전자거래를 위한 XML기반 통합 접근 관리에 관한 연구

성백호*, 박병철*, 신동규*, 신동일*, 문기영**,이재승**

*세종대학교 컴퓨터 공학과
** 한국 전자 통신 연구원

A study of the EAM based on the XML for e-Commerce

Baek-Ho Sung*, Byung Chul Park*, Dong-Kyoo Shin*, Dong-il Shin*,
Ki-young Moon**, Jae Seoung Lee**

*Department of computer Engineering Sejong Univ.
** 3Electronics and Telecommunications Research Institute

요 약

전자거래의 환경이 확장됨에 따라 다양한 사용자와 자원을 관리해야 하는 어려움에 대두되고 있다. 사용자 인증에 관한 기술은 전자거래의 시발점이라는 측면에서 상당히 강조되어야 할 부분이다. 또한 개별적으로 구축하여 운영하고 있는 전산 시스템에서 개별적으로 관리되고 있는 자원과 사용자는 보안상의 문제점을 야기할 수 있다. 따라서 기업내부의 모든 자원과 이러한 자원을 이용하는 사용자에 대한 일관된 자원 및 사용자 관리체계의 구축하는 통합접근관리 기술을 도입하여 보안상의 취약점을 보완할 수 있다. 따라서 본 논문에서는 XML기반 e-business 프레임워크에서 기존 보안기술의 취약점을 보완할 수 있는 국제 표준화된 XML보안 기술을 적용한 통합접근 관리를 연구하였다.

I. 서론

최근 빠른 속도로 발전하는 인터넷 기반의 서비스의 확대에 따라 네트워크를 통한 시스템통합과 전자거래 시장에서 다양한 사용자와 자원을 관리해야 하는 문제점이 대두되고 있다. 이에 따라 증가한 사용자와 자원을 사용자에 따른 인증정보와 권한에 관한 세밀하고 통합적인 관리가 필요하다. 이에 최근 기업의 전자거래인프라는 여러 가지 방법으로 사용자 DB의 통합을 시도하고 있지만 자원관리와 사용자 접근권한의 관리가 서로 독립되어 있는 게 현실이고, 또한 다양한 사용자 관리의 어려움으로 인해 보안에 취약점이 생기기도 한다. 따라서 개별적으로 구축하여 운영하고 있는 전산 시스템에서 개별적으로 관리되고 있는 자원과 사용자를 기업내부의 모든 자원과 이러한 자원을 이용하는 사용자에 대한 통합을 통해서 일관된 자원 및 사용자 관리체계의 구축을 도입을 추진하고 있다. EAM(Enterprise or Extranet Access Management)[7]은 현재의 기업에서 부각된 문제에 대한 요구에서 출발한 분산되어 운영되고 있는 자원과 사용자에 대한 통합을 통한 일관된 관리체계를 구축하는 보안 솔루션이다. 하지만 통합접근관리(EAM)에 대한 기술은 개념만 나와 있고 아직 표준시스템 시나리오나 설계가 거의 없다. 따라서 본 논문은 XML기반 시스템에서 비즈니스 파트너들간의 거래를 지원하는 XML의 개발을 주도하고 있는 W3C와 OASIS는 XML Signature [1], XML Encryption[2], SOAP [3], XKMS [4], SAML[5]과 XACML[6]등 현재 표준화하거나 진행중인 XML문서의 보안을 위한 XML기반의 보안기술 명세를 적용하여 통합접근관리(EAM)에 관한 연구를 하였다.

II. 관련연구

1. 사용자 인증 및 자원접근관리

디지털 정보에 대한 인증 및 자원 접근 관리는 종래의 대면 및 서면 방식이 아닌 비 대면적인 전자적 거래정보 교환 방식이므로 상호 신뢰와 사용자의 권한에 맞는 자원접근은 거래를 수행하기 위해서 최우선 고려되어야 할 측면이다.

