제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

GRID 보안 인프라 구축 연구

길원석, 서선영, 이봉환
대전대학교 정보통신공학과
e-mail: wsgil@ice.dju.ac.kr

Implementation of a GRID Security Infrastructure

Won-Suk Gil, Sun-Young Seo, and Bong-Hwan Lee
Dept of Information & Communications Eng., Daejeon Univ.

요 약

분산 컴퓨팅 환경에서 네트워크의 자원을 공동으로 이용하기 위한 가상조직의 구축이 활발히 이루어지고 있다. 본 연구에서는 Globus 툴킷을 이용하여 리눅스 네트워크 상에 그리드 보안 인프라(GSI) 환경을 구축하였다. GSI는 CA 서버, 호스트, 프락시 및 gatekeeper 등으로 구성된다. 구현한 GSI 구성 요소들을 이용하여 single sign-on, delegation 등 그리드 보안의 주요 기능을 확인하였다. 또한, GSI를 안전하고 확장 가능한 방법으로 엑세스할 수 있도록 설계되고 개발된 그리드 보안 서비스인 MyProxy와 Grid-FTP를 구현하여 그리드 보안의 효용성을 검증하였다.

1. 서 론

그리드(GRID)란 용어는 1990년대 중반 보다 진보된 형태의 과학 기술을 위한 분산컴퓨팅 인프라를 설계하는 과정에서 등장하였다[4]. 과학 기술 및 산업계에 종사하고 있는 개인 및 조직들은 자원을 공동으로 이용하여 함께 목표를 추구하는 가상조직(Virtual Organization)을 구축해나가고 있다. 예를 들면 NSF의 PACI (Partnerships for Advanced Computational Infrastructure) 프로그램은 컴퓨팅 사이언스에 대한 차세대 인프라를 제공하고 있다. 5년에서 10년 동안 지원을 받은 대형 조직인 PACI들은 약 50개 기관에 종사하는 수 천명의 과학자들을 연결하고 있다[1]. 가상조직의 참여자들은 데이터 아카이브, 컴퓨터 사이클, 네트워크 등 요청된 자원의 특성과 사용자의 신원에 의한 제한적으로 액세스 가능한 자원들을 공유한다. 따라서 공유 메카니즘은 사용자의 신원을 인증하기 위한 능력을 가지고 있어야 하며, 이 사용자가 해당 자원을 엑세스하기 위한 권한이 있는지를 검증하여야 한다. 가상조직들은 유동적이기 때문에 인증 메카니즘도 유동적이고 경량이어야 관리자들이 신속하게 자원 공유 메카니즘을 설정하고 수정할 수 있다. 그럼에도 불구하고 가상조직들은 기존의 조직들을 대체하는 것이 아니라 보완하는 것이기 때문에 공유 메카니즘은 로칼 정책을 변경할 수 없으며, 각 조직들이 자신들의 자원을 통제할 수 있도록 해주어야 한다.

그리드 연구 그룹에서는 이러한 요구사항을 만족하는 GSI(Grid Security Infrastructure)라는 인증 및 권한검증 인프라를 개발하여 사용하고 있다. GSI는 안전한 single sign-on을 제공하며, 액세스 정책과 로컬 보안에 대하여 사이트 제어를 유지한다. GSI는 FTP, 원격 로그인 및 안전한 응용을 개발하기 위한 프로그래밍 인터페이스 등의 기존의 응용을 수행시키기 위한 GSI 버전의 응용 및 인터페이스를 제공한다. 현재 많은 수퍼 컴퓨터와 저장 시스템들에서 GSI가 사용되고 있다. 본 논문에서는 현재 제공되고 있는 Globus 툴킷을 리눅스 네트워크 시스템에 구현하여 GSI 보안 능력 및 서비스 기능을 검증한다. 본 논문의 2절에서는 그리드 보안 요구사항과 프로토콜에 대해 소개하고, 3절은 Globus 툴킷을 이용한 GSI 구축에 대하여 소개하며, 4장에서는 그리드 보안 서비스인 GridFTP와 Myproxy의 구현에 대해 소개한다. 마지막 5절에서는 본 논문의 결론을 맺는다.

본 연구는 KOSEF 지원
(과제번호 R05-2002-01008)으로 수행되었음.

2. 그리드 보안 프로토콜

2.1. 그리드 보안의 요구사항[5]

그리드 보안의 요구사항은 그리드 인증, 통신 및 권한검증에 관한 요구사항으로 분류된다.

