특

XML 정보보호 개요

문기영[1] 손승원[2]

목 차

1. 서 론

비즈니스 세계에서의 보안은 비즈니스 처리의 안전을 보장하고 사생활과 기밀성을 유지하기 위해 사용되고 있으며 비즈니스 보안은 비즈니스의 생명에 비견될 만큼 중요하게 인식되고 있다. 오늘날의 인터넷 웹 기반의 사업 환경에서 비즈니스 안전을 제공하는 것에 대한 방법은 변화가 필요하다. 인터넷에서는 이질적인 하드웨어와 소프트웨어 그리고 복잡한 관리와 보안에 대한 다양한 요구 등으로 인해 포괄적인 보안을 구축하기 어렵다. 다양한 요구사항들과 새로운 기술, 기존의 기술들을 융합할 수 있는 모듈화되고 확장된 보안 표준이 요구된다.

XML은 최신 응용 분야와 인터넷 컨텐츠를 위해 폭넓게 채택되고 있다. XML은 SGML (Standard Generalized Markup Language)의 간략화된 버전으로 SGML의 확장성, 구조, 검증의 특성을 계승하고 있다. 이런 장점으로 인해 XML은 발표된 이래로 인터넷 상의 자료 표현의 표준으로 각광을 받았다. 기술의 발전으로 인해 인터넷은 문서 교류의 장에서 사이버 뱅킹 등을 거쳐 상거래의 장으로 발전되었고, XML 또한 단순한 문서 교환이 아니라 여러 형태의 문서를 통합하고 전달하는 전자상거래 문서 표준으로 자리잡고 있다.

문서와 프로토콜을 위한 XML 기술의 성장을 전제로, 보안기술과 XML 솔루션들과의 통합은 당연한 것이 된다. XML 정보보호는 보안 요구를 충족시키기 위해서 XML 어휘와 처리 규칙을 정의하고, XML 기술과 기존의 암호 및 보안 기술을 결합시켜 유연하고 확장성이 강한 보안 솔루션을 제공한다. XML 정보보호 표준으로 무결성과 서명 해법을 위한 XML 전자서명[3], 기밀성을 위한 XML Encryption[8], 공개 키 등록과 위치와 검증을 위해 XML Key Management (XKMS)[4], 인증과 인가 정보를 교환하고 속성에 대한 주장을 운반하기 위한 프로토콜인 Security Assertion Markup Language (SAML)[6], 접근 제어 규칙을 정의하는 XML Access Control Markup Language (XACML)[5], 그리고 사생활 정책과 선호를 정

1) 한국전자통신연구원 능동보안연구팀 선임연구원
2) 한국전자통신연구원 책임연구원(부장)

의하는 Privacy Preferences(P3P)를 위한 Platform[9]을 포함한다. 이들 XML 정보보호의 활용으로는 ebXML의 보안과 웹서비스 보안(WS-Security)[7], Digital Rights Management(eXtensible Rights Markup Language 2.0 - XrML)[12] 보안 등이 있다.

본 논문은 기초적인 XML과 보안에 대한 지식을 전제로 주요 XML 정보보호를 요약하여 기술하고, XML 정보보호 기술을 적용한 응용 서비스를 소개한다.

2. XML 정보보호 분류

2.1 특징 및 종류

XML 정보보호는 기존의 보안 알고리즘과 보안 기술들은 사용한다. 그러나 기존의 보안 기술들은 다음과 같은 이유로 대부분의 XML 응용에 적합하지 않다. 첫째, 기존의 보안 기술은 바이너리 형식을 가지고 있어서 문서를 해석하여 사용하거나 문서 중 일부를 보안 정보로 활용하는 응용에는 사용이 불가능하다. 두번째로, 기존 기술들은 XML의 사용을 전제로 만들어진 것이 아니므로 XML 기술의 장점인 컨텐츠 관리의 유연성, URI을 이용한 컨텐츠 기술, XML 컨텐츠 위치 정보 정의[10] 등을 위한 XML 유틸리티를 사용할 수가 없다. 세번째로 일부 기존 기술들은 특정 응용을 전제로 보안을 적용하여 다른 응용에 적용 시 상당한 수정이 필요하다. XML 정보보호는 기존의 보안 기술과 달리 보안이 더해짐으로써 응용에 추가적인 수정이 필요 없게끔 공통의 도구를 사용하여 응용 간 공통의 플랫폼과 처리 규칙을 정의한다.

