그리드 포탈 기반의 인증시스템 모델

황대복°, 허대영, 황선태
국민대학교
{cope3323°, dyheo, sthwang } @cs.kookmin.ac.kr

Grid Portal based Authentication and Authorization System

Daebok Hwang°, Daeyong Heo, Suntae Hwang,
Department of Computer Science, Kookmin University

요 약

그리드[1, 2]는 많은 응용분야에서 보다 효율적인 실험을 위한 컴퓨팅 자원들을 제공한다. 응용연구자들은 지리적으로 분산되어 있는 각 자원들과 서비스를 사용하기에 앞서 사용자 인증과 자원의 사용권한에 대한 인증과정을 거쳐야 한다. 아이디와 패스워드를 사용한 전통적 인증방식은 데이터의 공유와 통합을 전제로 하는 그리드환경에 적용하기에는 평범한 보안수준을 제공한다. 따라서 그리드 환경에 적합한 보안수준을 제공하는 인증방식이 필요하다 또한 기존의 아이디와 패스워드 인증방식에 익숙한 사용자들을 위해 편리한 인터페이스가 요구된다. 이러한 요구사항을 해결하기 위해 본 논문에서는 인증서를 활용한 그리드 포탈 기반의 인증시스템 모델을 제안하고자 한다.

1. 서 론

그리드는 GLOBUS [3] 나 Condor-G[4]와 같은 미들웨어를 통해 지리적으로 분산되어 있는 이기종의 다양한 자원을 통합하고 데이터를 공유할 수 있는 환경을 제공한다. 그리드 환경은 네트워크를 통한 연결을 전제로 하기 때문에 공유되는 자원과 데이터들의 보안이 중요하다. 따라서 사용자들은 이러한 컴퓨팅 자원과 데이터를 사용하는데 있어서 사용자 인증과 자원의 적절한 사용권한에 대한 인증과정이 반드시 필요하다.

이러한 요구사항을 해결하기 위한 인증방식에는 아이디와 패스워드를 이용한 전통적 인증방법과 인증서를 활용한 인증방식이 있다. 아이디와 패스워드 방식은 신원증명 방식이 서비스 제공자와 소비자관계에서 이루어지며, 인증서 방식은 제공자와 소비자 그리고 이를 공인해주는 제 3의 인증기관 사이에 이루어지는 방식이다. 보안 측면에서 아이디, 패스워드 방식에 비해 인증서 방식이 보안수준이 훨씬 높다. 그러나 사용자들은 아이디, 패스워드의 전통적 방식에 익숙해져있다. 따라서 인증서 기반의 보안 시스템을 그리드 환경에 활용하기 위해서는 사용자에 대한 교육이 우선적으로 밑받침 되어야 한다. 인증서 기반의 온라인 뱅킹 시스템과 온라인쇼핑몰에 비교적 익숙한 국내 사용자들을 감안하면 그리드에 인증서 기반의 인증시스템 도입을 위한 여건이 잘 갖추어져 있다고 볼 수 있다.

Globus Toolkit 의 경우 GSI (Grid Security Infrastructure) [5] 인증방식을 채택하고 있다. GSI 는 본인임을 입증하는 인증서를 통해 그리드서비스와 자원의 사용에 필요한 인증과정을 거치도록 한다.

본 논문에서는 GSI 인증 매커니즘을 토대로 인증서를 활용한 그리드 포탈기반의 인증시스템 모델을 제안하고자 한다. 기본적으로 인증서를 인증절차에 사용하기 때문에 아이디, 패스워드 기반의 인증시스템에 비해 보안수준이 향상되고, 그리드포탈 기반으로 구성되어 사용자에게 편리한 인터페이스를 제공할 것으로 기대된다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구를 살펴본다. 3장에서는 전체 시스템구조와 기능에 대해 설명하고, 4장에서는 3장의 구조와 기능에 따른 프로토타입 모델을 제시한다. 끝으로 5장에서는 결론을 맺고 향후 연구 계획을 소개한다.