1)사용자 인증

사용자 인증이란 IT 환경에서 일련의 동작을 수행하는 주체가 누구인지를 알 수 있도록 하는 것으로서 Identity가 확인된 주체에 대해 실제 주체와 동일인임을 확인하기 위한 메커니즘을 말하고 자원 접근 관리는 정책에 따라 수시로 변경되는 세부적 리소스에 대한 접근 권한을 조회하여 접근 가능여부를 세부 리소스에 통보하는 것을 말한다. 이러한 과정은 통합된 관리자 인터페이스를 통하여 가능하다.

2) 자원 접근 관리

자원 접근 관리는 자원에 허가받지 않은 접근을 차단하여 시스템의 안전성을 보장해 주는 것이다. 자원접근은 특성에 따라 3가지의 관리 방법이 있다.

①User ID based Access Control

사용자 ID에 기반 자원에 대한 접근 관리 방법으로 가장 많이 사용되고 있는 방법이다. 하지만 ID만을 사용한 자원접근 관리는 사용자의 증가에 따른 ID 관리와 확장성에 문제가 있다.

②Role-based Access Control

역할에 기반을 둔 자원에 대한 접근 제어 방법이다. 각 사용자에게 사용자의 자격에 맞는 역할들이 할당되고, 각 역할에 대하여 권한이 설정된다.

③Attribute-based access Control

속성에 기반 자원에 대한 접근 제어 방법으로 Group, Role, Clearance 등과 같은 다양한 속성을 설정하여 권한 관리한다.

2. XML기반 시스템에서 기존 보안 기술 적용의 문제점

기존 전자거래 인프라는 개별적으로 구축하여 운영되고 있어서 타 시스템과의 상호운영성이 떨어진다. 따라서, 타 시스템사이의 데이터 연동시 많은 비용이 소요되는게 현실이다.

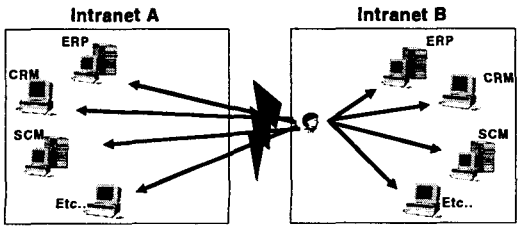

그림 1 기존의 기업환경

또한 기존의 전자거래 시스템은 보안을 위해 기본적으로 사용자 ID, 패스워드, PKI, IPsec, SSL, TLS, S/MIME등을 사용한다. 하지만 이러한 기술은 보안을 위해서 효과적으로 사용되지만 이를 사용하는 기업간의 확장성이 떨어지는 단점이 있고, XML기반의 시스템에서 XML 기술의 장점을 살리지 못한다. 예를 들면, SSL ,TLS와 같은 보안 기술은 전송하려는 데이터 전체에 대한 암호화를 수행함으로써 XML문서와 같이 데이터의 일부만 암호화가 필요한 경우에는 비효율적인 방법이다. 따라서 XML 정보보호 기술은 세계표준으로 이종 시스템과의 연동시 표준을 따르도록 구축을 하면 기존 시스템에서 발생하는 호환성 및 상호연동성 문제를 감소시킬 수 있다.

3. 관련 XML기반 보안 기술

1)XML전자서명(XML Digital Signature)

XML 전자서명은 XML의 장점인 구조적 정보 표현 능력 및 확장성을 기반으로 한 전자서명 기술로서 W3C와 IETF의 공동 표준이다. 기존의 전자서명의 경우 단일 홉(Single-hop) 메시지 전송에 적합한 메시지 인증 기능을 제공하지만 XML 전자서명의 경우 단일 XML 문서에 대한 다수의 전자서명을 포함할 수 있어 다중 홉(Multi-hop) 메시지 전송 모델 적합한 기술이다. 이러한 특징은 전자상거래 관련 메시지가 최종 목적지에 도달하기 전 여러 중간 경유지의 메시지 인증이 필요한 경우 매우 유용하다. 또한 XML 문서 전체에 대한 전자서명 뿐 아니라 개별적인 요소 또는 요소의 내용 자체에 세부적으로 전자서명을 수행 할 수 있다[1].

