Grid Security Infrastructure에 관한 연구

함동읍*, 박재영*, 문두현*, 박세현*, 송오영*

*중앙대학교, 전자전기공학부

A Study of Grid Security Infrastructure

Dong Eup Ham*, Jae Young Park*, Du Hyun Mun*, Se Hyun Park*, Oh Young Song*,

School of Electrical & Electronics Engineering Chung Ang Univ.

요 약

그리드 컴퓨팅은 지리적으로 분산되어 있는 고성능 컴퓨팅 자원(컴퓨터, 데이터베이스, 첨단, 장비 등)를 네트워크로 상호 연동하여 조직과 지역에 관계없이 사용할 수 있는 가상의 슈퍼 컴퓨터를 구성하는 것이다. 하지만 상호 연동과정에서의 보안적 취약성으로 인하여 많은 문제점을 안고 있는 것도 사실이다. 본 연구에서는 그리드 개요, 구조, 국내외적인 동향에 대해서 알아보고, 이를 바탕으로 그리드의 Security 문제를 해결하기 위한 방안을 제시한다.

I. 서론

그리드 이론의 창시자인 미국 시카고대학교 컴퓨터공학과 교수인 Ian Foster에 의해 "e-교육, e-과학, e-산업, e-비즈니스 등의 기반이 되는 새로운 정보통신 사회간접자본" 이라고 정의된 그리드(GRID)는 하이퍼텍스트 형태의 단일 자원만을 이용하는 웹과는 달리 지리적으로 분산된 고성능 컴퓨터, 대용량 데이터베이스 및 첨단 장비 등 정보통신 자원을 초고속 네트워크로 연동함으로써 기초 과학과 산업기술연구에 필수적인 고속연산, 대량의 데이터 처리, 첨단 장비의 상호공유 등을 가능하게 할 뿐만 아니라 사이버 공간에서 협업 연구나 작업을 가능하게 해주는 새로운 개념의 정보통신 서비스를 통칭하는 것으로서 1998년에 미국에서 처음 제안되었다.[1]

현재 인터넷상에서 널리 활용되고 있는 웹과 그리드를 비교하면 다음과 같다. 먼저, 웹은 HTML 문서에 대한 단일 액세스를 제공한다. 클라이언트/서버 모델에서는 웹서버라는 서버 프로그램과, 이 서버에 서비스 요청을 하수 있는 웹브라우저라는 클라이언트 프로그램이 있어야 한다. 이러한 클라이언트/서버 모델에서의 보안은 클라이언트와 서버만 고려하면 되었다.

반면에 그리드는 모든 주요 자원들에 대한 고성능의 유연한 액세스를 제공하며 요구가 발생할 때 강력한 가상 전산시스템을 생성한다. 그리드 환경에서는 컴퓨터가 서로 다른 기관, 국가에 걸쳐 존재하기 때문에 보안 정책도 기관, 국가에 따라 달라질 수 있다.

구조화 및 작성과 관련된 프로그래밍 문제에 실제 이용 가능한 그리드를 생성하는데 있어서 해결해야할 문제점들은 다음과 같다.

첫째, 문제해결에 대한 접근방식들로서 데이터 그리드, 분산 컴퓨팅, P2P, 협업 그리드 등이 있다.

둘째, 프로그램의(Programming problem)로서 추상화 및 도구 등이 있다. 여기에서는 고도의 애플리케이션 개발과 코드공유를 촉진하며 API(Application Programmer Interface), SDK(System Development Kit), 도구 등과 같은 프로그래밍 환경을 필요로 한다.

셋째, 각각의 기관들 사이에서의 자원공유가 가능한 기능과 관련된 시스템 문제(System problem)로서 자원검색, 액세스, 예약, 배분, 인증, 권한부여, 정책, 커뮤니케이션, 오류확인 및 통보 등이 있다. 여기에서는 다양한 자원의 통합된 활용과 인증, 권한부여, 정보서비스 등과 같은 기반구조의 공유를 촉진하며 프로토콜과 서비스 등과 같은 시스템들을 필요로 한다. 예를 들어 정보에 대한 액세스와 자원의 분배를 위한 포트, 서비스, 프로토콜 등이 필요하다.

이 중에서 본 보고서에서는 보안기능에 대해서 살펴본다.