2. 관련연구

2.1 GSI(Grid Security Infrastructure)

GSI 는 그리드 미들웨어 분야에서 De-facto 표준이라 할 수 있는 Globus Toolkit 에 구현된 보안기능이다. GSI는 공개키 암호화(Public key encryption)[6,7], X-509 인증서[8], Secure Socket Layer[9], Transport

Layer Security[10] 표준을 기반으로 인증서를 사용한 인증(Authentication)과 허가(Authorization)를 가능하게 한다. 인증이란 그리드 서비스를 사용할 때 사용요청을 한 주체가 누구인지 확인하는 과정이다. 그리드 환경에서는 서비스 소비자가 서비스 제공자가 될 수 있기 때문에 서비스 소비자와 제공자간의 신분증명인 상호인증(Mutual Authentication)이 중요하다. 허가란 인증된 사용자에 대해서 그리드 서비스를 이용할 적절한 권한이 있는지 판단하는 과정이다. 이 때 사용자가 누구인지에 따라 차별성을 두기 때문에 인증이 선행되어야 한다.

GSI 가장 중요한 기능은 통합 인증 기능(Single Sign On) 과 권한 위임(Authority Delegation) 이라고 할 수 있다. 사용자들이 그리드 자원을 사용하려면 가장 먼저 사용자 인증을 거쳐야 한다. 이 때 서로 다른 각각의 자원에 대한 사용자 인증과정을 한 번의 인증으로 통합하는 것이 통합인증기능이다. 권한위임이란 사용자의 작업을 처리하는 도중에 그리드 자원이 사용자를 대신해 또 다른 그리드 자원에 대한 인증을 처리하는 기능이다.

GSI 는 다음의 절차로 이러한 요구사항을 충족시킨다.

가. GSI 에서 그리드 사용자는 본인임을 입증하는 사용자 인증서를 소유한다.

나. 이 인증서를 사용해서 그리드 자원에 사용자를 인증하기 위한 프록시 인증서를 생성한다.

다. 프록시 인증서로 사용자 인증이 필요한 각각의 그리드 자원에 새로운 프록시 인증서를 생성한다.

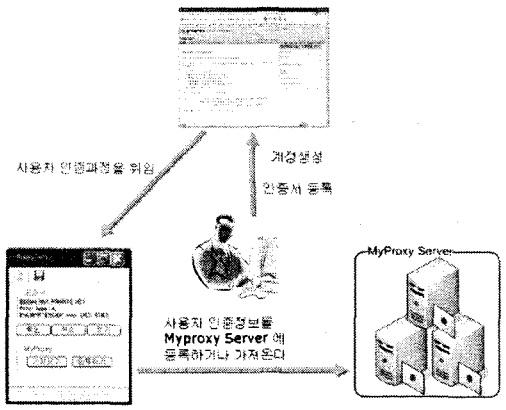
이처럼 GSI 가 그리드 환경의 보안에 필수적인 기능을 제공하지만, 사용자가 그리드 환경에 익숙해야 하고, GSI 관련 명령어들을 숙지해야 하는 어려움이 있다. 따라서 사용자에게 친숙한 인터페이스를 제공하는 인증모델이 요구된다.

2.2 GAMA (Grid Account Management Management Architecture)

GAMA[11]는 SDSC(San Diego SuperComputer Center)에서 개발한 그리드 포탈 기반의 GSI 인증 솔루션이다. GAMA 는 아이디와 패스워드를 사용한 인증방식에 익숙한 사용자들의 편의성을 목표로 하고 있다. 포탈에서 사용자 아이디와 패스워드를 발급하고 내부적으로 사설 인증서를 생성하여 사용자 아이디와 맵핑시켜 관리한다. 따라서 사용자는 그리드 서비스를 이용하기 위한 별도의 인증서를 소유하지 않아도 된다는 편리성이 있다. 그러나 사용자에게 제공한 아이디와 패스워드가 유출될 경우 인증서가 제공하는 보안상의 장점인 제 3자에 의한 신원증명이 무용지물이 될 여지가 있다. 이는 아이디, 패스워드를 사용한 인증방식과 같은 보안 수준이라고 할 수 있다. 본 논문에서 제안하는 인증모델은 사용자가 소유한 인증서를 통한 인증만 허용하기 때문에 GAMA 보다 보안 수준이 높다고 할 수 있다.

