SAML을 이용한 그리드 단일 인증 보안 기법

김용철° 허의남 황준 김영찬
중앙대학교 컴퓨터공학과 서울여자대학교 정보통신공학부
{pertzs°, yckim}@sslab.cse.cau.ac.kr {huh, hjun}@swu.ac.kr

Grid Single Sign-On Security Mechanism Using SAML

Yongchul Kim° Euinam Huh Jun Hwang Youngchan Kim

Dept. of Computer Science, ChungAng University, Dept. of Computer Science, Seoul Women's University

요 약

그리드는 고성능 컴퓨터, 대용량 데이터베이스, 각종 정보통신 첨단장비 등을 초고속 네트워크로 연동해 상호 공유하는 핵심기술과 운영체제를 말하며, 이를 효율적으로 활용하기 위해서는 자원의 특성과 사용자의 신원에 의해 제한적으로 액세스가 가능한 메커니즘과 신원이 확인된 사용자의 권한 유무를 검증할 수 있어야 한다. 따라서 사용자와 관리자 양방의 편리성과 안전성을 위해 그리드의 보안은 단일 인증 기능을 제공해야 하는데, 기존의 방식은 공개키 인증서 방식의 복잡한 알고리즘을 사용하므로 인증 시간이 오래 소요되며, 전체적으로 그리드 성능을 저하시키는 요인이 된다. 따라서 본 논문에서는 이를 해결하기 위하여 SAML을 이용한 그리드 단일 인증 보안 기법을 제안하고자 한다.

1. 서 론

그리드는 고성능 컴퓨터, 대용량 데이터베이스, 각종 정보통신 첨단장비 등을 네트워크로 연동해 상호 공유하는 핵심기술과 운영체제를 말한다. 엄청난 양의 데이터 처리를 위해 전 세계 컴퓨터들을 인터넷으로 연결해 마치 하나의 슈퍼컴퓨터처럼 사용하자는 개념으로 시작하였다. 특히나 과학 기술 및 산업계에 종사하고 있는 개인 및 조직들은 자원을 공동으로 이용하여 공통 목표를 추구하는 가상조직(Virtual Organization)을 구축하는 것을 목적으로 그리드에 대하여 많은 연구를 진행하고 있다[1].

그리드를 효율적으로 구축하기 위해서는 자원의 특성과 사용자의 신원에 의해 제한적으로 액세스가 가능한 자원을 공유할 수 있는 메커니즘과 사용자의 신원을 확인할 수 있는 능력, 그리고 신원이 확인된 사용자가 해당 자원을 액세스하기 위한 권한이 있는지의 여부를 검증할 수 있어야 한다. 따라서 이러한 요구를 바탕으로 그리드 연구 그룹에서는 GSI(Grid Security Infrastructure)라는 인증 및 권한과 관련된 인프라를 개발하여 사용하고 있다. GSI는 안전한 단일 인증(Single Sign-On), 액세스 정책과 로컬 사이트 보안에 따른 제어, 원격 로그인 및 안전한 보안 응용을 수행하기 위한 인터페이스를 제공하고 있다[2].

글로버스 GSI에서는 단일 인증을 구현하기 위하여 Proxy라는 개념을 이용한다. 하지만 Proxy 자체가 공개키 인증서 방식으로 구현되었기 때문에 공개키를 다루는 과정에서 복잡한 알고리즘을 사용해야 하므로 인증과정이 오래 소요되며, 사용자가 그리드 자원을 사용하는 중에 인증 단계를 계속해서 거쳐야 되므로 이러한 공개키 방식으로 구현된 사용자 Proxy는 전체적으로 그리드 성능을 저하시키는 요인이 된다[2].

이를 해결하기 위하여 본 논문에서는 SAML을 이용한 그리드 단일 인증 보안 메커니즘을 제안하고자 한다. SAML은 국제 컨소시엄인 OASIS(the organization for the Advancement of Structured Information Standards)에서 제정된 표준이며 S2ML(Security Services Markup Language)의 원리와 구조를 재사용하고, 신뢰할 수 있는 Single Sign-On, 인증 서비스, B2B Transaction, Sessioning같은 기능을 가진다[3].

이 논문의 구성은 다음과 같다. 먼저 2장에서는 본 논문에서 필요한 관련연구를 살펴보고, 3장에서는 본 논문에서 제안하는 기법에 대해 설명할 것이며, 4장에서는 향후 연구 방향을 제시하였다.