■ 인증관련 요구사항

● Single Sign-on

사용자는 단 한번의 로그인을 통하여 그리드 상에 있는 사용 허가된 모든 자원을 액세스할 수 있어야 한다.

● Delegation

사용자를 대신하여 수행하는 프로그램이 사용자가 사용할 수 있도록 허가된 자원들을 아무런 제약 없이 자유롭게 사용할 수 있도록 사용자의 권한을 해당 프로그램에게 전달할 수 있는 기능이 포함되어야 한다. 또한, 이러한 권한을 전달받은 프로그램은 조건적으로 그 권한의 일부분 또는 전체를 다른 프로그램에게 전달할 수 있어야 한다.

● 로컬 보안 솔루션과 상호 운용성

각 사이트는 Kerberos 및 UNIX 보안 방식 등 다양한 형태의 보안 관련 정책을 운용할 수 있으므로 그리드 보안 솔루션은 각각의 지역 보안 솔수션과 상호 운용성이 제공되어야 한다.

■ 통신관련 요구사항

● 융통성 있는 메시지 보호

어플리케이션들은 무결성 또는 무결성과 기밀성 등을 포함하여 다양한 레벨의 메시지 보호를 사용하기 위하여 동적으로 서비스 프로토콜을 구성할 수 있어야 한다.

● 신뢰성 있는 통신 프로토콜 지원

현재 인터넷 프로토콜인 TCP가 널리 사용되고 있지만 보안 메카니즘은 다른 신뢰성 있는 통신 프로토콜도 지원해야 한다.

2.2 그리드 보안 인프라(GSI) 프로토콜

가장 널리 사용되고 있는 두 인증 메카니즘인 Kerberos와 secure shell은 그리드 보안 요구사항을 만족시키지 못한다. 따라서 GSI 프로토콜이 개발되었다.

GSI는 사이트 간의 보안을 위한 대안이며, 분산 컴퓨팅 환경 또는 가상조직과 유사한 계산 그리드(Computational Grid)를 구축하기 위하여 Globus 프로젝트의 일환으로 개발되었다. GSI는 사이트들의 서로 다른 로컬 보안 솔루션들을 연계함으로서 도메인간의 작업과정을 처리한다.

• 비밀키로서 표준 X.509v3 인증서를 사용하는 증명서는 사용자, 자원, 프로그램 등 각 엔터티의 신원을 나타내며, 공개키와 같은 엔터티의 이름과 추가 정보를 명시한다. 제3의 신뢰기관인 인증기관(CA)은 인증서에 서명함으로서 신원을 공개키/비밀키 쌍과 바인딩 한다.

• SSLv3(Secure Socket Layer Version 3)에 의해 정의되는 인증 알고리즘은 엔터티의 신원을 확인한다. 엔터티 신원에 대한 신뢰성은 인증서를 발행하는 CA가 제공하는 신뢰성에 의해 좌우된다.

• 엔터티는 프록시라 불리는 일시적인 신원을 생성하여 자신의 권한의 일부를 제 3자에게 위임할 수 있다. 프록시 인증서는 체인을 형성할 수가 있는데 CA로부터 시작하여 먼저 사용자 그리고 사용자 프록시 순이다.

• 각 자원은 입력되는 요청을 수락할지 않을지를 결정하기 위하여 자신의 정책을 정할 수 있다.

• 인증 프로토콜은 구성원들의 글로벌 신원을 검증하지만 GSI는 로컬 보안 시스템이 이 이름을 사용하기 전에 이 이름을 로그인 네임과 같은 로컬 이름으로 변환해야 한다. GSI는 글로벌 이름과 로컬 이름 사이에 바인딩을 정의하는 로컬 사이트 제어에 따라 간단한 텍스트 형태의 맵파일을 이용하여 이 과정을 수행한다.

• 표준 인터페이스인 GSS-API는 보안 작업과정에 대한 엑세스를 제공한다. GSI는 인증 프로토콜로 OpenSSL이나 SSLeay를 사용하며 프록시 인증을 제공한다.

• 프록시 증명서와 위임은 자원을 엑세스하기 위하여 사용자를 대신하는 프로그램이 수행되는 것을 허용한다. X.509, SSLv3 및 GSS-API 표준을 사용하면 GSI가 가능한 툴 및 보다 복잡한 응용을 개발할 수 있다.