2)XML Encryption

기존의 보안기술은 데이터 전체에 대한 암호화를 수행함으로써 데이터의 일부만 암호화가 필요한 경우에는 비효율적인 방법이다. 이에 따라 데이터 중 일부분만을 암호화해 중간에 경유하게 되는 제 3자에게 특정 정보를 노출시키지 않으면서 최종 수신자에게 전달 할 수 있는 방법으로 현재 W3C에서 XML 기반의 표준화를 추진하고 있는 것이 XML Encryption이다. XML 전자서명과 통합 적용을 통해 송수신 메시지에 대한 기본적인 보안 요구를 만족시키기 위해 최적화되어 있다[2]. XML Encryption은 웹서비스와, ebXML프레임워크에서 메시지 기밀성 보장을 위한 표준 기술로 채택될 전망이다.

3) SAML(Security Assertion Markup Language)

SAML은 인터넷상에서의 자원 요청자에 대한 인증, 승인, 속성 확인 등을 수행하는 역할을 하며 이는 XML 기반의 다른 보안 기술들(XML 전자서명, XML Encryption, XKMS, XACML 등)과 통합되어 전체 보안 시스템을 구성하는 일부 요소로서 기능을 가진다. SAML 명세는 Assertion, 프로토콜, 바인딩으로 구성되어 있다. Assertion은 인증 및 승인 정보를 포함하는 XML 기반 구조를 가진다. 또한 Assertion의 인증을 위해 XML 전자서명을 적용한다. SAML 프로토콜은 XML 기반의 메시지 형태로서 요청 및 응답의 쌍으로 구성되어 각 Assertion에 대한 전송을 담당한다. SAML 바인딩은 SAML Assertion 요청 및 응답 프로토콜을 표준 메시지 전송 프로토콜과 연동함에 있어 처리되어야할 방식을 정의하고 있다. 현재 SOAP-over-HTTP 바인딩이 기본적으로 사용된다[5].

4) XACML(eXtensible Access Control Markup Language)

국제적인 컴소시엄인 OASIS에 의해 표준화된 XACML은 XML문서에 대한 접근을 정책리스트를 이용하여 제어할 수 있는 XML기반의 언어이다. XACML TC(Technical Committee)에서는 XACML로 정의된 기술로 정책과 인증을 표현하기 위한 XML 스키마를 제공하고 있다. 이 정책에서의 리소스는 XML을 사용하여 표현되는 어떠한 객체도 될 수 있으며 XACML은 XPath나 LDAP 등 다양한 프로토콜과 함께 바인딩하여 사용될 수 있으며 새로운 프로토콜과도 함께 사용될 수 있다. XACML은 인증시스템의 접근과 접근자 요청의 특징적인 역할에 대한 제어를 할 것으로 기대된다.[6].

Ⅲ. XML기반 통합접근관리 연구

1. 통합 접근관리(EAM)의 개요

EAM이란 SSO와 사용자의 역할(role)기반의 세분화된 접근 관리를 제공하는 적극적 시스템 인증, 제어관리 솔루션이다. SSO은 인증을 필요로 하는 서로 다른 사이트 간에 한번의 인증정보를 사용하여 인증을 수행한다. 현재 여러 사이트와 솔루션에서 많은 인증정보를 가지게 되므로 사용자는 리소스를 사용하기 위해 여러번의 인증 과정을 거쳐야 한다. 이러한 번거로움과 취약성을 해결하기 위해 SSO를 사용하여 한번의 인증으로 이 인증 시스템을 사용하는 사이트와 리소스를 사용하게 된다. 접근관리는 리소스에 대한 미세한 접근 제어를 수행하는 것으로 역할에 기반하여 정보를 제공한다. 접근은 시스템에서 정한 policy에 의해 판단되어 수행되며 이 판단 시스템 수행점을 PDP(Policy Decision Point)라고 한다. EAM은 복잡해진 기업환경과 e비즈니스를 위한 웹사이트를 안전하고 안정적인 운영능력을 부여하고 웹사이트를 이용하는 사용자의 편리성을 제공한다.

