유비쿼터스 환경에서의 안전한 웹 서비스를 위한 위임모델

황현식*, 고혁진*, 김규일*, 신준*, 옥지웅*, 박은경*, 김응모*
*성균관대학교 컴퓨터공학과
{hhs486, hjko, kisado, crashjun, okjwguy, okace, umkim}@ece.skku.ac.kr

Delegation Model to support Secure Web Services in Ubiquitous Environments

Hyun-Sik Hwang*, Hyuk-Jin Ko*, Kyu-Il Kim*, Jun Shin*, Jee-Woong Ok*, Ehun-Kyung Park*, Ung-Mo Kim*
*Dept of Computer Science, SungKyunKwan University

요 약

웹 서비스는 오늘날의 인터넷 환경에서 분산되어있고, 이질적인 시스템들 간에 상호운용을 제공하는 새로운 소프트웨어 시스템의 형태이다. 이러한 환경에 있어서 보안은 가장 중요한 이슈 중 하나이다. 공격자는 아무런 인증 없이 사용자의 비밀정보를 노출시킬 수도 있다. 더구나 유비쿼터스 환경에서 사용자들은 웹 서비스를 이용하기 위해 반드시 그들 대신 서비스를 처리할 에이전트들에게 그들의 권한 모두를 혹은 그 중 일부분을 일시적으로 위임해야만 한다. 이것은 사용자의 비밀정보가 에이전트들을 통해 외부에 노출되는 결과를 초래한다. 본 논문에서는 유비쿼터스 환경에서의 안전한 웹 서비스를 위한 위임모델을 제시한다. 우리는 에이전트를 통한 비밀정보의 노출을 막고 서비스의 기밀성과 단언정보의 무결성을 제공하기 위해 XML 암호화와 XML 전자서명 방식을 이용한다. 그리고 XACML 기반의 웹 서비스 관리 서버를 통해 웹 서비스 제공자들과의 서비스정책의 상호운용을 수행한다. 우리는 역시 멀티 에이전트들 간의 위임을 통해 웹 서비스 제공자들에게 전달될 위임 단언을 정의하기 위해 SAML 을 확장 시킨다.

1. 서론

웹 서비스는 XML 을 기반으로 SOAP, UDDI, WSDL 등의 공개표준을 이용하여 B2B (Business to Business)를 쉽게 통합하고, B2C (Business to Custom)간의 상호작용을 제공하기 위하여 고안되었다. 웹 서비스 제공자 (Web Service Provider)들은 자신들의 서비스를 WSDL (Web Service Description Language)을 이용하여 UDDI (Universal Description, Discovery and Integration) 레지스트리에 등록할 수 있고, 사용자들은 자신의 조건에 맞는 서비스를 찾고, 이용할 수 있다. 유비쿼터스 (Ubiquitous) 환경에서 사용자들은 웹 서비스를 검색하고, 이용하기 위하여 멀티 에이전트들을 이용한다. 멀티 에이전트들은 사용자의 자격 (Credential)정보를 전달하고, 사용자로부터 받은 정보를 가지고 사용자 대신 웹 서비스를 수행한다. 그리고 효율적인 웹 서비스를 제공하기 위하여 에이전트들은 자신의 업무를 다른 에이전트들에게 위임한다. 그러나 사용자는 웹 서비스 사용권한을 얻거나, 웹 서비스를 수행하기 위해 자신의 비밀 (Privacy)정보와 서비스정보를 에이전트들에게 노출시켜야 하고, 이는 사용자의 비밀정보가 외부에 노출될 수도 있는 결과를 초래 한다. 우리는 사용자의 비밀을 보호하고, 서비스의 기밀성과 무결성을 제공하기 위해서 XML 관련 보안기술들인 XML 전자서명과 XML 암호화 방식을 사용한다. 그리고 에이전

트를 통해 웹 서비스 제공자들에게 위임단언을 전달하기 위해서 SAML (Security Assertion Markup Language)을 확장한다. 또한 웹 서비스 제공자들과 상호운용하며, 인증된 사용자들에게 적합한 웹 서비스를 찾아 이용할 수 있는 역할 (Role)을 부여하기 위해 XACML (eXtensible Access Control Markup Language) 기반의 웹 서비스 관리 서버를 사용한다. SAML 과 XACML 은 OASIS 표준으로, 싱글 사인 온 (Single Sign-On), 신뢰(Trust)관리, 인증, 권한부여 등의 영역을 포함하고 있으며, 웹 서비스뿐만 아니라 다른 영역에서도 사용될 수 있다. 더 자세한 내용은 OASIS 표준명세서를 참고하기 바란다[1][2].