3. Globus 툴킷

3.1 Globus 툴킷 설치

리눅스 환경에서 Globus 툴킷 2.0을 설치하였다. Globus 툴킷은 다음의 세 가지 요소로 구성되어 있다.

• Resource Management 요소

Resource Management는 그리드 자원의 관리와 할당을 담당한다. 여기에는 GRAM, DUROC와 GASS 등이 포함된다.

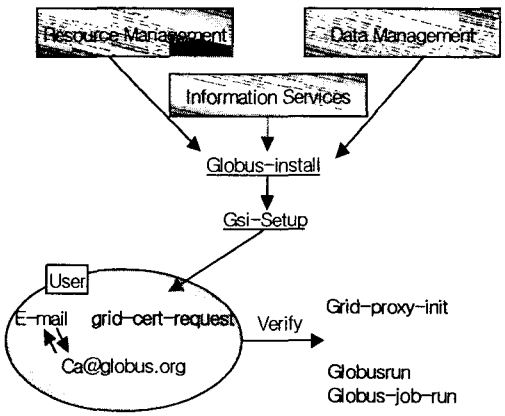
• Information Services 요소

Information Services는 그리드 자원에 관한 정보를 제공한다. 또한 GIIS와 GRIS 구성요소를 제공하는 MDS를 포함한다.

• Data Management 요소

Data Management는 그리드 환경에서 데이터 액세스 및 관리 기능을 제공한다. Data Management는 그리드 저장 시스템 사이에서 파일을 옮기는데 사용하는 GridFTP와 같은 구성요소를 포함한다.

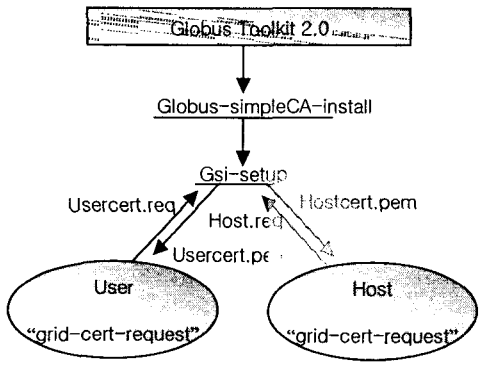
Globus 툴킷을 설치하는 과정을 나타내면 그림 1과 같다. GSI 환경을 셋업한 후 사용자는 CA 서버에 인증서를 요청하여 이메일로 인증서를 받는다. 그 다음 그리드 프락시를 초기화하고 Globusrun을 하여 설치 확인을 할 수 있다.



(그림 1) Globus 툴킷 설치 과정

3.2 인증 서버 구현

Globus simple CA 패키지는 인증서에 서명하기 위한 CA의 셋팅에 대한 편리한 방법을 제공한다. 그리드의 일부가 아닌 경우 즉, 테스트 목적으로 Globus 툴킷을 설치하기를 원하면 이 패키지가 유용하다. 이것은 또한 Globus 툴킷을 사용하는 몇몇의 사용자를 위한 테스트 그리드 환경에 적합하다. Simple CA를 설치하는 과정을 나타내면 그림 2와 같다.



(그림 2) Simple CA 서버 설치 과정

4. 그리드 보안 서비스

이 절에서는 GSI를 이용한 그리드 보안 서비스인 GridFTP와 Myproxy 프락시 온라인 저장시스템의 구현에 대하여 설명한다.

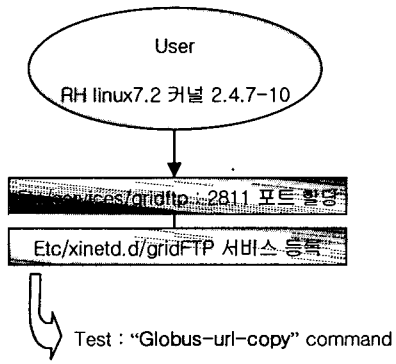
4.1 GridFTP

GridFTP는 고속의 안전하고 신뢰성 있는 네트워크 전송 프로토콜이다. 이 프로토콜은 현재 널리 사용되고 있는 파일 전송 프로토콜인 FTP를 기반으로 하고 있다. GridFTP는 기존의 FTP 프로토콜을 그리드 보안 요구사항을 충족시키도록 확장한 것으로 다음과 같은 특징을 가지고 있다[3].