2. 관련연구

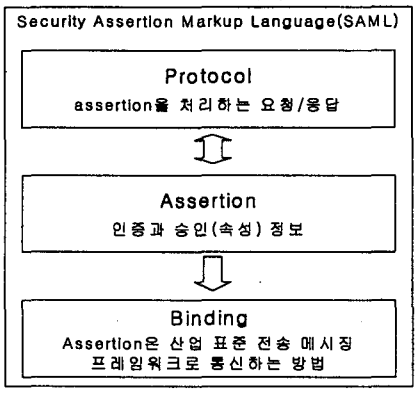
2.1 Grid VO (Grid Virtual Organization)

그리드 컴퓨팅과 기존의 컴퓨팅 환경과 비교할 때 가장 두드러진 차이점이 가상조직(VO)을 가능하게 한다는 것이다. 기존의 인터넷 컴퓨팅 환경은 어떤 물리적으로 나누어진 조직 또는 도메인과 이에 속한 개인이 다른 조직 또는 개인과 단순히 정보만을 공유할 수 있었다. 하지만 그리드 컴퓨팅은 물리적으로 다른 조직 또는 개인이 이런 한계를 넘어 가상의 공간에서 새로운 조직을 형성할 수 있도록 한다. 이런 가상의 조직에서 조직 또는 개인은 정보의 공유뿐만 아니라 자신이 가지지 못한 다양한 자원에 대해 사용할 수 있는 권리를 가질 수 있다. 또한 어떤 조직 또는 개인이 여러 가지 다양한 가상의 조직에 참여할 수 있게 된다.

2.2 SAML (Security Assertion Markup Language)

SAML은 XML 문서를 통해 인터넷상에서 보안 정보를 교환과 공유를 목적으로 하는 프레임워크이다. 이는 국제 컨소시엄인 OASIS에 의해 표준화되었으며, Netegrity에서 제정된 S2ML의 공인되고 신뢰된 기능만을 정의하고 가능한 많은 원리와 구조를 재사용하였기 때문에 보안 서비스의 제공과 서로 다른 시스템들 사이에 상호이

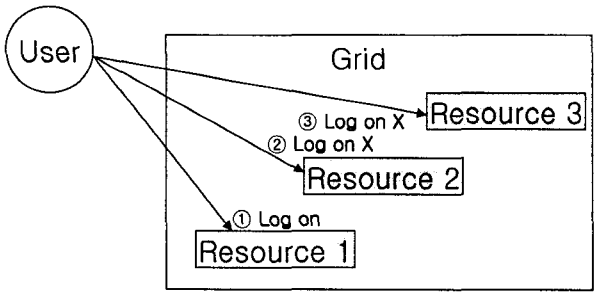
용이 가능하다. 또한 SAML을 이용하면 사용자는 사용자 인증을 한 사이트나 기업에서 받은 후에 인증해준 사이트나 기업과 서로 인증된 파트너 기업의 사이트를 검색할 수 있는 단일인증이 가능하다[3].



[그림 1] SAML의 기본 구조

2.3 SSO (Single Sign-On)

단일인증(SSO)란 그리드 상의 어떤 자원에 접근하기 위한 인증을 받기 위해서 사용자의 추가적인 인증과정이 없이 사용자는 단지 한번만 "log on"을 하는 것을 의미하는 것을 말한다.

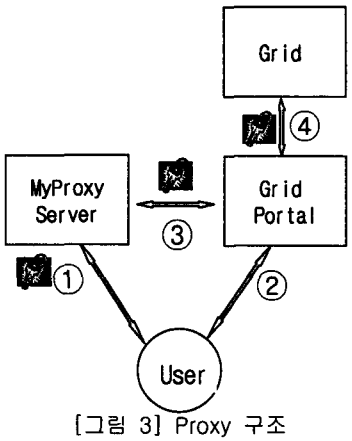


[그림 2] 단일인증 (SSO)

그리드에서의 보안 문제는 자원들이 고가이고, 그리드 상에서 수행되는 애플리케이션 또한 중요한 것이기 때문에 아주 중요하다. 각 자원들은 여러 기관에 흩어져 있고 나름대로의 보안 정책을 가지고 있다. 사용자 입장에서는 안전하면서도 사용의 편리성을 요구할 것이고 각 자원을 소유하고 관리하는 관리자 입장에서는 자원이 그리드 환경에 노출되는 것이기 때문에 사용의 편리성보다는 더 안전한 보안을 요구할 것이다. 따라서 사용자와 관리자 양방의 편리성과 안전성을 위해 그리드의 보안은 단일 인증 기능을 제공해야 한다. 사용자는 그리드 환경에서 단 한 번의 인증 과정을 거침으로써 그리드에서 사용이 허용된 모든 자원들을 쉽고 안전하게 사용할 수 있어야 한다는 것이다. 현재 그리드 환경에서는 이를 구현하기 위해 Proxy의 신임장 발부 기법을 사용하고 있으며 이 방식은 공개키 인증서 기반의 복잡한 알고리즘을 사용하고 있다.

