韓國 컴퓨터情報學會 論文誌
第12卷 第3號, 2007. 7.

2007-12-3-1-3

그리드서비스와 포털간의 대칭키 기반 사용자 단일인증에 관한 연구

황 대 복*, 허 대 영**, 황 선 태***

Symmetric key based user authentication between Grid Service and Portal

Daebok Hwang*, Daeyoung Heo**, Suntae Hwang***

요 약

최근 포털 시스템이 그리드환경의 사용자 인터페이스로 많이 이용되고 있다. 전통적인 포털 시스템은 아이디와 패스워드를 사용자 인증방식으로 사용하는 반면 그리드 시스템은 공개키와 개인키로 이루어진 대칭키[1]를 기반으로 사용자 인증을 수행한다. 이와 관련하여 포털 시스템의 사용자 계정과 그리드 시스템의 대칭키를 중심으로 포털과 그리드시스템의 통합에 대한 많은 연구가 진행중이다. 특히 GAMA[2]와 PURSE[3]처럼 아이디, 패스워드 방식에 익숙한 사용자의 편의성에 초점을 둔 연구가 활발하다. 그러나 그리드 환경은 네트워크를 통한 연결을 전제로 하기 때문에 공유되는 데이터와 자원의 보호가 중요하다. 따라서 본 논문에서는 UI 계층에서 대칭키를 사용하여 포털 시스템과 그리드 시스템의 인증 방식을 단일화함으로써 그리드의 사용자 환경[4][5]에서도 보안 수준을 향상시키는 방안을 제안하고자 한다.

Abstract

In recent years, web portal system has received much attention as a user interface for the grid environment. Grid system uses symmetric key for authenticating user identity while the traditional portal system does a password-based authentication. Regarding this, many researches are progressing to integrate portal accounts with symmetric key. Specially, researches such as GAMA and PURSE are active and those focus on easy usability for users who familiar with password-based authentication. However the protection of data and resources is a critical issue in Grid environment, because those are shared through a wide-area network. In this paper, we suggest a new authentication mechanism which unify authentication mechanisms between portal system and grid service by using symmetric key. It will improve a security level in UI layer as much as in grid service.

▸ Keyword : Grid, Security, Authentication, Authorization

• 제1저자 : 황대복 • 교신저자 : 황선태
• 접수일 : 2007.5.31, 심사일 : 2007.6.18, 심사완료일 : 2007. 7.20.
* 국민대학교 일반대학원 전산과학과 석사과정, ** 국민대학교 일반대학원 전산과학과 박사과정
*** 국민대학교 전자정보통신대학 컴퓨터공학부 교수
※ 본 논문은 2007년도 국민대학교 교내 연구비를 지원받아 수행된 연구입니다.

Ⅰ. 서 론

최근 포털 시스템이 그리드 환경의 사용자 인터페이스로 많이 이용되고 있다. 사용자가 그리드 미들웨어의 설치 없이 손쉽게 그리드 환경을 이용할 수 있다는 장점으로 인해 그리드 포털에 관한 연구가 활발하다. 대표적인 예로 그리드스피어[6] 의 GridPortlet[7] 과 OGCE[8] 의 GridPort[9] 프로젝트가 있다.

그리드[10][11]는 지리적으로 분산되어 있는 다양한 실험 장비 및 컴퓨터와 같은 자원을 공유할 수 있는 환경을 제공한다. 그리드는 네트워크를 기반으로 분산된 자원을 공유하기 때문에, 자원의 보안과 자원에 저장되는 데이터의 보호가 중요하다. 따라서 그리드에서는 공개키와 개인키로 이루어진 대칭키를 기반으로 한 보안메커니즘을 사용한다. 그러나 전통적인 포털 시스템은 텍스트 기반의 아이디와 패스워드를 사용자 인증으로 사용한다. 텍스트를 기반으로 하는 포털 시스템의 인증 방식은 네트워크상에서 사용자 신원 인증 정보가 그대로 노출될 수 있는 위험이 있다. 또한 다른 포털 시스템 혹은 그리드 시스템과의 통합 서비스에 보안상의 어려움이 존재한다.