II. 그리드 구조 및 동향

2.1 그리드 구조

그리드 구조를 기술하는 목적은 그리드 프로토콜과 서비스의 나열이 아니라 범용 적인 구성 요소들을 위한 요구사항을 나타내기 위해서 이다. 이러한 구성요소들은 각각의 계층으로 나뉘어져 있다. 그리드 구조의 다양한 계층을 나타날 때 흔히 "모래시계"[2] 모델을 사용하는데 모래시계의 좁은 목 부분은 핵심적인 기능과 프로토콜을 나타낸다. 모래시계 모델의 상위 부분에는 서로 다른 고수준(high-level) 기능들이 매핑 되고 이와 같은 기능들은 핵심 프로토콜을 통해서 모래시계의 아래 부분에 위치하는 수많은 기반 기술과 대응된다. [3]

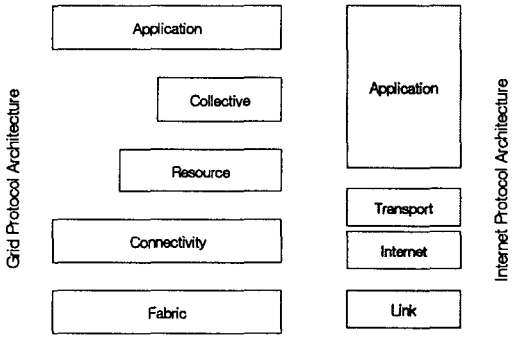

그림 1 그리드 계층 구조와 인터넷 프로토콜 계층의 관계

2.2 국내외 그리드 연구 동향

미국과 유럽 등의 선진국에서는 2000년대 이후에 그리드 관련 연구 분야에 많은 투자를 하고 있다. 그리드의 개념이 본격적으로 소개된 이후 이들 선진국은 그리드 연구가 현재의 응용 연구계산 혹은 슈퍼컴퓨팅의 벽을 뛰어넘을 수 있다고 판단하여 이러한 투자를 추진한 것이다. 따라서 과거에 수행되어온 다양한 종류의 슈퍼컴퓨팅 관련 연구들이 그리드 환경으로 집결되었다. 표 1은 주요 선진국에서 수행하고 있는 국가차원의 그리드 프로젝트를 나타내고 있으며, 그리드 연구가 2000년 이후에 관련 투자가 집중적으로 시작됨을 알 수 있다. 현재는 표에 나타나지 않은 유럽의 여러 국가에서도 그리드 연구 투자가 시작되고 있으며 대만, 싱가포르 등의 아시아 국가들에서도 연구가 시작되고 있다. 현재의 그리드는 그리드 인프라 구축과 미들웨어 연구에 많은 투자가 이루어지고 있으나 그리드를 활용한 응용 연구 또한 초기 단계에서부터 지원되고 있다[5, 6].

표 1 그리드 프로젝트 현황 (단위 : 백만)

GriPhyN	미국	NSF	$ 13.5	'00 - '05
e-Science	영국	영국정부	£ 98	'00 - '02
EuroGrid	유럽연합	EC	Eur 2	'01 - '04
EU DataGrid	유럽연합	EC	Eur 10	'01 - '04
LCG(Ph1)	스위스	CERN	CHF 30	'02 - '04
NEESGrid	미국	NSF	$ 10	'01 - '04
TeraGrid	미국	NSF	$ 53	'01 - '04
IPG	미국	NSF	$ 9.5	'01 - '04
ITBL	일본	RIKEN	-	-

국내 국가 그리드의 기본 계획은 2001년도 5월에 정보통신부는 세계적인 그리드 연구 활동에 부응하기 위해 KISTI 슈퍼컴퓨팅센터와 국가 그리드 기본계획을 발표하였다. 국가 그리드 기본계획에는 그리드 프로젝트를 수행하기 위해 필요한 4가지 요소(4As)는 Advanced User, Advanced Computer, Advanced Application, Advanced Network 가 모두 포함되어 있다. 그 중에서도 KISTI 슈퍼컴퓨팅센터는 국가 그리드 사업을 수행하는데 있어서 응용연구에 가장 주안점을 두고 있다. 이것은 기존의 네트워크 환경에서 연구 가능한 핵심 응용 분야를 선택하고, 응용연구를 위한 미들웨어 기술을 개발하는 것이다. 한편, 국가 그리드 사업을 세부적으로 수행하고 관련 연구자 간의 교류를 촉진하기 위해 그리드 포럼 코리아 (http://www.gridforumkorea.org)가 2001년 10월에 결성되었으며, 현재 24개로 구성되어 활동 중에 있다[7].