2.3 Proxy

그리드 시스템에서는 단일인증을 구현하기 위하여 Proxy를 사용하며, 현재 사용 중인 시스템으로 MyProxy가 있다[4]. 이 시스템을 단일인증을 위하여 다음과 같은 시스템 구조를 가진다.



[그림 3] Proxy 구조

사용자는 MyProxy Client 프로그램을 사용하여 MyProxy Server에게 신임장을 위임하고, 이를 보호하기 위해 사용자 이름과 패스워드를 선택한다. 이 때에 사용자는 신임장의 생명주기를 정할 수 있다. 이후 사용자는 웹 브라우저를 사용하여 그리드 포탈에 접속하고 사용자 이름과 패스워드를 제공한다. 이 후 그리드 포탈은 MyProxy 서버에게 사용자 이름과 패스워드 검증을 요구하고 MyProxy 서버는 단기간 신임장을 발부한다. 마지막으로 그리드 포탈은 발부받은 단기간 신임장으로 사용자를 대신하여 그리드 자원에 접근할 수가 있는 것이다.

2.4 CAS (Community Authorization Service)

분산 가상 통신의 연산과 표준화에 관련된 가장 큰 문제는 커뮤니티의 정책을 명세하고 적용하는 것이며 기존 방식에서는 프로젝트 관리자가 자원 소유자와 연락하여 계정을 생성하고 할당 받아야 하는 불편함이 있었다. 이를 위해 글로버스 CAS 구조가 제안되었고, 이는 자원 제공자와 사용자간에 신뢰 받는 제 3의 호스트 존재하며, 이를 CA(Community Authority)라고 한다. CA는 모든 구성원과 세밀한 접근 제어 정책들을 유지, 관리 하며 글로버스 CAS는 확장성과 유연성을 위해 분산된 관리 기법을 제공한다[5].

3. SAML를 이용한 제안기법

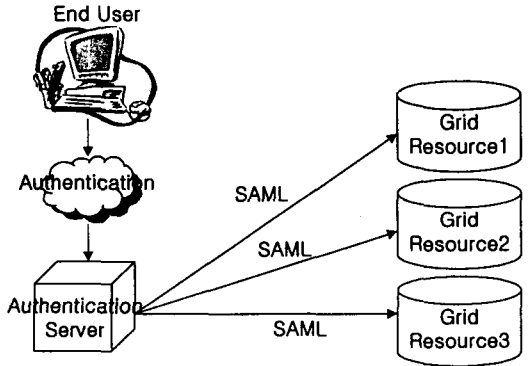
현재 그리드 시스템에서는 단일 인증을 구현하기 위하여 공개키 인증서 방식의 Proxy를 사용하고 있으며, 이는 복잡한 알고리즘을 사용하기 때문에 인증과정이 오래 소요되며, 그리드 자원을 사용하는 중에 인증 단계를 계속해서 거쳐야 하므로 Proxy는 전체적으로 그리드 성능을 저하시키는 요인이 된다. 이를 해결하기 위해 본 논문에서는 복잡한 공개키 방식 대신에 SAML을 이용하여 그리드 단인일증 과정에서 보다 높은 성능을 얻을 수 있

는 기법을 제안하고자 한다.

