있어 중요 논제가 되고 있는 그룹 인증과 사용자 인증을 통해 더욱 견고한 보안을 제공하여야 할 것이다. 또한 그룹 가입자에 따른 확장성을 가지는 키 관리 기법을 이용한 연구가 이루어져야 할 것이다.

참고문헌

[1] A. Zisman, "An overview of XML", COMPUTING & CONTROL ENGINEERING JOURNAL AUGUST 2000.

[2] XML Encryption Working Group, http://www.w3c.org/Encryption/2001/

[3] Takeshi Imamura, "Proposal: Syntax for keying Information & Encryption Algorithm," W3C XML Encryption Workshop, 2000.

[4] 한근희, "멀티캐스트의 정보보호," 정보처리 제 7 권 제 2 호, 2000.