XML 정보보호는 보안 요구를 충족하는 표준들을 제공한다. 이들 표준은 XML 형식에 따라 설계, 기술되며, 다음은 XML 정보보호 표준에 대한 기술 고려 사항이다.

- XML 정보보호 표준은 XML 스키마, DTD 등과 같은 XML 표준을 사용, 보안 정보와 방법을 표현하고 보안에 관한 XML 어휘를 정의한다.
- XML 정보보호 표준은 융통성과 확장성을 제공한다. XML 문서뿐 아니라 바이너리 문서도 적용할 수 있게한다.
- XML 정보보호 기술은 종단간 보안에 적용된다. 종단간 보안은 XML 메시지가 여러 중간 노드를 거쳐 발송지까지 전달되어야 할 때 중요하다. XML 정보보호의 경우는 종단 간 보안 범위가 기존 보안 기술의 전송 포터 수준의 보안에서 컨텐츠 수준의 보안을 보장한다.
- XML 정보보호 기술은 가능하면 기존의 암호 알고리즘이나 보안 기술을 재사용할 수 있게 정의한다.

2.2 현황

XML 정보보호는 적용방식에 따라 XML 전자문서 정보보호와 XML 기반 정보보호로 구분할 수 있다. XML 전자문서 정보보호는 전자문서 보호를 위한 XML 암호화 (XML Encryption)[8] 기술과 XML 전자서명(XML Signature)[3] 기술이 있다. XML 기반 정보보호는 XML을 기반으로 하는 보안 서비스로 경량화된 PKI를 제공하는 키관리 (XKMS: XML Key Management Specification)[4] 기술과 사용자와 자원간의 사용 인가를 정의하는 접근제어(XACML: eXtensible Access Control Markup Language)[5] 기술 그리고 다양한 벤더들 간 상호운용성을 위한 인가, 인증 정보 교환 (SAML: Security Assertion Markup Language)[6] 프레임워크 등이 있다.

이들 기술의 표준화는 W3C과 OASIS를 중심으로 수행되고 있으며, 미국은 MS와 IBM을 중심으로 XML 정보보호 기술 및 표준 개발을 주도하면서 기술적 우위를 선점하고 있다. 유럽은 밀

라노대학, 크레마(Crema) 대학 등이 XML의 표준화를 주도하고 있으며, 유럽연합의 패스터 프로젝트(FASTER Project)를 통해 연구개발을 진행하고 있다.

국내의 경우에는 ETRI에서 XML 전자서명, XML 암호화 기술, 자바 기반의 암호 라이브러리로 구성되는 XML 기반 전자상거래 보호기술을 개발하였으며[1,2] 그 외의 XML 정보보호 기술에 대해서도 개발이 계속적으로 이루어지고 있다. 또한, 한국전산원에서는 ebXML에서의 XML 보안인증 적용방안 및 표준화에 대한 연구가 진행되고 있다. 현재는 XML 전자서명, XML 암복호 기술이 주류를 이루고 있으나, 향후에는 응용서비스 통합과 다양한 벤더들 간의 상호운용을 위한 XML 기반 정보보호 기술 위주로 발전할 것으로 예상된다.

3. 주요 XML 정보보호 기술

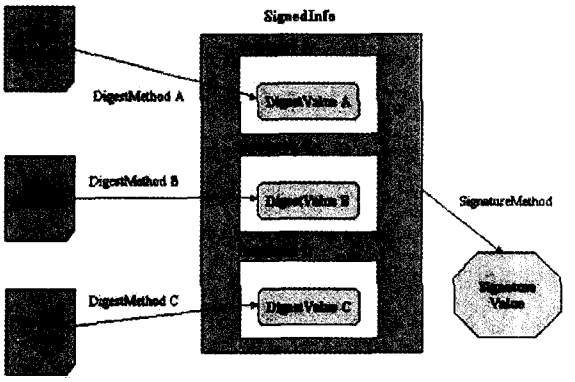
다음은 주요 XML 정보보호 기술들이다.