2. 관련연구

[4]에서는 제한된 위임을 위한 SAML 단언을 기술한다. 이 논문에서는 SAML 1.1 과 SAML 2.0 단언 명세서에서 제공되지 않는 SubjectStatment 를 SubjectDelegationStatement 로 확장한다. 우리는 SAML 1.1 과 SAML 2.0 단언 명세서에서 제공하는 AttributeStatement 를 확장하는 방법을 사용할 것이다. V. Welch[5]는 위임을 제공하기 위하여 X.509 인증서 (Certificate)를 확장시킨 Proxy X.509 인증서를 정의하며 이 방법은 현재 Globus 프로젝트[6]에서 이용되고 있다. Proxy X.509 인증서는 상당히 유용한 방식이나 웹 서비스를 위한 상용화 툴들은 이러한 인증서들을 올바르게 인식하지 못한다[10]. J. Y. Hu[7]는 PKI (Public Key Infrastructure)를 기반으로 하여 에이전트 시스템을 어떻게 구성하는가를 기술하였다. 위임과 관련해서는 사슬규칙 (Chain-ruled) 위임, 임계치 (Threshold) 위임, 조건부 (Conditional) 위임을 고려했다. 그러나 이러한 방법은 모바일 에이전트 시스템이나 이종의 멀티 에이전트 시스템에는 적용하기 어렵다. [8]은 모바일 에이전트를 위한 접근제어 구조를 기술했다. 이 논문에서는 위임을 제공하기 위해서 역할 (Role)을 모바일 에이전트에게 할당하는 방식을 사용한다.

3. 멀티에이전트를 이용한 위임모델

3.1 가정

우리의 모델은 다음의 가정들을 기반으로 한다.

가정 1 *웹 서비스 관리서버와 웹 서비스 제공자들은 인증/위임기관과 신뢰관계 (Trust Relationship)를 갖는다. - 인증/위임기관이 인증/인가한 사용자/에이전트들은 신뢰할 수 있다.*
가정 2 *사용자는 인증기관에 미리 등록되어있고, 웹 서비스관리 서버에 계정을 갖고 있다. - 웹 서비스 사용자로써의 역할 (Role)을 가지고 있다.*
가정 3 *웹 서비스 관리 서버가 인가된 사용자들에게 부여하는 역할은 사용자의 검색조건에 맞는 웹 서비스 제공자들의 역할과 공유되는 역할이다.*

3.2 컴포넌트

우리의 모델은 사용자가 자기 자신의 특권 (Privilege)의 위임을 관리할 수 있도록 한다. 에이전트들은, 사용자와 에이전트를 식별하여 인증 (Authentication)하는, 인증기관 (Authentication Authority)과, 위임 받고자 하는 에이전트의 위임을 인가 (Authorization)하는, 위임기관 (Delegation Authority)의 도움을 받아 사용자에 의해 위임 받은 특권에 따라 서비스 이용을 제어한다. 다음은 우리의 위임모델의 기본적인 컴포넌트들이다.