SAML 구조는 SAML 주장(Assertion), 프로토콜(Protocol), 바인딩(Binding)과 프로파일(Profile)로 분류할 수 있으며, 이 중에서 주장은 인증, 속성, 권한으로 구성되고, 전자 서명으로 승인된다. 이른바 SAML의 주장이 단일인증의 필수요소를 내포하고 있으며, 프로토콜 바인딩을 통해서 보안 도메인 또는 여러 권한 정책을 가지는 여러 사이트에서 단일인증을 실현할 수 있는 것이다. 다음은 간단한 SAML의 Assertion의 한 예제로서 이 구문으로 간단히 SAML를 이용한 단일인증을 설명할 수 있다.

```
<saml:Assertion
 MajorVersion="1" MinorVersion="0"
 AssertionID="186CB370-5C81-4716-8F65-F0B4FC4B4A0B"
 Issuer="www.example.com"
 IssueInstant="2001-05-31T13:20:00-05:00">
 <saml:Conditions
  NotBefore="2001-05-31T13:20:00-05:00"
  NotAfter="2001-05-31T13:25:00-05:00"/>
   <saml:AuthenticationStatement
    AthenticationMethod="password"
    AuthenticationInstant="2001-05-31T13:21:00-05:00">
    <saml:Subject>
     <saml:NameIdentifier>
      <SecurityDomain>"www.example.com"</SecurityDomain>
       <Name>"cn=Alice, co=example, ou=sales"</Name>
     </saml:NameIdentifier>
    </saml:Subject>
   </saml:AuthenticationStatement>
</saml:Assertion>
```

[그림 4]에서 볼 수 있듯이, 사용자가 PMI(Permission Management Infrastructure)에 접속하여, 인증을 받으면, SAML Assertion이 생성되며, 이 Assertion의 내용에는 AssertionID와 발행자 그리고 조건으로 생명주기를, 인증 메서드로 패스워드를 사용한다는 내용을 알 수 있다. 이를 현존하는 그리드 시스템의 Proxy와 비교해 본다면, 복잡한 알고리즘을 사용하는 공개키 연산을 피하고, 프로토콜 바인딩을 통해 이미 인증 받은 사실을 다른 사이트에 통보하는 것이다. 따라서 인증 소요 시간과 공개키 연산을 상당 부분 줄일 수 있을 것이다.



[그림 4] 멀티 도메인에서의 SAML을 사용한 단일인증

이 SAML을 이용한 단일인증 기법은 기존 방식의 공개키 연산이 불필요 할뿐 아니라, SAML이 S2ML의 정당한 모든 기능을 정의하고 있으므로, 각기 다른 인증 정책을 사용하는 다른 기관에게도 복잡한 인증과정이 필요 없게 되며, 보다 유연하게 단일인증 과정을 효율적으로 수행할 수 있다.

4. 결론 및 향후연구

그리드 네트워크에는 수많은 이질적인 호스트와 기관들이 각기 다른 커뮤니티 정책과 로컬 알고리즘을 가지며 현존하고 있다. 그리드의 특성상 고성능 컴퓨터, 대용량 데이터베이스, 고가의 정보통신 청단장비를 연동하는데 있어 이는 커다란 성능저하의 원인이 되고 있으며, 이를 해결하기 위해 단일인증 기능을 서비스에 부가하고 있지만, 또한 이 기능으로 인해 그리드의 성능저하를 피할 수 없게 되었다. 하지만 SAML을 그리드 환경에 적용하면, 기존 기법에서 사용한 공개키 연산을 피할 수 있고, 보다 유연하고 효율적인 단일인증을 실현할 수 있으며, 그 결과 높은 성능을 꾀할 수 있다.

향후 연구로는 이 기법을 그리드 가상조직에 연동해, 한번의 단일인증으로 멀티캐스팅을 사용해 가상조직 내의 모든 호스트들의 자원을 이용할 수 있는 기법이 있겠으며, SAML 자체의 보안 취약점에 대해서도 연구할 것이다.

5. 참고문헌

[1]"그리드 컴퓨팅, 인터넷을 통한 자원 대 통합", 마이크로소프트웨어 7월호 pp.204-270, 2002.

[2]Security for Grid Services. V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Cajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, S. Tuecke. Twelfth International Symposium on High Performance Distributed Computing (HPDC-12), IEEE Press, to appear June 2003.

[3]SAML기반의 보안 서비스 관리에 관한 연구, 차석일, 김현희, 송준홍, 이형석, 신동일, 신동규, 정보과학회 2002년 춘계학술대회, VOL.29, NO.01, pp.0793~0795, 2002.04

[4] An Online Credential Repository for the Grid: MyProxy. J. Novotny, S. Tuecke, V. Welch. Proceedings of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10), IEEE Press, August 2001.

[5]A Community Authorization Service for Group Collaboration. L. Pearlman, V. Welch, I. Foster, C. Kesselman, S. Tuecke. Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002.

[6]http://www.rsasecurity.com/doc_library/index.asp, Security Assertion Markup Language. A standards Approach to Authorization and Web Single Sign-on document.