- 인증과 무결성, 전자서명, 부인봉쇄 - XML Digital Signature
- 문서의 기밀성 - XML Encryption
- 효율적인 키 관리 - XML Key Management Specification(XKMS)
- 인터넷에서 인증과 인가 정보 교환 - Security Assertion Markup Language (SAML)
- 인가 규칙 - XML Access Markup Language (XACML)

3.1 XML 전자서명

XML 전자서명[3]은 XML을 비롯한 다양한 형태의 전자문서에 대해 XML 형태의 전자서명을 생성하고 검증할 수 있는 XML 기반의 전자서명 기법이며 전자문서에 대해 인증, 무결성, 부인봉쇄 등의 정보보호 서비스를 제공해 준다. XML 전자서명은 XML을 비롯한 다양한 디지털 컨텐츠에 대해 적용 가능하며 하나 혹은 그 이상의 리소스들에 대해 전자서명 처리를 할 수 있다.

(그림 1)은 XML 전자서명 생성절차를 간략하게 나타낸 그림이다. 먼저 서명대상 리소스들에 대한 다이제스트 값을 구하여 그 값을 다른 정보들과 함께 Reference라는 이름의 특정 엘리먼트 내부에 삽입하고, 이들 Reference들을 포함하고 있는 SignedInfo라는 이름의 엘리먼트에 대해 전자서명 값을 구한 후, 이들과 키 정보 등의 부가적인 정보를 XML 문서 형태로 구성하여 저장한다.



XML 전자서명은 (그림 2)와 같은 구조를 갖는 Signature 엘리먼트로 표현된다. XML 전자서명은 URI를 통해 서명 대상인 리소스와 연관지어진다. XML 문서 내부에서 XML 전자서명은 단편식별자 (fragment identifier)를 이용해 같은 XML 문서 내에 존재하는 서명 대상인 리소스와 연관지어진다.

Signature 엘리먼트가 서명 대상인 XML 문서 내부에 포함된 경우를 Enveloped Signature라 부르며, 반대로 서명 대상인 문서가 Signature 엘리먼트 내부에 포함되는 경우는 Enveloping Signature 라고 부른다. 서명 대상이 Signature

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

(그림 2) XML 전자서명의 구조

엘리먼트가 들어있는 문서의 외부에 존재하여 전자서명과 서명 대상이 별개로 분리되어 있는 경우는 Detached Signature 라고 한다.

3.2 XML 암호화

XML 암호화[8]는 XML 문서의 내용이 의도된 사용자에게만 구별 가능하고, 그 외의 사람들에게는 알기 힘들게 XML 문서를 암호화하는 방법을 기술한다. W3C XML 암호화 작업 그룹은 XML 문서와 그 일부분을 포함한 디지털 콘텐츠를 암호화/복호화하는 절차를 개발하고, 의도된 사용자만이 복호화할 수 있도록 정보들과 암호화된 내용을 표시하는 데 사용하는 XML 구문을 정의한다. XML 암호화는 전달되는 정보뿐 아니라 저장된 정보에 대해서도 기밀성을 제공한다. 기존의 SSL이나 TLS, VPNs(Virtual Private Networks) 같은 기술들은 정보 전달 시만 기밀성을 제공해 주고 저장된 형태의 문서에 대한 기밀성은 제공하지 않는다.

암호화는 양이 많은 문서를 효과적으로 암호화하기 위해 대칭 키를 사용하여 수행된다. 대칭 키는 복호화를 위해 암호화한 키와 동일한 키를 사용해야 한다. 대칭 키를 공유하기 위해 XML 암호화 표준에서는 암호화에 사용된 대칭 키를 공개 키 암호화를 사용하는 방법을 사용하여 대칭 키를 상대방에게 전달한다. 공개 키 방식은 상대방의 공개 키를 사용하여 암호화에 사용된 대칭 키를 암호화하여 암호문과 같이 전달하여, 상대방이 자신의 개인 키로 대칭 키를 복호화하여 문서 복호화에 사용하도록 한다.