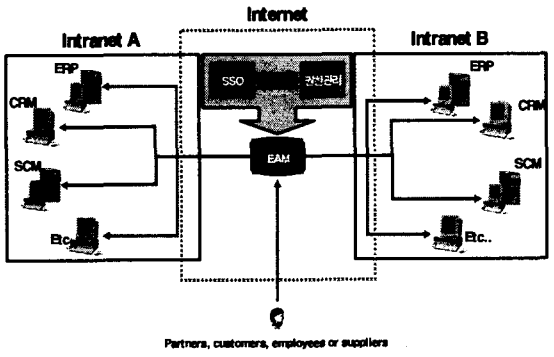

그림 2 EAM 적용

2. XML 정보보호기술을 적용한 통합 접근관리에 대한 연구

EAM에 적용 가능한 XML정보보호 기술은 표준인증 메커니즘인 SAML(Security Assertion Markup Language)과 자원 접근관리 표준 명세인 XACML이 있다. SAML은 일반 인터넷과 웹서비스를 위한 SSO와 접근제어를 위한 스키마를 정의하고 있어 EAM 솔루션으로 구축될 수 있다. SAML에서는 사용자의 인증 정보를 다룰 수 있는 인터페이스의 스키마나 전송규칙 등을 제정하며 기업의 정책을 결정하기 위한 수단과 방법, 파트너나 시스템의 통합에 대한 구체적인 방법에 대해서는 제공하지 않는다. 제공되지 않는 부분은 솔루션 구현에 따라 다양하게 이루어 질 수 있다. XACML은 접근제어 정책을 통해 보안이 요구되는 자원에 대해 미세한 접근 제어 서비스를 제공할 수 있는 XML 기반의 언어이다. XACML은 SAML PDP(Policy Decision Point)의 일부로서 역할을 수행 해 최종적인 자원 접근 요청에 대한 결과를 생성한다.

3. EAM 아키텍처

기본적인 EAM 시스템은 그림 3과 같다. 브라우저에서 사용자는 특정 서비스에 접근을 하려고 한다. 목적 서비스에 접근하기 전 인증과 접근 제어를 하기 위한 인증 web agent에 접속하게 되고 최초접속 시 인증의 과정이 수행되며 이후 시스템이 유지하는 세션 정보를 이용하여 정책에 따라

역할에 따른 접근제어를 수행한다. 정책은 policy 서버에서 유지하는 사용자 정보와 접근 제어 정보를 사용하여 접근 허용여부를 결정한다. 접근제어에 성공한 요청은 웹리소스에 접근할 수 있다.

EAM의 리포팅 기능은 인증과 권한 설정 같은 중요한 보안 이벤트를 관리하고, 고객의 사용 목적에 따라 커스터마이즈 될 수 있어야 한다.그리고 EAM 솔루션은 기존 솔루션과 통합되어 상호 보완 효과를 기업에게 줄 수 있어 전반적인 통합 관리를 용이하게 하고 안전하게 웹사이트를 관리할 수 있도록 한다.

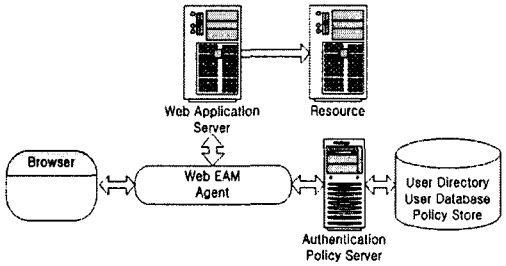

그림 3 표준 EAM 아키텍처

4. SAML 인증 아키텍처

SAML의 기본 기능은 인증서를 통한 객체의 인증이다. 인증서를 사용하기 때문에 강력한 인증을 보장할 수 있으므로 중요한 데이터의 전송과 처리, 시스템에 접근을 설정할 수 있다. 그러나 인증 시 기밀성과 무결성을 유지하기 위한 전자서명과 암호화가 이루어지므로 처리속도는 저하된다. 그러나 통합된 인증과 신뢰성있는 인증을 보장하는 것에 중요한 의미가 있다. SAML 인증의 아키텍처는 그림 4와 같다.