3. 전체 시스템 구조 및 기능

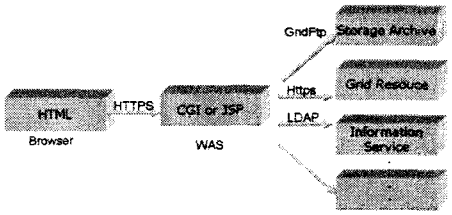
<그림 1> 은 본 논문에서 제한 인증시스템의 전체 구조를 나타낸 것이다. 각 구성 요소를 살펴보면 그리드 미들웨어가 제공하는 서비스와 자원을 사용하기 위한 인터페이스역할을 하는 그리드 포탈과 포탈의 실제 로그인을 담당하는 Proxy Tool, 그리고 사용자 인증정보를 가지고 생성한 프록시를 저장하거나, 사용자에게 제공하는 MyProxy Server 3가지로 나눌 수 있다. 각 구성요소의 세부 기능은 다음 절에서 자세히 설명한다.



< 그림 1 전체 시스템 구조>

3.1. 그리드 포탈 (Grid Portal)

그리드 포탈은 웹 인터페이스를 통해 그리드 서비스를 제공하는 환경으로 그리드 환경에 익숙하지 않은 사용자에게 보다 쉬운 인터페이스를 제공하는 장점이 있다. 포탈의 목적은 사용자에게 편리한 작업환경뿐 아니라 그리드 자원에 대한 단일한 접근환경을 제공하는 것이다. 일반적인 그리드 포탈의 구조는 다음과 같다.



< 그림 2 그리드 포탈의 일반적 구조>

<그림 2> 와 같이 그리드 포탈은 그리드 미들웨어 서비스를 이용하는 전형적인 3계층의 웹 기반 시스템이다. 그리드 미들웨어에서 제공하는 서비스들을 CGI 등의 웹 어플리케이션에서 호출함으로써 그 결과를 사용자에게 웹페이지 형태로 보여준다. 본 논문에서는 포탈을 구축하기 위해 제공되는 다양한 프레임워크 중 그리드 스피어[12]를 사용한다. 그리드 스피어는 포틀릿 기반의 프레임워크로 각 서비스 별로 재사용이 가능하도록 구현되었으며 사용자 관리, 세션 관리, 그룹 관리, 레이아웃 관리 기능 등을 제공함으로써 사용자가 포탈을 통해 그리드 서비스를 쉽게 이용할 수 있도록 한다.

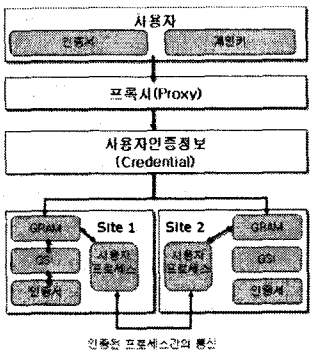
사용자는 포탈에서 계정을 생성하고 Proxy Tool 을 사용해 자신이 소유한 인증서를 등록하는 과정을 거쳐야 한다.

3.2. Proxy Tool

그리드 보안에서 프록시 는 사용자 인증서와 함께 중요한 요소라고 할 수 있다. 인증서를 통해 생성된 Proxy를 사용하여 통합인증이나 권한위임과 같은 기능을 수행하기 때문이다. Proxy는 일반적으로 사용자의 모든 권한을 가지는 풀프록시(full proxy)와 제한된 권한을 가지는 리미티드 프록시(limited proxy)가 있으며 사용자가 그 유효기간을 정할 수 있다.