XML 암호화는 (그림 3)과 같은 구조를 갖는 EncryptedData 엘리먼트로 표현된다. XML 암호화는 URI를 통해 암호 대상인 리소스와 연관지어진다.

```
〈EncryptedData Id? Type?〉
  〈EncryptionMethod/〉?
  〈ds:KeyInfo〉
    〈EncryptedKey〉?
    〈AgreementMethod〉?
    〈ds:KeyName〉?
    〈ds:RetrievalMethod〉?
    〈ds:*〉?
  〈/ds:KeyInfo〉?
  〈CipherData〉
    〈CipherValue〉?
    〈CipherReference URI?〉?
  〈/CipherData〉
  〈EncryptionProperties〉?
〈/EncryptedData〉
```

(그림 3) XML 암호의 구조

XML 암호화는 대상 문서를 다음과 같이 4가지 유형으로 암호화한다.

- XML Element Content 단위 암호화 - 엘리먼트 단위 암호화
- XML Element Character Data 암호화 - 엘리먼트에 속한 데이터 단위 암호화
- XML 문서 단위 암호화 - 문서 전체 암호화
- EncryptedData 엘리먼트에 대한 암호화 (Super-Encryption) - 암호문에 다시 암호화

3.3 XML 기반 키 관리

XML 기반 키 관리[4] 표준은 공개 키 관리를 위한 프로토콜을 정의한다. 이 표준의 주요 목적은 전자서명을 검증하거나 데이터를 암호화하기 위해 사용되는 공개키를 키 사용자에게 필요한 키 위치를 명시하고, 이름이나 속성정보를 해당 비밀키 소유자와 관련지어 주는 것이다. 공개 키 기술은 XML 전자서명와 XML 암호화, 기타 여러 보안 응용에 필수적으로 사용된다. 전자서명을 위해 개인 키로 서명하고, 수신측은 상대방의 공개키로 서명을 검증한다. 또, 암호화에서는 공개키로 암호화하고 개인 키로 복호화한다. XML 기반 키 관리는 서명을 검증하거나 암호화하는 공개키의 공유를 효율적으로 도와주는 기능을 정의한다.

XML 키 관리의 2가지 주요부분은 다음과 같다.

- X-KISS(XML Key Information Service Specification)
- XML 응용에서 신뢰할 제3자(relying party)에 의해 XML 디지털 서명, XML 암호화 데이터 또는 기타 공개키 사용과 관련된 키 정보의 처리를 지원하는 프로토콜을 정의한다. (그림 4)와 같이 X-KISS의 기능은 주어진 식별자 정보에 필요한 공개키의 위치를 부여하고 공개키를 연결(binding) 하는 것이다. 프로토콜 설계의 핵심적인 목표는 기본적인 PKI에서의 구문과 복잡성을 극복하고, 응용 구현의 복잡함을 최소로 하기 위한 것이다.
- X-KRSS(XML Key Registration Service Specification)
  키 쌍이 XML 키 관리와 관련되어 계속 사용될 수 있도록 키 쌍 소유자에 의한 키 쌍의 등록을 지원하는 프로토콜을 정의한다. 신뢰 서비스로 요청과 응답 교환으로 이루어진다.

```
〈element name="KeyInfo"〉
〈complexType〉
〈choice maxOccurs="unbounded"〉
  〈any processContents="lax" namespace="##other"
       minOccurs="0" maxOccure="unbounded"/〉
  〈element name="KeyName"type="string"/〉
  〈element ref="ds:KeyValue"/〉
  〈element ref="ds:RetrievalMethod"/〉
  〈element ref="ds:X509Data"/〉
  〈element ref="ds:PGPData"/〉
  〈element ref="ds:SPKIData"/〉
  〈element ref="MgmtDat"type="string"/〉
〈/choice〉
〈attribute name="Id" type="ID" use="optional"/〉
〈/complexType〉
〈/element〉
```

(그림 4) XML 디지털서명에 의해 정의된 KeyInfo에 대한 XML 스키마

XML 키 관리의 적용 범위는 각 구현 어플리케이션마다 상이하다. 이러한 이유로 인해 XML 키 관리에서는 계층적 서비스 모델로 세분화시킴으로써 업무에 따른 정확한 처리 계층을 선택할 수 있도록 정의하고 있는데 3가지로 구분하면, Tier 0 (〈ds:RetrievalMethod〉의 처리), Tier 1 (Locate Service), Tier 2 (Validate Service)

로 나뉜다. X-KRSS는 공개키 정보의 등록을 처리하는 웹 서비스에 대한 프로토콜을 정의한다. X-KRSS는 키 등록, 키 취소 및 키 복구의 전체 인증 처리과정을 단순한 단일 명세서에서 지원한다. 공개키는 등록된 즉시 X-KISS를 포함하는 다른 웹 서비스와의 결합으로 사용되어질 수 있다.