이와 관련하여 포털 시스템의 사용자 계정과 그리드 서비스의 대칭키의 맵핑관계를 중심으로 포털과 그리드 시스템의 통합에 대한 많은 연구가 진행 중이다. 특히 GAMA (Grid Account Management Architecture)와 PURSE (Portal-Based User Registration Service) 처럼 아이디, 패스워드 방식에 익숙한 사용자의 편의성에 초점을 둔 연구가 주목받고 있다. 그러나 그리드 서비스에서 사용하는 대칭키 인증 방식을 포털에 적용하고 그리드 시스템 전체에서 대칭키를 기준으로 한 사용자 인증에 관한 연구는 미비하다.

본 논문에서는 대칭키를 사용하여 포털 시스템과 그리드 시스템의 인증 방식을 단일화함으로써 그리드 환경의 보안 수준을 향상시키고자 한다.

Ⅱ. 설계 기준

그리드 서비스와 포털간의 사용자 단일인증을 설계하는데 있어서 주로 고려한 것은 보안 수준의 향상이다. 이를 위해 그리드 포털의 사용자 인증을 대칭키 기반으로 확장하고, 다음과 같은 설계기준을 적용하였다.

2.1. 보안수준

포털과 그리드 서비스계층은 사용자 인증시 각각 아이디와 대칭키를 사용한다. 포털과 그리드 시스템의 통합에 관한 초기의 연구들은 단순히 포털의 사용자 아이디와 그리드 서비스의 대칭키를 맵핑하여 포털과 그리드 시스템의 사용자 인증을 해결하였다. 이후에 사용자가 대칭키를 그리드 서비스 제공자에게 등록하고 그리드 인증시스템의 중앙에서 관리하는 방식이 도입되었다. 대표적인 예로 GridAuth[12]가 있다. 이러한 방식의 단점으로는 대칭키를 관리하는 중앙 서버에서 문제발생시 모든 사용자가 그리드 서비스를 이용할 수 없다는 것이다. 이러한 단점을 개선하고자 인증시스템에서 내부적으로 사설 대칭키를 생성하고 대칭키와 맵핑된 사용자 아이디를 사용자에게 발급하는 방안이 소개되었다. 대표적인 예로 SDSC (San Diego SuperComputer Center)에서 개발한 그리드 포털 기반의 GSI(Grid Security Infrastructure)[13] 인증 솔루션인 GAMA 가 있다. GAMA는 사용자의 대칭키 생성과 관리를 책임지는 GAMA 서버컴포넌트들을 그리드 포털과 물리적으로 분리하고 SSL(Secure Socket Layer)[14] 프로토콜을 사용하는 서비스 인터페이스를 제공함으로써 아이디, 패스워드의 사용자 인증방식이 가지는 보안상의 단점을 해결하고자 하였다. 이와는 다르게 포털과 그리드서비스 전체에서 사용자 인증방식을 대칭키로 통일함으로써 보안 수준을 향상시킬 수 있다.

2.2. 사용자 인터페이스

전통적인 그리드 환경에서 사용자는 그리드 미들웨어를 설치하고, UNIX 쉘 커맨드 형태의 명령어를 통해서 그리드 서비스를 이용해야 했다. 그리드 환경을 이용하는 일반 사용자들이 특정 응용분야의 연구자들이라는 점을 감안하면 사용자에게 보다 친숙한 인터페이스를 제공해야 한다. 그리드 포털은 그리드 미들웨어의 설치 없이 사용자가 그리드 환경을 손쉽게 이용할 수 있다는 점에서 그리드의 사용자 인터페이스로 적절하다. 또한 웹브라우저를 통해 시간, 공간의 제약없이 접근이 가능하며, 개인화 설정이 용이하다는 장점이 있다.

2.3. 인증방법

그리드는 네트워크 연결을 전제로 유휴자원을 공유한다. 따라서 사용자들이 컴퓨팅 자원과 데이터를 사용하는데 있어서 신뢰할 만한 수준의 보안 메커니즘이 필요하다. 그리

드 환경에서 대칭키 기반의 인증방식은 사용자들이 그리드 환경에 익숙해야 하고, GSI 관련 인터페이스를 사용하기 위한 사전 교육이 선행되어야 하는 어려움이 있다. 따라서 사용자 관점에서 대칭키 기반의 인증방식은 편리성이 부족하다고 할 수 있다. 그러나 대칭키 기반의 온라인 뱅킹 시스템과 온라인쇼핑몰에 익숙한 국내 사용자들을 감안하면, 그리드 환경에 대칭키 인증 도입을 위한 여건이 비교적 잘 갖추어져 있다고 볼 수 있다.