- 제어 채널과 데이터 채널에 대한 GSI 보안 제공
- 병렬 전송을 위한 다중 데이터 채널
- 부분적인 파일 전송
- 서버 간 직접 데이터 전송
- 인증된 데이터 채널
- 재사용 가능한 데이터 채널
- 명령어 파이프라이닝

GridFTP 프로토콜은 globus_ftp_control과 globus_ftp_client의 두 라이버러리로 구현되어 있으며 globus_gass_copy와 명령 라인 툴인

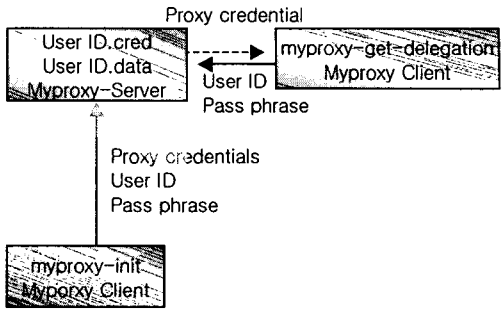
globus-url-copy를 이용하여 GridFTP, HTTP 및 로컬 파일 I/O 프로토콜에 의한 안전한 파일 전송을 제공한다. Globus-url-copy를 이용한 GridFTP 구동과정은 그림3과 같다. 사용자는 services 파일에 포트를 할당하고 xinetd.d에 서비스를 등록한 다음 globus-url-copy 명령어를 이용하여 안전하게 파일을 전송할 수 있다.



(그림 3) GridFTP 구동 절차

4.2 MyProxy

MyProxy 증명서 저장소 시스템은 하나의 저장소 서버와 저장소에게 증명서를 위임하고 저장소에서 증명서를 검색하는데 사용되는 일련의 클라이언트들로 구성된다. 일반적으로 사용자는 저장소에 접속하기 위하여 자신의 영구적인 증명서와 함께 myproxy-init 클라이언트 프로그램을 사용하여 세션을 시작하고 인증 정보와 검색 조건과 함께 서버에게 일련의 프록시 증명서를 위임한다[2]. 사용자는 또한 myproxy-destroy 클라이언트 프로그램을 사용하여 이전에 저장소에게 위임한 어떠한 증명서도 파기할 수 있다. 사용자 또는 사용자를 위한 서비스는 서버와 연결하기 위하여 myproxy-get-delegation 프로그램을 사용하여 사용자의 증명서에 대한 위임을 요청한다. 저장소는 사용자가 위임과 함께 제시한 제한조건을 확인한 다음 프록시 증명서를 사용자 또는 서비스에게 제공하게 된다. 저장소로부터 이렇게 위임된 프록시는 그리드 상에서 사용자를 대신하는 기능을 시작할 때 사용자를 위한 증명서로서 사용될 수 있다. MyProxy 동작 과정은 그림 4와 같다.



(그림 4) MyProxy 동작 과정

5. 결 론

본 연구에서는 그리드 보안의 요구사항 및 프로토콜에 대하여 기술하였고 Globus 툴킷 및 CA 서버 설치하여 GSI 환경을 구축하였다. 리눅스 환경에서 설치한 툴킷 및 CA 서버를 이용하여 그리드 보안의 주요 기능을 확인하였으며, 그 동작원리를 연구하였다. 또한, 그리드 포탈이 GSI를 안전하고 확장 가능한 방법으로 엑세스할 수 있도록 설계되고 개발된 MyProxy 온라인 증명서 저장소와 GridFTP의 기능을 검증하였다. MyProxy는 현재 NCSA, NPACI 및 NASA Power GRID 등 여러 곳의 생산 포탈에서 사용되고 있으며, 포탈 이외에도 다른 응용 레벨의 서비스에도 유용할 것으로 사료된다.

참고문헌

[1] Randy Butler et al, "A National-Scale Authentication Infrastructure," IEEE Computer, pp.60-66, December 2000.

[2] J. Novotny and S. Tuecke, "An Online Credential Repository for the Grid: MyProxy," In Proc. of 10th IEEE International Symposium on HPDC 2001, pp.104-111, San Francisco, USA, Aug. 2001.

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

[4] Ian Foster, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," In Proc. of Cluster Computing and the GRID 2001," pp.6-7, Vrisbane, Australia, May 2001.

[5] S. Tuecke, "Grid Security Infrastructure Roadmap," draft-gridforum-gsi-roadmap-02.doc, July 2001.