ebXML에서의 인증 및 접근제어 모델 연구

차무홍, 정종일, 유석환, 신동규, 신동일
세종대학교 컴퓨터공학과
e-mail: bidon@gce.sejong.ac.kr

A Study on Authentication and Access Control model in ebXML

Moo-Hong Cha, Jong-Il Jeong, Seok-Hwan Yu, Dong-Kyoo Shin, Dong-Il Shin
Dept of Computer Engineering, Se-jong University

요 약

ebXML 프레임워크는 전 세계적으로 폭넓은 지지를 받으며 전자 상거래 표준 프레임워크로 그 영역을 넓혀가고 있는 시점이다. 이에 따라 ebXML의 보안적인 요소가 중요시되는 가운데 인증분야에서도 위험성을 내포하고 있어 각 시스템마다 존재하는 많은 인증 정보관리 문제와 리소스에 대한 접근제어 문제가 부각되고 있다. OASIS에서는 인증관리 문제를 해결하기 위해 SAML이라는 표준 인증 방식을 제시하였고 접근제어를 위해 XACML이라는 표준을 제정하였다. SAML은 XML기반의 표준화된 인증 방식을 취하여 안전성과 확장성뿐만 아니라 인증 간 상호운용성을 제공하는 강력한 기능을 가지고 있으며 XACML은 ebXML 스펙 2.5에서 접근제어를 XACML을 통하여 예를 제시하고 있다. 본 논문에서는 SAML과 XACML을 ebXML 인증 및 접근제어 모델을 연구하고자 한다.

1. 서론

UN/CEFECT와 OASIS(Organization for the Advancement of Structured Information Standards)의 국제적 기구가 주도가 되어 XML을 기반으로 한 범용적인 전자 상거래 프레임워크를 개발하였는데 이것이 바로 ebXML (electronic business eXtensible Markup Language)[1]이다.

ebXML 프레임워크가 폭넓은 지지를 받으면 전자 상거래 표준 프레임워크로 그 영역을 넓힌 현재 ebXML은 보안상에 위험성을 가지고 있다. ebXML에서는 전자 상거래에 있어 가장 우선 해결되어야할 보안 문제에 있어 기 승인된 기술명세 외에 향후 작업을 통해 기술명세로 발전시켜 나갈 기술보고서 중 보안 관련 보고서로 ebXML Security Team에서 제출한 “Technical Architecture Risk Assessment v1.0”과 Technical Architecture Security Team에서 공개한 “ebXML Registry Security Proposal” 이 있다. 이 보안 관련 보고서에서는 ebXML 메시지와 등록기/저장소(Registry/ Repository)의 상호 연 동시 보장되어야 할 각종 보안 요구사항을 어떻게 만족시킬 것인지에 대한 표준을 제시하고 있다.

본 논문에서는 SAML(Security Assertion Markup Language)과 XACML(eXtensible Access Control Management Language)을 이용하여 ebXML 프레임워크의 보안 위험성을 줄여줄 수 있는 인증 및 SSO(Single Sign On)과 접근제어에 대한 적용 개념을 소개하고 SAML과 XACML을 연동한 인증 및 접근제어 모델을 제시한다.

2. 관련 연구

2.1 ebXML

ebXML은 기존의 전자 상거래 프레임워크 표준과는 다르게 거래 당사자간의 송수신 메시지 형식뿐 아니라 각각의 비즈니스 프로세스와 분산된 저장소의 구축 모델까지 포함하는 포괄적인 시스템 구조를 제시하고 있다. 이러한 이유는 기존의 집중화된 시스템 적용 시 발생하는 각각의 거래 당사자간의 비즈니스 프로세스 최적화 및 확장의 어려움 등의 문

제를 해결하기 위해 수평적(horizontal) 프레임워크를 정의하고 있는 것이다.

"Technical Architecture Risk Assessment v1.0"에서 나와 있는 ebXML에서의 위험은 다음과 같다.