시스템보안 관점에서 사용자와 서비스 제공자 그리고 이를 공인해주는 제3의 인증기관 사이에서 인증과정이 이루어지는 대칭키 인증방식이 텍스트 기반의 아이디, 패스워드방식보다 보안 수준이 높다. 따라서 그리드 포털에 아이디, 패스워드를 사용한 인증방식 대신 대칭키 기반의 인증방식을 적용함으로써 보안 수준의 향상을 기대할 수 있다.

2.4. 대칭키의 발급과 관리

아이디, 패스워드방식과 달리 대칭키 기반의 인증은 인증기관에 대칭키를 신청하고 발급받는 과정이 필요하다. 대칭키의 발급과는 별도로 대칭키의 관리 기능을 제공해야 한다. 대칭키의 분실이나 유효기간의 만료시 해당 대칭키에 대해 취소신청이나 기간의 연장과 같은 적절한 추가 조치가 이루어져야 한다. GAMA, PURSE 와 같은 기존연구에서는 사용자의 편의를 위해 대칭키 발급과 관리를 그리드 시스템에서 담당하였다. 또한 사용자에게 대칭키를 사용한 인증은 배제하고 아이디, 패스워드를 통한 접근만 가능하게 하였다.

2.5. Client 어플리케이션 지원

그리드의 사용자 인터페이스로 포털외에 자바웹스타트나 애플릿 같은 웹 서비스 기반의 응용프로그램이 대두되고 있다. 이러한 추세에 따라 독립어플리케이션 형태의 클라이언트 지원은 기존 그리드 시스템과의 통합과 시스템의 유연성 향상을 위해 필요한 기능이다. 특히 그리드 리소스 모니터링이나 원격실험과 같은 분야에서는 웹브라우저보다 플러그인 형태의 어플리케이션 개발이 생산성 측면에서 유리하다고 할 수 있다.

2.6. 배포

그리드서비스를 제공하는 입장에서 운영중인 시스템에 대칭키 인증방식을 적용하기 위해 추가적인 개발부담이 최소화되어야 할 것이다. 기존 연구에서는 특정분야의 문제해결을 위해 최적화된 패키지형태로 배포되는 경우가 많다. 따라서 기존 그리드 시스템과의 통합에 어려움이 예상된다. 이러한 문제점을 해결하기 위해서 포틀릿 이나 WAR(Web Archive) 형태의 배포방식이 요구된다. 특히 포틀릿형태의 배포는 JSR168 표준을 준수하는 포틀릿 컨테이너를 사용하는 포털이라면 플랫폼 독립적이기 때문에 기존 시스템과 통합에 유리하다는 장점이 있다.

2.7. 위임

사용자들이 그리드 자원을 사용하려면 가장 먼저 사용자 인증을 거쳐야 한다. 권한위임이란 사용자의 인증후사용자의 작업을 처리하는 도중에 그리드 자원이 사용자를 대신해 또 다른 그리드 자원에 대한 인증을 처리하는 기능이다. 이를 위해 GSI 에서는 사용자의 대칭키로부터 프록시를 생성하고 이 프록시를 사용하여 사용자 대신 그리드 서비스를 요청한다. 프록시는 일반적으로 사용자의 모든 권한을 가지는 Full Proxy와 제한된 권한을 가지는 Limited Proxy가 있으며 사용자가 그 유효기간을 정할 수 있다. 위임에서는 생성된 프록시의 정해진 사용기간 내에서만 그리드 서비스를 사용할 수 있기 때문에 그리드 서비스 호출시에 사용자 대칭키를 사용하는 것보다 보안상의 이점이 있다.

2.8. 통합인증(SSO-Single Sign On)

통합인증은 사용자가 처음 한번만 인증을 받고나면 추가적인 인증과정 없이 허가된 권한 내에서 분산된 자원과 서비스들을 이용할 수 있게 하는 것이다. 초기의 통합인증은 인증과정의 단순화가 목적이었다. 기존의 통합인증의 경우, 실제 사용자 아이디와 패스워드는 남겨둔 채로, 사용자 관점의 로그인 과정을 자동화하는 것이었고, 운영자 관점에서는 계정관리 작업을 자동화하는 것에 지나지 않았다. 이러한 초기의 통합인증은 사용자의 편의성을 향상시킨다는 점에서 이점이 있지만, 보안 관점에서는 진보된 해결방안이라고는 볼 수 없다. 즉, 네트워크상에서 아이디, 패스워드가 텍스트로 전달된다는 점에서 기존의 방식과 차이가 없다. 따라서 그리드에서 통합인증은 사용자 인증의 단순화와 암호화가 모두 가능한 대칭키를 사용해야 할 것이다.