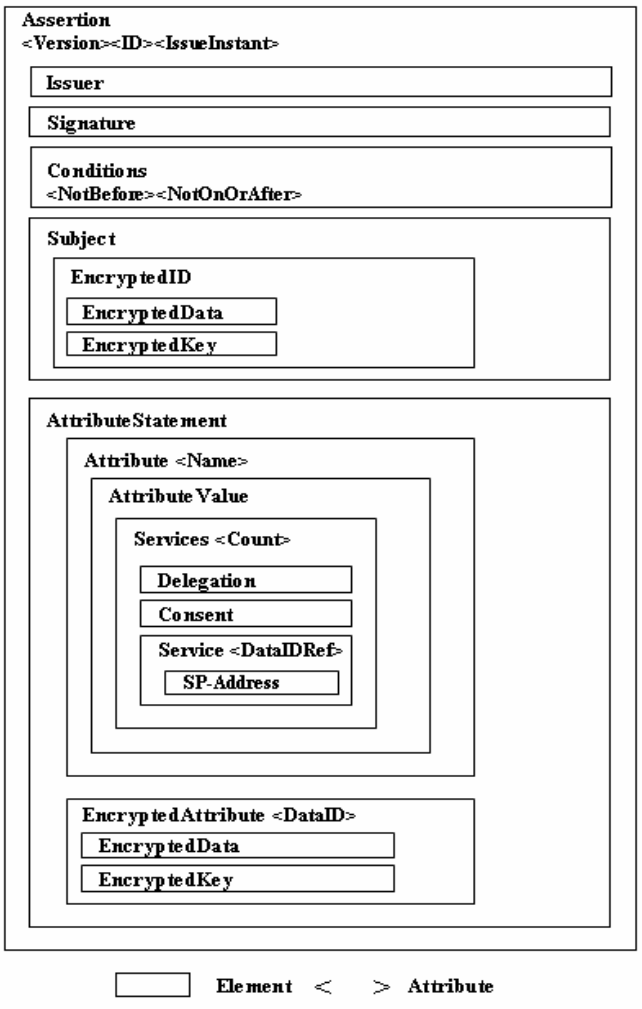
정의 1 *(주체). 주체(P)는 역할을 가지고, 웹 서비스를 수행하기 위해 자신의 특권을 에이전트들에게 일시적으로 위임하는 사용자이다. 역할은 웹 서비스 관리서버에게 특정 조건들과 주체의 자격정보와 함께 웹 서비스 요청을 함으로써 획득된다.*
정의 2 *(주체 에이전트). 주체 에이전트(Pa)는 주체와 상호작용하고, 주체대신 다른 에이전트들과 상호 작용하는 소프트웨어이다.*
정의 3 *(전달 에이전트). 전달 에이전트(Ca)는 그것이 오직 위임단언을 전달한다는 것만 제외하고 Pa 와 유사하다.*
정의 4 *(서비스 에이전트). 서비스 에이전트(Sa)는 그것이 웹 서비스 제공자의 에이전트인 것만 제외하고 Pa 와 유사하다.*
정의 5 *(인증기관). 인증기관(AA)은 주체와 에이전트를 인증하는 기관이다. AA 는 주체와 에이전트가 인증되었는지를 나타내는 인증단언을 발행한다.*
정의 6 *(위임기관). 위임기관(DA)은 주체의 특권을 에이전트들에게 인가하기 위한 기관이다. DA 는 자신이 주체의 권한을 주체/에이전트에서부터 에이전트들에게 인가한다는 것을 보증하는 위임단언을 발행한다. 위임단언을 발행하기 전에 DA 는 반드시 AA 를 통해 위임 받을 에이전트의 인증단언을 획득해야 하고, Pa 에게 위임단언 발행에 대한 동의를 얻어야 한다.*
정의 7 *(웹 서비스 관리서버). 웹 서비스 관리서버 (WSMS)는 웹 서비스 제공자들과 상호작용하고, 주체의 요청을 처리하는 시스템이다.*

3.3 웹 서비스 관리서버(WSMS)

WSMS 는 웹 서비스 제공자들의 서비스를 등록하고, AA 에 의해 인증된 주체의 검색조건에 따르는 적합한 서비스를 UDDI 레지스트리에서 찾아 역할 (Role)을 부여하는 시스템이다. WSMS 는 주체들에게 적합한 역할을 부여하기 위해 관련된 서비스 제공자들과 상호 작용하여 정책들을 모으고, 서비스를 이용할 수 있는 최소한의 특권 (Least Privilege)을 가진 역할을 부여한다. 역할의 부여는 역할계층 (Role Hierarchy)을 고려하는데 만약 서비스를 이용할 수 있는 최소한의 특권이 주체가 가진 역할보다 상위계층이면, 역할은 부여되지 않는다. 그리고 부여된 역할은 특정한 제한시간 (Time Constraint)을 가지는데, 제한시간이 지난 역할은 유효성을 상실한다.