3.4 XML 기반 접근제어

XML 기반 접근제어[5]는 인가에 대한 규칙을 표현하기 위한 XML 어휘로 구성된다. 접근제어 규칙을 정의한 XML 어휘를 이용하여 보안이 요구되는 자원에 대해 미세한 접근 제어 서비스를 제공한다.

(그림 5)와 같이 XML 기반 접근제어는 접근제어 주체와 행동을 표현하기 위해 보안 정보 교환 표준인 SAML에서 사용하는 XML 어휘를 사용하며 접근제어 객체(target)와 효과(effect), 조건(condition)을 정의한다. 접근제어 객체는 접근제어 주체와 자원, 행동을 포함하며 SAML에 의해 정의된다. XACML에서 효과는 허락(Allow) 또는 거절(Deny) 중 하나로 표현된다.

3.5 SAML

SAML[6]은 인증과 인가 정보를 안전하게 교환할 수 있게 하는 표준이다. 주요 목적은 인증(Authentication)과 인가(Authorization) 서비스를 제공하는 다양한 벤더 플랫폼 간의 상호 운용성(Interoperability)을 성취하는 것이다. SAML은 OASIS의 SSTC(Security Service Technical Committee)에 의해 표준화가 수행된다.

SAML 표준은 Assertion, 프로토콜(Protocol), 바인딩(Binding), 그리고 프로파일(Profile)을 포함한다. SAML은 세가지 종류의 assertion을 포함하는데, 인증 assertion(사용자 식별), 속성 assertion(사용자에 관한 정보), 인가 decision assertion(사용자가 한 아이템을 사도록 인가되었는지를 식별)이다. 프로토콜은 개체(entity) 간에 교환되는 요청, 응답 메시지다. 프로토콜은 SAML이 HTTP 상에서 SOAP을 이용하여 assertion을 요청하고 추출하는 방법을 제

```
<?xml version="1.0" encoding="UTF-8" ?>
- <Rule RuleId="//medico.com/rules/rule1" Effect="Permit" xmlns="urn:oasis:names:tc:xacml:0.15i:policy"
  xmlns:function="urn:oasis:names:tc:xacml:0.15i:function"
  xmlns:identifier="urn:oasis:names:tc:xacml:0.15i:identifier"
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
  instance" xsi:schemaLocation="urn:oasis:names:tc:xacml:0.15i:policy http://www.oasis-
  open.org/tc/xacml/v15/draft-xacml-schema-policy-15i.xsd">
  <Description>A person may read any record for which he or she is the designated patient</Description>
- <Target>
  - <Subjects MatchId="function:rfc822Name-equal" DataType="xs:boolean">
      <AttributeDesignator Designator="//xacmlContext/Request/Subject/Attribute
        [@DataType='identifier:rfc822Name']" DataType="identifier:rfc822Name" />
      <Attribute DataType="identifier:rfc822Name">@</Attribute>
    </Subjects>
  - <Resources MatchId="function:string-match" DataType="xs:boolean">
      <AttributeDesignator Designator="//xacmlContext/Request/Resource/@ResourceURI"
        DataType="xs:anyURI" />
      <Attribute DataType="xs:anyURI">//medico.com/record.*</Attribute>
    </Resources>
  - <Actions MatchId="function:subset" DataType="xs:boolean">
      <AttributeDesignator Designator="//xacmlContext/Action[@Namespace=]" DataType="xs:string" />
      <Attribute DataType="xs:string">read</Attribute>
    </Actions>
  </Target>
- <Condition FunctionId="function:string-equal" DataType="xs:boolean">
    <AttributeDesignator Designator="//xacmlContext/Request/Subject/SubjectId"
      DataType="xs:string" />
    <AttributeDesignator Designator="//xacmlContext/Request/Resource/patientName"
      DataType="xs:string" />
  </Condition>
</Rule>
```

(그림 5) XML 기반 접근제어 규칙 예

시한다. 프로파일은 바인딩과 프로토콜의 집합으로 구성한다. 예를 들면, SAML에서 "Browser/POST 프로파일"은 브라우저를 가지고 HTTP POST와 HTML 폼을 사용해서 요청과 응답이 교환되는 방법을 기술한다.