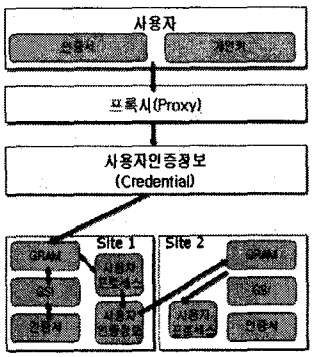
Proxy Tool 은 인증서를 기반으로 그리드 포탈의 실질적인 로그인을 담당하는데, 인증서나 MyProxy Server 에 저장된 프록시로부터 생성한 사용자 인증정보로 포탈에 로그인하게 된다. 따라서 Proxy Tool은 사용자의 인증서로 프록시를 생성해서 MyProxy Server 에 저장하고, 저장된 프록시를 가져오는 등의 프록시 관리 기능을 제공한다. 이것은 사용자의 인증서와 개인키를 사용하고자 하는 자원에 직접적으로 제공하는 대신 인증서보다 제한적이고 한시적인 프록시를 사용한다는 것을 의미한다. 따라서 본 논문에서 제안하는 인증시스템은 그리드환경에서의 보안성을 향상시킬 것으로 예상된다.

<그림 3> 과 <그림 4>는 프록시를 사용한 통합인증, 그리고 권한위임을 나타낸다. <그림 3>에서 보는 것처럼 사용자는 개인키와 인증서를 이용하여 사용자 프록시를 생성하고, 이 프록시를 사용해서 분산되어 있는 그리드 자원을 사용하게 된다. 사용자는 프록시와 원격지의 GRAM 사이에 개입하지 않기 때문에 사용자 프록시를 생성시킬 때에만 비밀번호 입력과 같은 인증과정을 거치게 된다. 두 사이트에서 생성된 프로세스들은 동일한 사용자로부터 실행된 프로세스이기 때문에 상호 인증(Mutual Authentication)된 통신이 가능하다.



< 그림 3 프록시를 사용한 통합인증 과정 >

<그림 4>는 권한 위임과정을 보여준다. 사용자 프록시는 일시적으로 사용자의 권한을 원격 프로세스나 자원에 위임할 수 있다. 사이트 1에서 수행 중인 작업이 다른 그리드 자원을 사용하기 위해 사이트 2에 사용요청을 하는 경우 사이트 1에서 수행 중이던 프로세스는 위임받은 권한으로 사이트2의 그리드 자원을 사용자 개입 없이 사용할 수 있다.



< 그림 4 프록시를 사용한 권한위임 과정 >

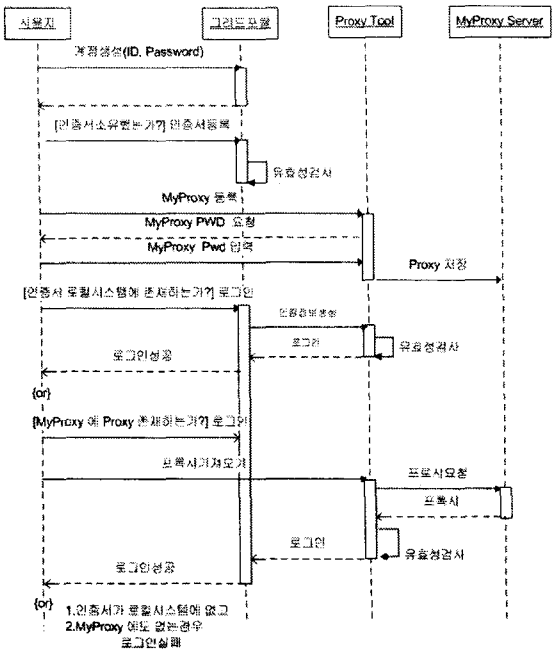
3.3. MyProxy Server

MyProxy Server 는 사용자의 개인키와 인증서를 가지고 Proxy Tool 을 통해 생성한 프록시를 저장하는 역할을 한다. 사용자가 MyProxy Server에 프록시를 등록한 경우 해당 프록시의 정해진 사용기간 내에는 사용자의 인증서를 대신해서 사용할 수 있다. 이는 사용자의 로컬 시스템에 인증서가 반드시 존재해야하는 제약을 없앰으로써 사용자의 편의를 도모한다는 장점이 있다.

4. 프로토타입 설계

인증서를 활용한 포탈기반의 인증시스템을 구축하기

위해 본 논문에서는 사용자들이 쉽게 접근하여 사용할 수 있는 그리드 포탈을 설계하였다. 또한 사용자의 인증 과정을 처리하기 위한 어플리케이션인 Proxy Tool을 포탈에 제공함으로써 그리드 환경에 적합한 인증모델을 제시하였다. 그리드 포탈은 그리드 스피어를 사용하여 구성하였으며, Proxy Tool 은 그리드 포탈과의 연동을 고려하여 자바로 구현하였다. 사용자가 인증서를 소유하고 있다는 전제하에 본 논문에서 제안한 인증시스템의 사용자 인증과정은 다음과 같다.