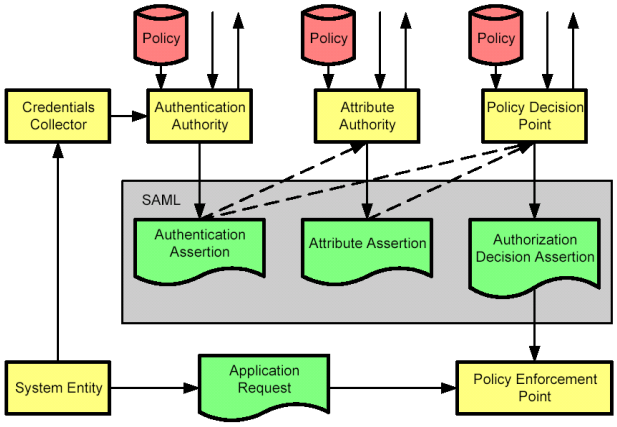
■비인가된 거래 및 사기
■기밀성 상실
■에러 감지
■괸리 및 회계에 있어서의 잠재적 손실
■잠재적인 법적 책임

이와 같은 위험의 주요 범주 및 일부 대응책을 간략하게 정의하였는데 비인가된 거래 및 사기의 범주에 속하는 위험 요소 중 Identification, Authentication, Authorization에 대한 대응책으로 SAML을 지목하고 있다[2].

ebXML의 현재 표준은 2.0 명세이다. OASIS/ebXML Registry Services 2.0 명세까지는 접근제어를 위해서 세 가지 역활(Role)과 각각의 권한(Permissions)을 정의해 놓았다. TC approved 상태의 OASIS/ebXML Registyr Information Model 명세 2.5에서는 XACML을 이용한 접근제어 모델(Access Control Model)을 구현 제시하고 있다[3].

2.2 SAML(Security Assertion Markup Language)

인증과 권한 정보 교환을 위한 XML기반의 Security specification으로 OASIS에서 표준안을 제정하였다[4].



(그림 1) SAML 아키텍처

XML스키마로 security assertion과 assertion의 요청, 응답에 대한 포맷을 정의하고 assertion사용에 관한 규칙들을 설명하고 있다 (그림 1). SAML은 서비스간의 인증 상호운용성을 제공하고 Single Sign On을 실현할 수 있다. 가장 중요한 목표는 보안서비스를 요구하는 다른 시스템간의 표준 인증방식으로 상호운용성을 도모하는 것이라 할 수 있다. SAML은 크게 인증(Authentication), 속성(Attribute), 권한(Authorization)에 관한 내용을 SAML 시스템에 요청하고 이에 대한 응답으로 assertioin을 받게 된다. 인증은 요청 주체에 대한 고유 ID와 같은 인증 정보를 일컫는 것이고, 속성은 요청 주체에 대한 속성에 대한 정보를 제공한다. 즉 email주소, 시스템이나 조직에서의 역할(role)등이 될 수 있다. 권한은 시스템의 리소스에 접근할 수 있는지 여부에 대한 요청이며 이 요청은 시스템 정책(Policy)에 따라 접근 여부를 허가 또는 거부하게 된다. 요청과 응답에 대한 메시지는 SOAP을 통하여 이루어지게 된다.

2.3 XACML(eXtensible Access Control Management Language)

XACML은 접근제어를 통해 보안이 요구되는 자원에 대해 미세한 접근제어 서비스를 제공할 수 있는 XML기반의 언어이다. 2003년 2월 18일 현재 XACML은 OASIS에서 표준으로 완료된 상태이다[5].

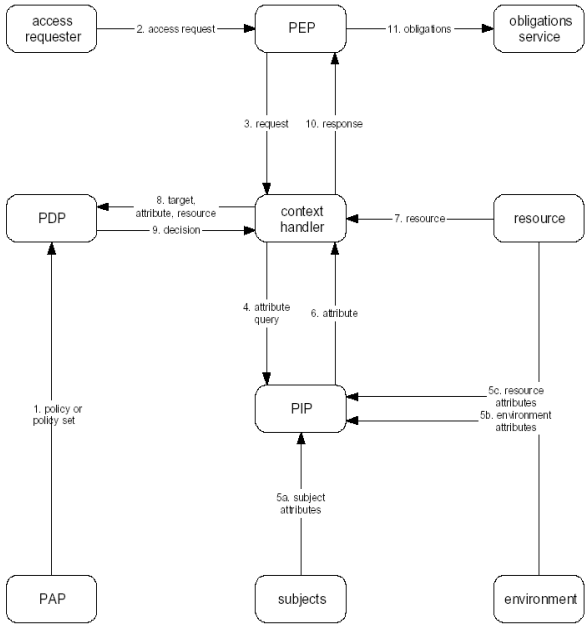
서브젝트(Subject)인 접근 주체는 XML문서 자원에 접근하기 위하여 접근하려는 자원의 요청정보가 담긴 Decision Request를 제출한다. XACML프로세서는 인증 정보를 바탕으로 정책에 따라 접근권한평가 후 권한에 따른 자원의 접근을 허가한다. 접근 주체는 권한에 따른 적절한 실행 결과를 알 수 있다.