2.9. 계정관리(Account Management)

하나의 가상조직에는 사이트 별로 각각의 그리드 서비스를 제공하는 여러 그리드 포털이 존재한다. 따라서 가상조직 전체에서 사용자의 유일성을 보장하기 위한 방안이 필요하다. 예를 들어 사용자 '갑'이 포털 A와 포털 B 모두에서 동일한 사용자로 인식되어야 할 것이다. 이를 해결하기 위해 이메일주소를 각 포털의 사용자 아이디로 사용하거나 각

각의 포털이 아닌 중앙에서 사용자 계정관리를 담당하기도 한다. 또한 각 사이트의 독립적인 사용자 정책을 지원하기 위해서 포털마다 동적인 사용자 계정 생성이 가능해야 한다.

III. 기능과 구현

본 논문에서는 앞에서 언급한 원칙들을 기준으로 대칭키를 사용하여 그리드 서비스와 포털간의 인증을 단일화하는 방법을 제시하고자 한다. 아래와 같은 세부 설계 기준을 바탕으로 제안한 방안의 프로토타입을 구현하고 KOCED[15] 에 적용하였다. 이러한 설계 기준은 KOCED 프로젝트에 적용하면서 정리한 요구사항들이다. KOCED는 분산 공유형 건설연구인프라 구축사업으로 각 센터별로 사용자 계정과 권한이 서로 독립적인 가상 조직이다. 각 센터에는 원격실험과 데이터공유를 위한 그리드 서비스와 그리드 서비스를 제공하기 위한 인터페이스를 담당하는 여러 그리드 포털이 존재한다.

1) 대칭키의 관리를 그리드 시스템이 아닌 사용자에게 위임하였다.
2) 사용자의 개인키로 시그니처를 생성하고 이 시그니처를 사용하여 포털에 로그인한다.
3) 포털간의 통합인증시 사용자가 로그인에 사용한 시그니처를 이동 대상이 되는 포털에 전달한다.
4) 사용자 대칭키로 포털계정을 동적으로 생성하고, 대칭키를 사용한 로그인만 가능하게 함으로써 보안 수준을 향상시킨다.
5) 독립 어플리케이션에서 그리드 서비스 이용이 가능하도록 대칭키로 로그인 가능한 API를 제공해야 한다.

〈그림 1〉 은 본 논문에서 제안하는 방안에서 사용자가 그리드 서비스를 이용하는 전체 구조를 나타낸 것으로 사용자는 그리드 포털과 자바 웹스타트와 같은 어플리케이션을 통해 그리드 서비스를 이용할 수 있다.

사용자는 로컬 컴퓨터에 존재하는 대칭키를 이용하여 사용자 인증과정을 거치게 된다. 각 구성 요소를 살펴보면 그리드 미들웨어가 제공하는 서비스와 자원을 사용하기 위한 인터페이스역할을 하는 그리드 포털과 포털의 실제 로그인과 포털 사이의 통합인증을 담당하는 로그인 도구, 그리고 그리드 서비스를 이용할 때 필요한 프록시를 사용자에게 제공하는 위임 서비스 3가지로 나눌 수 있다. 각 구성요소의 세부 기능과 구현은 다음 절에서 자세히 설명한다.

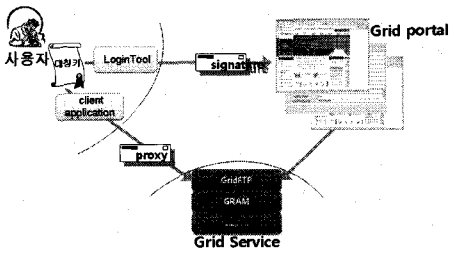

그림 1. 그리드서비스와 포털의 단일인증 방안
Fig 1. Unified authentication between Gridservice and Portal

3.1 그리드 포털

그리드 포털의 목적은 웹 인터페이스를 통해 사용자에게 그리드 서비스를 제공하는 것이다. 이는 사용자가 그리드 서비스를 이용하기 위해 그리드 미들웨어나 특정 어플리케이션을 로컬 컴퓨터에 설치하지 않아도 된다는 장점이 있다. 이처럼 그리드 포털은 사용자에게 편리한 작업환경뿐만 아니라 그리드 자원에 대한 단일한 접근 환경을 제공한다. 따라서 그리드 포털은 사용자의 관점에서 최종적인 사용자 인터페이스를 담당하는 구성요소라고 할 수 있다. 본 논문에서는 포털을 구축하기 위해 제공되는 다양한 프레임워크 중 그리드스피어를 사용한다. 그리드스피어는 포틀릿 기반의 프레임워크로 각 서비스 별로 재사용이 가능하도록 구현되었으며 사용자 관리, 세션 관리, 그룹 관리, 레이아웃 관리 기능 등을 제공함으로써 사용자가 포털을 통해 그리드 서비스를 쉽게 이용할 수 있도록 한다.