3.4 위임단언

SAML 명세서[1]는 세 가지 다른 타입의 단언문(Assertion Statement): Authentication Statement (주어진 시간에 대상이 특정 수단에 의해 인가되었다는 것을 나타내는), AuthorizationDecision Statment (접근요청에 대해 접근의 허가되었는지 거부되었는지를 나타내는) 그리고 Attribute Statement (대상이 주어진 속성들과 값들과 관련되어있다는 것을 나타내는)를 정의한다. 그러나 위임을 위한 스키마는 SAML 명세서에 직접적으로 정의되어 있지 않다. 그러나 다행이 SAML 은 스키마의 확장을 허용한다. 우리의 위임단언을 생성하기 위해서 우리는 이러한 특성을 이용할 수 있다. 우리는 위임에 관한 정보를 담기 위해 속성단언 (Attribute Assertion)을 확장한다. (그림 1)에서는 위임단언의 구조를 기술한다.



(그림 1) 위임단언의 구조

• Issuer: 위임단언의 발행자, DA.
• Signature: DA 의 전자서명.
• Conditions: 위임단언의 유효기간. NotBefore 와 NotOnOrAfter 속성(attribute)들은 유효한 기간을 나타내는데 사용된다.
• Subject: 이름 식별자(Name identifier)같은 주체의 정보를 포함한다.
• EncryptedID: AA 의 공개키에 의해 암호화된 형태의 이름 식별자. 이것은 사용자의 비밀보호(Privacy Protection)를 제공한다.
• Name: 속성의 이름.
• Count: 서비스의 개수.
• Delegation: 이 위임단언을 받은 에이전트가 다른 에이전트들에게 과제를 위임하는 것이 허가되었는지 여부를 나타낸다. 만약 이것이 true 이면 재귀적인 위임의 자격이 부여된다.
• Consent: DA 가 위임단언을 발행하는데 있어서 사용자의 동의를 얻었는지 여부를 나타낸다. 만약 이것이 true 이면 동의는 얻어진 것이다.
• Service: IDRef 속성에 의해 EncryptedAttribute 를 참조할 수 있다.
• SP-Address: 서비스 제공자(Service Provider)의 URL.
• EncryptedAttribute: 서비스를 수행하기 위한 주체의 입력데이터. 이것은 WSDL 의 입력 (Input)에 따른다. 이것은 서비스의 기밀성 (Confidentiality)을 제공하기 위하여 서비스 제공자의 공개키로 암호화된다.

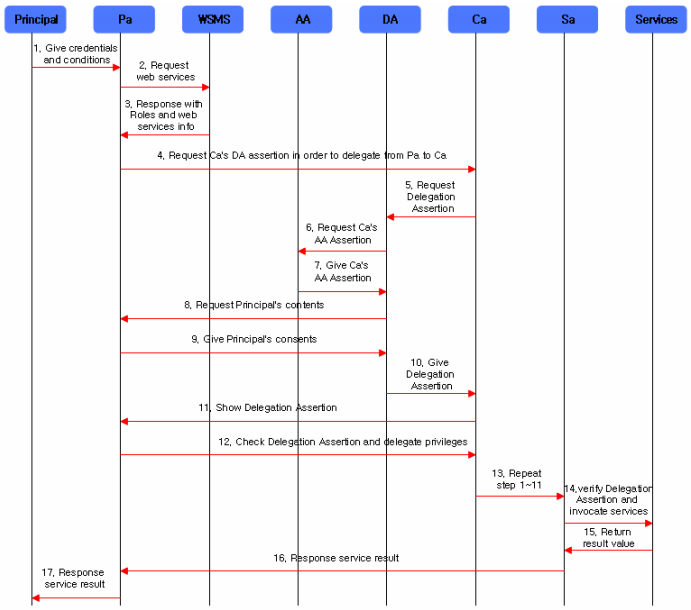
```
<Assertion ID="_a75ad55-010d-dads142-rchadb434d"
        IssueInstant="2005-03-05T02:46:02Z" Version="2.0">
  <Issuer>http://www.delegation-authority.com</Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    digital signature of delegation authority </ds:Signature>
  <Conditions NotBefore="2005-03-05T02:46:02Z"
        NotOnOrAfter="2005-03-05T02:55:00Z">
  <Subject>
    <EncryptedID>
      <xenc:EncryptedData> ... </xenc:EncryptedData>
      <xenc:EncryptedKey> ... </xenc:EncryptedKey>
    </EncryptedID>
  </Subject>
  <AttributeStatement>
    <Attribute Name="DeleInfo1">
      <AttributeValue>
        <Services count="2">
          <Delegation>true</Delegation>
          <Consent>true</Consent>
          <Service DataIDRef="Serv1">
            <SP-Address>http://www.SP1.com</SP-Address>
          </Service>
          <Service DataIDRef="Serv2">
            <SP-Address>http://www.SP2.com</SP-Address>
          </Service>
        </Services>
      </AttributeValue>
    </Attribute>
    <EncryptedAttribute DataID="Serv1">
      <xenc:EncryptedData> ... </xenc:EncryptedData>
      <xenc:EncryptedKey> ...</xenc:EncryptedKey>
    </EncryptedAttribute>
    <EncryptedAttribute DataID="Serv2">
      <xenc:EncryptedData> ... </xenc:EncryptedData>
      <xenc:EncryptedKey> ... </xenc:EncryptedKey>
    </EncryptedAttribute>
  </AttributeStatement>
</Assertion>
```