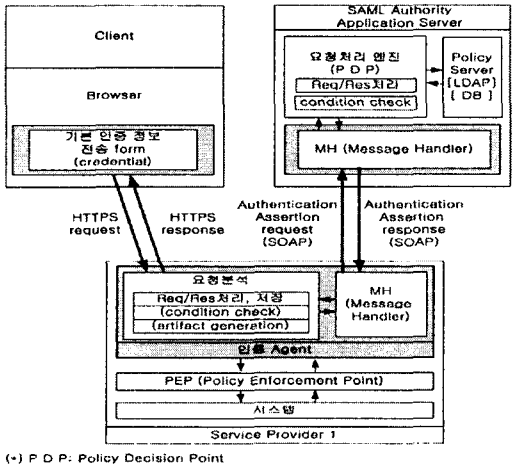

그림 4 SAML 적용 인증 아키텍처

5. XACML 접근 권한 결정 아키텍처

SAML의 권한결정 요청은 XACML 정책 서버에 의해 분석되어 지고 접근의 허가 여부를 리턴한다. Request는 접근 권한 제어에 대한 몇 가지 정보를 가지고 있다. Resource속성은 접근하려는 리소스의 URI를 제공하고 이 리소스에 대한 행위는 Action에서 제공한다. Evidence는 saml assertion을 제공하는 제공자를 의미한다. 즉 SAML Authority 자체에 대한 인증 assertion이다. Evidence는 있을 수도 있고 없을 수도 있다. Evidence는 SSO한 경우 다른 Destination 리소스에 접근했을 때 사용될 수 있다.

접근정책은 시스템의 구현에 따라 자유롭게 설정할 수 있으며 특별하게 요구되는 사항은 별도의 스키마의 확장을 통해 유연하게 정보를 제공하고 이를 처리하므로써 접근 제어를 할 수 있다. Request에 대한 Response는 접근 평가에서 Status로 성공, 실패 여부를 알려주며 이에 따라 접근자의 리소스에 대한 접근제어를 한다.

XACML 접근 권한 결정 아키텍처는 그림 5와 같다.

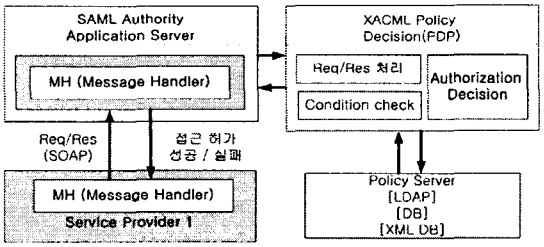

그림 5 XACML 접근 권한 결정 아키텍처

6. 통합 접근 관리(EAM) 아키텍처

아래 그림 6은 상기에 설계한 SAML과 XACML 아키텍처를 결합하여 사용자 인증과 자원 접근관리에 관한 일을 수행하는 아키텍처이다. 서비스 제공측은 자원의 접근제어를 위해 SAML Authority서비스를 인증 서비스로 이용한다. SAML Authority는 서비스제공자와 사용자 사이에 신뢰된 인증 서비스 시스템으로서 역할을 수행한다. 인증은 PKI, PMI등과 연동을 하여 좀더 강화된 신뢰성을 제공할 수 도 있다. 인증은 SAML Authority에서 수행하고 접근 권한에 대한 서비스는 XACML이나 독립적인 인트라넷내의 정책(Policy)서버를 통해 수행될 수 있다. subject가 신뢰하는 SAML Authority와 연계된 Policy server를 사용할 수도 있으나 이 방법은 효율성이 떨어

질 수 있다.