3.2 로그인 도구

로그인 도구는 사용자 대칭키를 기반으로 그리드 포털의 실질적인 로그인을 담당한다. 로그인 도구를 통해 사용자 대칭키로 그리드 포털에 동적으로 사용자 계정을 생성한다. 로그인 도구는 대칭키를 통해 생성된 시그니처를 사용하여 포털과 그리드 서비스에서의 인증을 수행하기 때문에 시그니처는 사용자 대칭키와 함께 인증에 있어서 중요한 요소라고 할 수 있다. 시그니처는 〈개인키로 사인한 message, checksum〉 형태로 생성되며 사용자의 전자서명이라고 할 수 있다. 사용자가 로그인 도구를 사용하여 로그인할 때 사용자의 시그니처를 포털에 보낸다. 이 때 SSL 프로토콜을 사용하여 시그니처의 안전을 보장한다. 로그인 도구는 위임 서비스에 사용자의 프록시 생성을 요청하고, 생성된 프록시로 그리드 서비스들을 사용한다. 사용자 대칭키로 그리드 포털에 로그인하는 상세한 절차(그림 2) 는 다음과 같다.

1) 로그인 도구는 그리드 포털에 사용자 대칭키로부터 생성한 Message 를 보낸다.

2) 로그인 도구는 message 에 MD5 해쉬 함수를 적용하여 Message Digest 를 생성한다.
3) 로그인 도구는 사용자의 개인키로 시그니처를 암호화하여 그리드 포털에 보낸다.
4) 그리드 포털은 사용자의 공개키로 2)에서 생성한 시그니처를 복호화한다.
5) 1)과 2)에서 각각 얻은 두개의 Message Digest 를 비교한다.
6) 두개의 Message Digest 가 같으면 로그인 성공하고 다르면 로그인 실패한다.

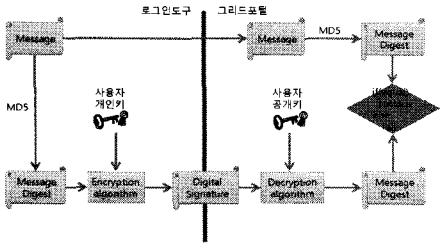

그림 2. 로그인 절차
Fig 2. Login Procedure

본 논문에서 제안한 방안에서 사용자는 대칭키를 통해서만 로그인이 가능하다. 이로 인해 사용자인터페이스인 그리드 포털 계층에서 보안 수준의 향상을 기대할 수 있다.

로그인 도구(그림3)는 자바를 사용하여 구현하였으며, 포털간의 통합인증을 위하여 그리드 포털에 애플릿의 형태로 적용시켰다. KOCED에서 제공하는 그리드 환경은 서비스기반으로 제공되기 때문에 포털이 아닌 자바 웹스타트와 같은 클라이언트 어플리케이션으로 접근하여 사용할 수 있다. 따라서 로그인 도구를 자바 라이브러리로 제공하여 클라이언트 어플리케이션에서 사용자 대칭키로 그리드 서비스를 사용할 수 있게 하였다.

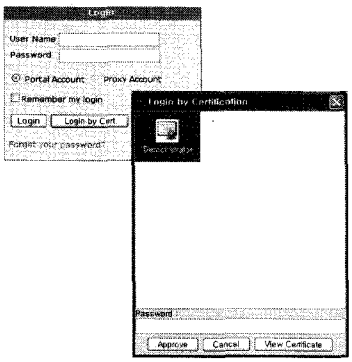

그림 3. 로그인 도구
Fig 3. Login Tool

3.3 위임

본 논문에서는 대칭키 관리를 사용자에게 위임하였다. 따라서 대칭키로 그리드 포털에 로그인한 사용자들이 그리드 서비스를 이용하고자 할 때 사용자 대신 그리드 서비스의 사용 요청을 수행하는 서비스가 필요하다. 다른 그리드 서비스들과의 호환을 고려하여 GSI 기반으로 구현하였다. GSI 의 자세한 위임절차는 다음과 같다. 〈그림 4〉 는 사용자가 그리드 포털에 로그인한 후에 GSI 위임 절차에 따라 그리드 서비스를 이용하는 과정을 시퀀스다이어그램으로 나타낸 것이다.