SAML이 인증과 인가 서비스를 위한 기초로서 사용되는 방법에 대한 예제는 다음과 같다.

- 믿을 수 있는 파트너 간에 SSO(Single Sign On)을 가능하게 한다. 사용자가 웹 사이트에 대해 인증하고 나면 다시 인증을 하지 않고 다른 벤더들에 의해 제공되는 웹 자원에 접근할 수 있도록 허가된다.
- 어플리케이션이 사용자(인증 assertion)를 식별하고 인증 assertion과 지역 정책에 기반한 접근 허가를 할 수 있도록 한다.

4. XML 정보보호 응용 서비스

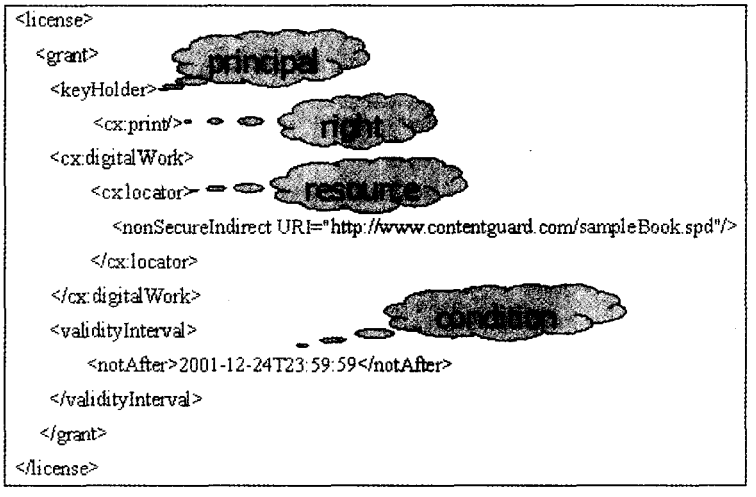
XML 정보보호 표준들은 XML 응용에 쉽게 적용 된다. 본 장에서는 XML 정보보호를 적용하는 대표적인 응용 서비스로 디지털 저작권 보호에 대해 소개한다.

XrML[12]은 디지털 컨텐츠를 사용하는데 필요한 저작권, 과금, 조건들과 이에 덧붙여 메시지의 무결성과 엔터티 인증에 대하여 정의한다. 이 표준은 전자 도서, 디지털 영화, 디지털 음악, 인터넷 게임, 컴퓨터 소프트웨어 등을 출판하고 파는 디지털 컨텐츠 산업을 지원하기 위하여 만들어졌다.

XrML은 XrML core와 목적과 조건에 따라 확장 문장으로 이루어진다. (그림 6)과 같이 XrML Core는 원칙(Principal), 권리(Right), 자원(Resource), 조건(Condition)의 엘리먼트로 구성된다. 원칙 엘리먼트는 권리의 주체가 되는 유일한 개체를 표현하기 위한 인증 매카니즘으로 XML 전자서명이 사용된다. XrML은 저작권을 표현하기 위한 표준이지만, 실제 수행을 위해 자원 접근제어를 위해 XML 접근제어 기술이나 상호 인증을 위한 SAML 등을 사용하여야 한다.

5. 결 론

본 논문에서는 XML 정보보호에 대한 개략적인 기술을 통해 개념 이해와 제공 기술들을 소개하였



(그림 6) XrML Core 구조

다. XML 정보보호 기술은 기존의 보안 기술들과 완전히 다른 기술은 아니다. 그러나 XML 기술과 접목을 통한 기존 기술이 가지고 있지 않은 융통성과 확장성을 가지고 있다. XML 정보보호는 인증, 인가, 무결성, 접근제어, 보안 정보 교환 등의 보안 요구 사항을 만족하는 처리 규칙과 관련 XML 어휘에 대해 정의한다. 이들 기술들 상호간에도 각 보안 요구사항을 충족하기 위해 상호연동하여 사용된다. 예를 들어, XML 키 관리 등의 XML 정보보호 기술은 인증을 위해 XML 전자서명을 사용하고, 메시지 통신 시 기밀성을 보장하기 위해 XML 암호화를 사용한다. 또, XACML은 SAML의 엘리먼트를 사용하여 접근제어를 표현하고 인가 정책에 대한 내용을 공유한다. 이와 같은 상호연동의 용이성은 실제 응용에서도 보안 기술을 적용할 때 유연성과 확장성을 유지할 수 있게 한다.