(그림 2) 위임단언의 예제

(그림 2)는 위임단언의 예제를 보여준다. 우리는 어떻게 <EncryptedData>와<EncryptedKey>를 처리하는지 설명하지 않지만 이것은 XML 암호화 명세서[3]에 기술된 방법을 이용하여 처리될 수 있다.

3.5 멀티에이전트를 이용한 위임모델의 상호작용

(그림 3)은 멀티 에이전트를 이용한 위임모델의 순서도표 (Sequence Diagram)를 기술한다.



(그림 3) 위임모델의 순서도표

4. 결론

본 논문에서는 유비쿼터스 환경에서 멀티 에이전트를 이용하여 안전한 웹 서비스를 이용하기 위한 모델을 제시하였다. 우리는 3.4 단락에서 언급한 위임단언을 이용하여 사용자의 비밀보호와 서비스 기밀성을 제공하였다. 그리고 멀티 에이전트를 이용하여 사용자의 특권을 재귀적으로 위임함으로써 서비스 이용의 효율성을 증가시켰다. 다음 연구에서는 메모리의 용량에 제한이 있는 모바일 디바이스에 위임모델을 적용시킬 것이다.

참고문헌

[1] OASIS "Security Assertion Markup Language(SAML) V2.0".
OASIS Standard, 15 March 2005

[2] OASIS "eXtensible Access Control Markup Language(XACML) V2.0".
OASIS Standard, 1 February 2005

[3] XML Encryption Syntax and Proceeding, http://www.w3.org/TR/2002/REC-xmlenc-core-2002121

[4] G. Navarro, B.S. Firozabadi, E. Rissanen and J. Borrell, Constrained delegation in XML-based Access Control and Digital Rights Management Standards, 2003

[5] V. Welch, I. Foster, C. Kesselman, O. Mulmo, L. Pearlman, S. Tuecke, J. Gawor, S. Meder and F. Siebenlist, X.509 Proxy Certificates for Dynamic Delegation, In 3rd Annual PKI R&D workshop, 2004

[6] Globus, http://www.globus.org

[7] Y. J Hu,Some thoughts on agent trust and delegation, In Proceedings of the fifth International Conference on Autonomous Agents, 2001

[8] G. Navarro, J. A. Ortega-Ruiz, J. Ametller, S. Robles,Distributed Authorization Framework form Mobile Agents, 2003

[9] Hidehito Gomi, Makoto Hatakeyama, Shigeru Hosono, Satoru Fujita, A Delegation Framework for Federated Identity Management, In Proceedings of DIM workshop, 2005

[10] Jun Wang, David Del Vecchio, Marty Humphrey, Extending the Security Assertion Markup Language to Support Delegation for Web Services and Grid Services, In Proceedings of the IEEE International Conference on Web Services, 2005