1) 로그인한 사용자는 포털에 그리드서비스를 요청한다.
2) 포털은 위임 서비스에 프록시 생성을 요청한다.
3) 위임서비스는 사용자가 로그인할 때 사용한 시그니처의 유효성을 체크한다.
4) 유효한 시그니처라면 위임서비스는 사용자를 대신하여 그리드 서비스를 요청한다.

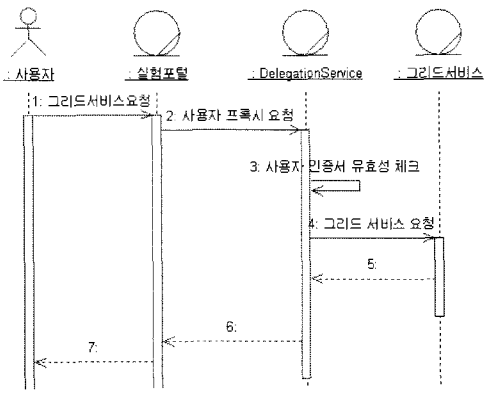

그림 4. 그리드 서비스 이용과정
Fig 4. A process for using grid serivce

IV. 평가

포털 시스템의 사용자 계정과 그리드 서비스의 대칭키로 그리드 시스템의 사용자 인증을 통합하려는 많은 연구가 진행 중이다. 대표적인 예로 GAMA, GridAuth, PURSE, DOE 등이 있다. 본 논문에서 제시한 방안과 관련연구들을 2장에서 기술한 설계원칙 에 따라 그 특징들을 비교하였다. GAMA, GridAuth, PURSE, DOE[16] 모두 아이디와 패스워드를 사용한 인증방식에 익숙한 사용자들의 편의성을

목표로 하고 있다. 사용자 인터페이스를 포털로 제공한다는 점에서 본 논문에서 제시한 방안과 유사하지만 사용자에게 포털의 아이디와 패스워드를 제공한다는 점에서 큰 차이가 있다. 사용자에게 제공한 아이디와 패스워드가 유출될 경우 대칭키가 제공하는 보안상의 장점인 제 3자에 의한 신원증명이 무용지물이 될 여지가 있다. 이는 아이디, 패스워드를 사용한 텍스트 기반의 인증방식과 같은 보안 수준이라고 할 수 있다.

포털에서 사용자 아이디와 패스워드를 발급하고 내부적으로 사설 대칭키를 생성하여 사용자 아이디와 맵핑시켜 관리한다는 점에서 GAMA, GridAuth, PURSE 는 유사하다. 이러한 메커니즘은 사용자가 그리드 서비스를 이용하기 위한 별도의 대칭키를 소유하지 않아도 되는 편리성이 있다. GridAuth 사용자는 서버컴포넌트의 웹인터페이스를 통해 계정을 요청하고 관리자도 서버 컴포넌트의 웹인터페이스를 통해 계정을 관리한다. PURSE 사용자도 이와 비슷하게 사용자 등록 웹페이지에서 사용자의 기본정보를 입력하고 발급되는 아이디와 패스워드를 통해 그리드 서비스를 이용한다.

PURSE에서 대칭키의 발급과 관리는 PURSE 시스템에서 담당한다. 사용자 대칭키의 관리를 사용자가 아닌 시스템에서 한다는 점에서 PURSE는 GAMA 와 유사하다. 그러나 GAMA 가 사용자에게 시스템 내부적으로 대칭키를 생성하는 반면 PURSE 는 사용자가 기존에 소유하고 있는 대칭키를 PURSE 시스템에 등록할 수 있는 인터페이스를 제공한다. 또한 PURSE 는 MyProxy[17] 와 SimpleCA 그리고 PURSE 포털이 하나의 시스템으로 동작하는 데 비해 GAMA는 서버구성요소들인 CACL, MyProxy, CAS(Community Authorization Service)[18] 가 그리드 포틀릿으로 제공되는 사용자 인터페이스와 분리되어 웹서비스 형태로 제공된다.