인터넷 전자거래가 보편화됨에 따라, 인터넷 온라인 전자문서의 표준으로 자리잡고 있는 XML 문서에 대한 정보보호의 중요성이 대두되고 있다. 전자결제, 전자계약 등 전자상거래 서비스의 XML화가 급속히 진행되고 있으며 ebXML (e-business XML), 웹 서비스 등 국제 전자상거래 표준이 XML 기반으로 이루어지고 있어, XML 정보보호는 전자상거래 활성화를 위해 중요한 기반을 제공하는 기술이 되고 있다.

참고문헌

[1] 문기영 외 4명, XML 기반 안전한 전자상거래를 위한 보안 플랫폼, 전자통신동향분석, 제17권, 제6호, 2002년 12월.

[2] Joo-Young Lee, Ju-Han Kim, Jae-Seung Lee, Ki-Young Moon, and Hyun-Sook Cho, "ESES: XML Security for Secure Electronic Commerce," Proceedings of WISA 2001, Sept. 2001

[3] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia and Ed Simon, "XML Signature Syntax and Processing", http://www.w3.org/TR/xmldsig-core/, 2002.

[4] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia and Ed Simon, "XML Key Management Specification (XKMS 2.0)", http://www.w3.org/TR/xmldsig-core/, Mar. 2002.

[5] OASIS, "OASIS extensible Access Control Markup Language (XACML) Working Draft 14, http://www.oasis-open.org/committees/xacml/docs/, Jun. 2002

[6] OASIS, "Security Assertion Markup Language, http://www.oasisopen.org/committees/security/,Jan. 2003

[7] OASIS, "Web Services Security (WS-Security) Version1.0, http://www-106.ibm.com/developerworks/library/Ws-secure/, Apr. 2002

[8] Takeshi Imamura, Blair Dillaway and Ed Simon, "XML Encryption Syntax and Processing", http:// www.w3.org/TR/xmlenc-core/, 2002

[9] W3C, "The Platform for Privacy Preferences 1.0 Specification., http://www.w3.org/TR/P3P, Apr. 2002

[10] W3C, "XML Path Language (Xpath) Version 1.0," J. Clark and S. DeRose (Editors), http://www.w3.org/TR/xpath, Nov. 1999

[11] W3C, "Simple Object Access Protocol SOAP Version 1.2 Part 0: Primer, W3C Working Draft, http://www.w3.org/TR/soap12-part0/, Jun. 2002

[12] XrML.org, "extensible rights Markup Language (XrML) 2.0 Specification, http://www.xrml.org/, Nov. 2001

저자약력

문 기 영

1986년 경북대학교 전자공학과 (공학사)

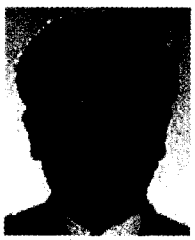
1989년 경북대학과 전자공학과 석사 (공학석사)

1992년-1994년 (주)대우정보시스템 기술연구소 전임연구원

1994년-현재 한국전자통신연구원 능동보안연구팀 선임연구원 (과제책임)

관심분야 : XML 정보보호, 응용 보안, 분산시스템, 트랜잭션 처리

이 메 일 : kymoon@etri.re.kr



손 승 원

1984년 경북대학교 전자공학과 (공학사)

1994년 연세대학교 전자공학 석사 (공학석사)

1999년 충북대학교 컴퓨터공학과 박사 (공학박사)

1991년-현재 한국전자통신연구원 책임연구원(부장)

관심분야 : 네트워크 보안, 라우팅 알고리즘, 생체인식기술

이 메 일 : swsohn@etri.re.kr