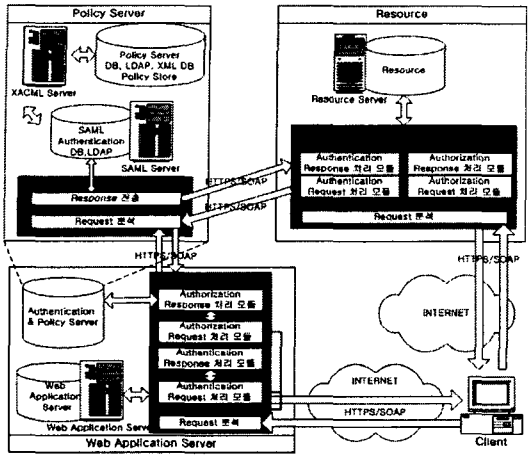

그림 6 EAM 통합 접근 관리 아키텍쳐

일반적으로 subject의 시스템 내에 신뢰하는 SAML Authority가 제공하는 policy 서버를 설치하며 해당 시스템의 정책에 따라 자원에 접근을 허가 또는 거부하게 된다. 자원에 인증과 요청 접근은 SAML에 의해서 이루어지고 policy에 관한 부분은 SAML에서 구체적인 구현 방식에 대해 언급하지 않는다. XACML은 이러한 부분을 보완해 준다. XACML은 사용자가 요청하는 자원에 대한 접근을 관리하며 만약 자원 접근에 권한이 없으면 서비스 거부를 통보하여 부적절한 사용자의 접근을 막을 수 있다. 권한에 대한 정보는 Policy 서버에 저장되어 있으며 이를 위해서 기존의 LDAP이나 XML DB를 사용할 수 있다.

Ⅳ. 결론 및 향후 과제

본 논문에서 XML기반의 보안기술 명세를 적용하여 통합접근관리(EAM)에 관한 연구를 하였다. 인터넷 기반의 확장과 더블어 비약적으로 증가하는 사용자 인증정보와 자원증가는 시스템의 비효율성과 신뢰성 저하를 야기할 것이다. 전세계를 무대로 하는 단일화 된 시장에서의 신뢰성있는 인증 및 자원 접근 제어 시스템은 Global시장을 형성하고, 확장시키는 기반이 될 것이다. 따라서, 증가하는 데이터와 이에 따른 시스템의 확장과 유지보수는 중요한 문제이다. 기존의 일반 웹사이트 및 차세대 전자거래 프레임 워크인 Web Services, ebXML등 다양한 환경에서 XML을 적용한 보안 프레임워크 표준이 개발되고 있다. 암호화, 전자서명, 접근제어, 인증 등의 다양한 보안 기술들은 XML포맷을 이용하여 확장성과 유연성을 가지고 여러 분야에 응용될 수 있다. 따라서 세계 표준인 XML기반 보안 기술을 적용한 통합접근관리의 활발한 기술개발과 보급이 이루어져야 할것이다. 향후 과제로 본 논문에서 연구한 통합접근관리 시스템의 구현과 PKI 및 PMI등과의 연동을 연구하여 시스템의 효율성을 검증하는 것이다.

참고문헌

[1] W3C Recommendation, M. Bartel, J. Boyer, B. Fox, B. LaMacchia and E. Simon. XML Signature Syntax and Processing. http://www.w3.org/TR/xmldsig-core

[2] W3C Recommendation, XML Encryption Syntax and Processing(2002), http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[3] W3C Recommendation, XML Protocol Working Group, Simple Object Access Protocol (SOAP) Version 1.2, http://www.w3.org/2000/xp/Group/

[4] W3C Working Draft. W. Ford, P. Hallam-Baker, B. Fox, B. Dillaway, B. LaMacchia, J. Epstein and J. Lapp. XML Key Management Specification (XKMS) 2003. http://www.w3.org/TR/2003/WD-xkms2-20030418

[5] OASIS Committee Specification, Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1 (2003), http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

[6] OASIS Standard, eXtensible Access Control Markup Language (XACML) Version 1.0, http://www.oasis-open.org/committees/documents.php?wg_abbrev=xacml

[7] Gartner Research Note, J. Pescatore, Extranet Access Management 2H01 Magic Quadrant, http://www.gartner.com/reprints/ibm/104593.html