GridAuth, PURSE, DOE 가 MyProxy 의 사용자 아이디와 패스워드로 통합인증을 지원하는데 반해 GAMA 는 포털의 사용자 계정을 기준으로 통합인증을 지원한다. 따라서 GAMA 는 서로 독립적인 사용자 계정을 기반으로 운영되는 포털들의 계정통합에는 어려움이 따른다.

GAMA 가 그리드스피어의 포틀릿형태로 구현되어 배포가 용이한 반면 GridAuth 는 플러그인 아키텍처를 기반으로 서버와 클라이언트 컴포넌트로 구성되어 있다. 또한 개발환경을 그리드 스피어로 통합한 GAMA 와 달리 클라이언트 컴포넌트의 구현을 규정짓지 않았다. 따라서 GridAuth 를 활용하기 위해서 클라이언트 컴포넌트의 추가 구현이 필요하다. PURSE 는 JAVA API를 사용하여 구현되었으며, AXIS 컨테이너를 통해 포털에서 호출된다.

DOE(Department Of Energy)는 사용자 인증시스템으로 ROAM(Resource Oritented Authorization Manager)[19] 시스템을 제공한다. ROAM 은 FusionGrid 에서 제공하는 그리드 서비스와 사용자에 관한 정보들을 관리하는 back-end 계층과 사용자 인터페이스를 담당하는 웹인터페이스형태의 front-end 계층으로 구성되어 있다. 사용자는 MyProxy 클라이언트 툴을 사용해서 ROAM 에 대칭키를 등록하고 ROAM 으로부터 사용자의 인증을 받는다. 따라서 ROAM 을 사용하기 위해서 사용자들은 MyProxy 에 대한 교육이 우선적으로 필요하다.

다음은 앞에서 언급한 관련연구들의 특징을 테이블형태로 정리한 것이다. 본 논문에서 제시한 방안과 GAMA, GridAuth, PURSE, DOE 모두 포털 형태로 사용자 인터페이스를 제공한다. 그러나 본 논문에서는 대칭키의 관리를 시스템이 아닌 사용자에게 위임하는데 반해 관련연구들은 대칭키의 관리를 시스템에서 담당한다. 이는 사용자에게 포털 또는 MyProxy 아이디를 발급하고 사용자에게 발급한 아이디로 사용자인증을 한다는 점에서 큰 차이가 있다. 또한 본 논문이 제시한 방안은 JAVA 웹스타트와 같은 클라이언트 프로그램을 지원함으로써 기존시스템과의 통합에 유연성을 제공한다는 점이 특징이라고 할 수 있다. 뿐만 아니라 그리드스피어의 모듈형태로 배포하기 때문에 기존시스템에 적용이 용이하다는 장점이 있다.

표 1. 관련연구의 특징비교
Table 1. a comparison of related works

대상 / 기준	제안 방안	GAMA	GridAuth	PURSE	Doe
사용자 인터페이스	포털	포털	포털	포털	포털
인증방법	대칭키	아이디, 패스워드	아이디, 패스워드	아이디, 패스워드	아이디, 패스워드
대칭키의 관리	사용자	GAMA Portlet	Centeral Server	PURSE System	ROAM
Client 지원	O	O	X	X	X
배포	그리드스피어모듈	그리드스피어모듈	source (tgz)	source (war)	package
위임	O	O	O	O	O
통합인증	시그니처	myproxy	myproxy	myproxy	X
계정관리	그리드 스피어	그리드 스피어	Centeral Server	PURSE System	ROAM
authorization	-	role based	policy based	policy based	resource based

V. 결론

그리드의 보안문제는 분산된 자원들을 네트워크로 연결함에 따라 필연적으로 발생하는 중요한 문제이다. 특히 그 공유 대상이 실험결과와 같은 중요한 데이터들이기 때문에 높은 보안 수준을 필요로 한다. 따라서 보안수준 측면에서 제3자의 공인을 거치는 대칭키 기반의 인증방식이 그리드 환경에 적합하다고 할 수 있다.

본 논문에서는 최근 그리드 환경의 사용자인터페이스로 대두되고 있는 그리드 포털과 그리드 서비스 계층의 인증을 대칭키로 단일화하는 방법을 제시하였다. 이를 통해 그리드 포털과 그리드 시스템의 보안 수준의 향상을 기대할 수 있다.