< 그림 5 사용자 인증 시퀀스 다이어그램>

가. 사용자는 포탈에 계정을 생성하고 인증서 등록한다.

나. 프록시 툴을 사용해 인증서로부터 생성한 프록시를 MyProxy Server 에 저장한다. 이 때 MyProxy 아이디는 포탈의 아이디를 그대로 사용하지만 MyProxy 패스워드는 사용자로부터 새로 입력 받는다

다. 사용자는 인증서가 로컬 시스템에 존재하면 인증서를 통해 로그인할 수 있다.

라. 인증서가 로컬 시스템에 존재하지 않을 경우 Proxy Tool을 사용해서 MyProxy Server 에 저장한 프록시를 가져와 그리드 포탈에 로그인 할 수 있다.

다. 로컬시스템에 인증서가 존재하지 않고, MyProxy Server 에도 저장된 프록시가 없을 경우 로그인은 실패한다.

5. 결론 및 향후 과제

그리드의 보안문제는 분산된 자원들을 네트워크로 연결함에 따라 필연적으로 발생하는 중요한 문제이다. 특히 그 공유 대상이 실험결과와 같은 중요한 데이터들이기 때문에 아이디, 패스워드 방식보다 높은 보안 수준을 필요로 한다. 따라서 보안수준 측면에서 제3자의 공인을 거치는 인증서 기반의 인증방식이 그리드 환경에 적합하다고 할 수 있다. 그러나 인증서기반의 인증방식은 복잡한 사용방법으로 인해 아이디, 패스워드 방식보다 사용자의 편리성이 떨어진다.

본 논문은 인증서를 사용하여 그리드의 보안 수준을 향상시키고자 하였으며 MyProxy의 패스워드를 한번 더 입력하는 과정만으로 아이디 패스워드방식에 준하는 사용자의 편리성을 제공한다. 또한 그리드 포탈을 통해 사용자에게 익숙한 웹 인터페이스 환경을 구성하였다.

향후 과제로써 본 논문에서 제시한 모델을 기반으로 그리드 서비스에 활용할 수 있는 인증시스템을 구축할 것이다.

6. 참고문헌

[1] Grid, Foster, I., et al. A Security Architecture for Computational Grids. in 5th ACM Conference on Computer and Communications Security. 1998.

[2] Grid, The Grid: Blueprint for a New Computing Infrastructure, 2nd Edition, Morgan Kaufmann, 2004. ISBN: 1-55860-933-4.

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

[4] Condor-G, http://http://www.cs.wisc.edu/condor/

[5] GSI, http://www.globus.org/toolkit/docs/security/

[6] PKI, A Survey of Public-Key Infrastructure, Marc Branchaud, Dept. of Computer Science McGill University, Montreal, 1997

[7] PKI, CCITT Recommendation, X.509: The Directory - Authentication Framework. 1988.

[8] X-509 Ceritficate, Housley, R., Polk, W., Ford, W., and Solo, D., Internet X.509 Public Key Infrastructure Certificateand Certificate Revocation List (CRL) Profile. RFC 3280, IETF, April 2002.

[9] SSL, D.Wagner and B. Schneier. Analysis of the SSL 3.0 Protocol. In Proceedings of the Second

USENIX Workshop on Electronic Commerce, November 1996

[10] TLS, Dierks, T. and C. Allen, The TLS Protocol Version 1.0, http://www.ietf.org/rfc/rfc2246.txt

[11] GAMA, Karan Bhatia, Sandeep Chandra, Kurt Mueller, Grid Account Management Architecture 2.0, http://grid-devel.sdsc.edu/

[12] GridSphere, Jason Novotny, Michael Russell, Oliver Wehrens: "GridSphere: a portal framework for building collaborations." Concurrency - Practice and Experience 16(5): 503-513 (2004)