2.3.1 데이터 흐름도

XACML의 데이터 흐름 모델은 (그림 2)와 같다. 다이어그램에서 보여주는 데이터 흐름은 저장소(repository)에서 유용하게 사용될 수 있는데 예를 들어 PDP(Policy Decision Point)와 PAP(Policy Administrator Point)사이의 통신이 적절하게 이용 될 수 있다. 그러나 XACML 명세서는 저장소에서의 사용이나 특정한 통신 프로토콜에서의 활용에 제한을 두고 설계되지는 않았다. 모델에서 보여주는 데이터의 흐름은 다음과 같은 순서를 따른다.

(1) PAP는 policy statements를 만들어서 PDP에서 사용가능 하도록 한다.
(2) 접근자는 PEP에 접근하기위한 요청을 한다.
(3) PEP는 context handler에 접근 요청을 전송한다. 접근 요청은 subject의 attribute, resource, action을 선택적으로 포함한다.
(4) PIP는 attributes를 요청할 수 있다.
(5) PIP는 요청된 attributes를 얻는다.
(6) PIP는 요청된 attributes를 context handler로 반환한다.
(7) Context handler는 context에 resource를 선택적으로 포함한다.
(8) Context handler는 PDP에 decision request를 전송한다.
(9) PDP는 context handler에 권한 결정을 포함한 응답 context를 반환한다.
(10) Context handler는 PEP에 응답을 반환한다.

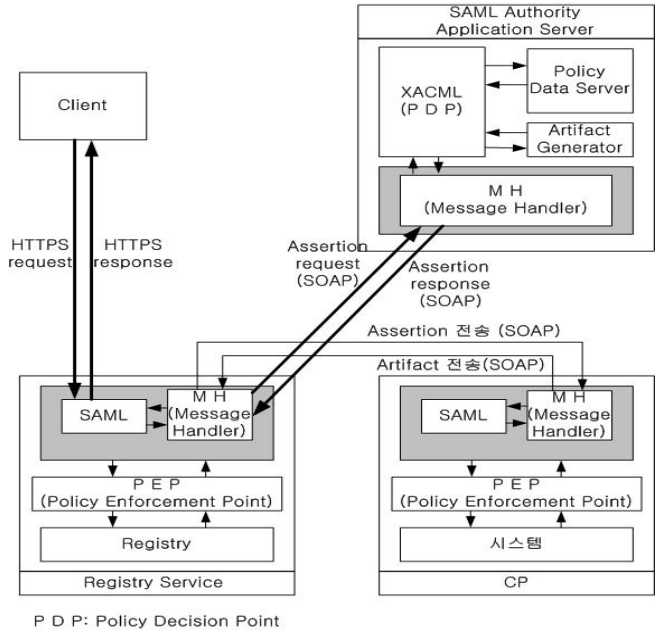
(11) Context handler는 응답 context를 PEP형식에 맞게 변환하고 PEP는 프로세스를 이행한다.
(12) 접근이 허용되면 PEP는 resource의 접근을 허용하고 허용되지 않으면 접근이 거부된다.



(그림 2) XACML 데이터 흐름도

3. SAML과 XACML의 연동

SAML 아키텍처의 Policy Decision Point의 역할을 XACML이 이행하면서 (그림3)과 같이 SAML과 XACML을 연동할 수 있다.



(그림 3) SAML과 XACML의 연동

클라이언트는 Registry Service 서버에 인증을 요청하게 되고 SAML을 이용한 인증 Agent는 Assertion request를 SAML Authority Application Server에 전달하게 된다. SAML Authority Application Server는 클라이언트의 정보를 가지고 Artifact를 생성하게 되고 XACML을 통해 클라이언트의 Policy를 결정하게 된다. 이때 생성된 Artifact는 일종의 token으로써 SSO(Single Sign On)을 구현할 수 있게 해준다.