향후 과제로써 하나의 포털이 아닌 여러 그리드 포털에서 SSO 를 지원하기 위해 구현을 웹서비스화 하고, 서비스 계층에서 사용자의 인증서로 authorization 이 가능하도록 CAS 와의 연동을 추가적으로 구현할 예정이다.

참고문헌

1) M. Thompson, A. Essiari, S.Mudumbai, "Certificate-based Authorization Policy in a PKI Environment", in ACM Transactions on Information and System Security (TISSEC), Vol. 6, No. 4, pp. 566-588, 2003.

2) Karan Bhatia, Kurt Mueller, Sandeep Chandra, "GAMA: Grid Account Management Architecture", IEEE International Conference on EScience and Grid Computing, Dec 2005

3) GridCenter, N., "A Portal-based User Registration Service for Grids", April, 2005, http://www.gridscenter.org/solutions/purse/

4) 심규호, 황선태 "계산 그리드에서 워크플로우기반의 사용자 환경 설계 및 구현" 한국컴퓨터정보학회, 한국컴퓨터정보학회논문지 제10권 제4호, 2005. 9, pp. 165 ~ 171

5) 박다혜, 이종식 "계산 그리드 컴퓨팅에서의 자원 성능 측정을 통한 그리드 스케줄링 모델" 한국컴퓨터정보학회, 한국컴퓨터정보학회논문지 제11권 제5호, 2006. 9, pp. 87 ~ 94

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

7) M. Russell. GridPortlets overview. February 2005. http://www.gridsphere.org/gridsphere/html /mardigrasworkshop2005/02 gridportlets.pdf

8) OpenGrid Computing Environments Collaboratory. http://www.ogce.org/, cited in May 2005.

9) Thomas, M., et al. "The Gridport Toolkit: a System forBuilding Grid Portals", in 10th IEEE International Symp. on High Perf. Comp. 2001.

10) Foster, I., et al. A Security Architecture for Computational Grids. in 5th ACM Conference on Computer and Communications Security. 1998.

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

12) Timothy Warnock, Wei Deng, Lawrence Miller, Adam Lathers, The GridAuth Credential Management System

13) Foster, I., C. Kesselman, G. Tsudik, and S. Tuecke, "A Security Architecture for Computational Grids", ACM Conference on Computers and Security. 1998. p. 83-91.

14) D.Wagner and B. Schneier. Analysis of the SSL 3.0 Protocol. In Proceedings of the Second USENIX Workshop on Electronic Commerce, November 1996

15) 신수봉, 강수용, 김철영, 염헌영, 김재관 "KOCED: 건설분야의 그리드 기술 활용" 한국정보과학회, 정보과학회지 제24권 제5호, 2006. 5, pp. 46 ~ 52

16) Burruss, J.R., Fredian, T.W., Thompson, M.R., "Simplifying FusionGrid Security", Challenges of Large Applications in Distributed Environments (CLADE) workshop at HPDC14, July 2005

17) Novotny J, Tuecke S, Welch V. An online credential repository for the grid: MyProxy. Proceedings of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10). IEEE Press: San Francisco, August 2001.

18) Pearlman, L., et al. "A Community Authorization Service for Group Collaboration", in IEEE 3rd International Workshop on Policies for Distributed Systems and Networks. 2002.

19) K. Czajkowski, et al., "A Resource Management Architecture for Metacomputing Systems", in Proc. 4th Workshop on Job Scheduling Strategies for Parallel Processing in Conjunction with IPPS/SPDP '98, Orlando, Florida, March 30, 1998, p. 62.

저자소개

황대복
2005년 국민대학교 컴퓨터학부(학사)
2006년 ~ 국민대학교 전산과학 석사과정
관심분야 : 그리드 시스템, 디자인패턴, 임베디드, 시스템아키텍처
email : cope3323@cs.kookmin.ac.kr

허대영
2004년 국민대학교 컴퓨터학부(학사)
2005년 국민대학교 전산과학(석사)
2006년 ~ 국민대학교 전산과학 박사과정
관심분야 : e-Science, 그리드 시스템, PSE, 디자인패턴, 공개소프트웨어
email : dyheo@cs.kookmin.ac.kr

황선태
1985년 서울대학교 컴퓨터공학과(학사)
1987년 서울대학교 컴퓨터공학과(석사)
1996년 Manchester University(PhD)
1997 ~ 국민대학교 전자정보통신대학 컴퓨터공학부 부교수
관심분야 : e-Science, 그리드 시스템, PSE, 공개소프트웨어
email : sthwang@kookmin.ac.kr