Assertion response를 받은 SAML 인증 Agent는 SSO을 위해 Assertion과 Artifact를 가지고 있게 되고 ebXML에 적용하는 경우 Policy는 XACML의 PEP를 통해서 Registry에 대한 접근제어에 이용하게 되는 것이다.

XACML은 Decision Request 문서에 <표 1>과 같이 subject, resource, action 정보와 SAML의 인증, 승인, 역할 정보를 함께 가질 수 있으므로 SAML이 가지고 있는 정보를 그대로 사용한다.

<표 1> Decisioin Request의 기본 구조

```
<?xml version="1.0" encoding="UTF-8"?>
<Request>
<Subject>...</Subject>
<Resource>…</Resource>
<Action >...</Action>
<saml:Assertion>
   <saml:AuthenticationStatement>
   <saml:Subject> … </saml:Subject>
   </saml:AuthenticationStatement>
</saml:Assertion>
<saml:Assertion>
   <saml:AttributeStatement>
   <saml:Subject> ... </saml:Subject>
   <saml:Attribute AttributeName="role">...
   </saml:Attribute>
   </saml:AttributeStatement>
</saml:Assertion>
</Request>
```

이렇게 SAML과 XACML의 연동으로 구성된 인증 및 접근제어 모델은 XML을 사용하는 프레임워크에 적용이 가능하다. 특히 ebXML Registry에 적용할 경우 보안적인 측면에서 상당한 효과를 가져올 수 있다.

4. ebXML Registry에의 적용

SAML로 구현된 인증 Agent를 통한 접근은 ebXML이 안고 있는 Identification, Authentication 그리고 Authorization에 있어서 내재되어 있는 risk에 대응할 수가 있다. 또한 SAML을 거쳐서 인증을

받은 클라이언트는 XACML의 Rule을 따라서 Registry내의 리소스에 대한 접근제어를 받게 된다. 마지막으로 SAML의 사용으로 Registiry에 등록되어 있는 company와의 SSO 구현이 가능하다는 장점을 가지게 된다. SSO을 구현하기 위해서는 등록되어 있는 업체역시 SAML기반의 인증 Agent가 구축되어있어야 한다.

5. 결론 및 향후 과제

SAML서비스는 효율적인 인증정보를 제공하는 동시에 XML전자서명, 암호화와 함께 유기적으로 서비스가 제공되어 질 수 있다. 본 논문에서는 ebXML Registry서비를 위한 인증을 처리하기 위해 SAML 인증서비스 모델을 제시하였다

XACML은 XML자원의 미세한 접근을 제어하며 접근자의 특징적인 행위에 대한 정책을 수립하고 실행하므로써 효율적인 자원 관리를 할 수 있는 접근제어 표준 기술이다.

“Technical Architecture Risk Assessment v1.0”에서 나와 있는 ebXML에서의 위험은 다음과 같다.

■비인가된 거래 및 사기
■기밀성 상실
■에러 감지
■괸리 및 회계에 있어서의 잠재적 손실
■잠재적인 법적 책임

SAML과 XACML을 연동한 인증 및 접근제어 모델이 ebXML에 적용되는 경우 ebXML이 안고 있는 비인가된 거래 및 사기의 범주에 속하는 Identification, Authentication 그리고 Authorization에 대한 위험과 ebXML이 요구하는 접근제어를 동시에 해결 할 수 있다는 것을 알 수가 있었다. XACML API를 현재 개발 중이기 때문에 본 논문에서는 SAML과 XACML을 연동하는 모델만을 제시하였다. 향수 XACML API가 완성되면 실제로 이 모델을 구현 ebXML Registry에 적용을 할 것이다.

참고문헌

[1] ebXML, http://www.ebxml.org
[2] Technical Architecture Risk Assessment v1.0, http://www.ebxml.org/specs/secRISK.pdf
[3] OASIS/ebXML Registry Information Model Specification v2.5, http://www.oasis-open.org/committees/regrep/documents/2.5/specs/ebrs-2.5.pdf
[4] Security Assertion Markup Language (SAML), http://www.oasis-open.org/committees/security/
[5] OASIS eXtensible Access Control Markup Language,http://www.oasis-open.org/committees/xacml/