국가 그리드 기본계획이 수립되기 수년 전부터 국내에서는 KISTI 슈퍼컴퓨팅센터 중심으로 그리드 컴퓨팅 연구를 수행해 왔으며, 1단계 그리드 테스트베드로서 IBM, Compaq, Cray T3E 등 국내에 산재해 있는 다양한 이 기종의 슈퍼컴퓨터들을 연결하여 실제 응용 연구를 수행하였다.

현재, 국가 그리드 기본 계획에는 항공우주 분야뿐 만 아니라 다양한 응용 분야의 연구들이 포함되어 있다. 나노물질의 구조를 파악하고 우수한 물질의 개발을 위한 나노 그리드, 신약 개발과 새

로운 단백질의 구조 규명 등 생물학 분야의 연구를 위한 바이오 그리드, 환경 오염 문제의 해석 등을 위한 환경 그리드 등이 국가 그리드의 일부로서 연구되고 있다. 아울러, 세계적으로 경쟁력을 가지는 그리드 기술의 확보를 위하여 그리드 미들웨어의 세부 기술들과 연계하여 자동화된 그리드 컴퓨팅 구현을 위한 기술 개발을 수행 중에 있다.

III. 그리드 보안 요구사항

3.1 일반적인 보안 요구사항

3.1.1 인증

인증은 어떤 요구나 요청이 전달될 때 상대방이 누구인지 확인하는 과정이다. 어떤 서비스가 이루어지기 전에 먼저 상대방이 누구인지를 알아야 서비스를 받을 자격이 있는지 아닌지를 판단할 수 있다.

그리드 이전의 클라이언트/서버 모델에서는 서버에 대한 클라이언트 인증이 중요했지만, 그리드 환경에서는 서버와 클라이언트 사이에 상호 인증(Mutual Authentication)이 중요하다 그리드 환경에서는 서비스 요청자(클라이언트)가 서비스 제공자(서버)의 기능도 함께 가지는 등 클라이언트와 서버가 서로 대등한 기능을 한다. 따라서 정보 제공자에게 알려진 신원 증명을 위한 데이터에 의해 서비스 요청자가 악용될 소지가 있다. 이런 이유 때문에 클라이언트에 대한 서버의 인증 또한 중요하다.

3.1.2 허가

허가는 인증된 사용자에 의해 특정한 조작이 가능한지를 판단하는 과정이다. 웹 컨텐츠에 접속할 때 Access Control List를 참조하여 사용자마다 실행권한이나 접근권한을 제어하는 것처럼 그리드에서도 사용자에 대한 허가 기능이 있어야 한다. 허가를 하려면 인증된 사용자가 누구인지 알아야 하므로, 당연히 인증 과정이 선행되어야 한다. 그리드에서는 여러 가지 계산 자원이 존재하는데, 사용자가 누구인가에 따라 사용할 수 있는 계산 자원의 종류를 다르게 설정할 수 있어야 한다. 예를 들어 로컬 디스크를 이용하지 못하게 한다든지, 네트워크 대역폭을 미리 예약한다든지, 특정한 컴퓨터에만 작업을 수행할 수 있게 한다든지, 또는 외부에서 실행파일을 가져와서 실행할 수 없게 한다든지 하는 것은 모두 허가 또는 권한을 부여하는 과정에서 결정된다.

3.1.3 자격 부여

서비스 제공자가 서비스 요청자의 권한을 검사하는 과정이 허가라면, 그 전에 서비스 요청자는 적절한 서비스 제공자를 선택해야하는 과정을 거쳐야 한다. 서비스 요청자는 자신의 요구사항을 만족시킬 수 있는 서비스 제공자의 성능, 신뢰성 또는 보안 정도 등을 판단해 가장 좋은 조건을 가진 서비스 제공자를 선택하려고 한다. 이 때 서비스 제공자가 제시한 서비스 질의 정도를 서비스 요청자가 신뢰할 수 있도록 하기 위해서는 서비스 제공자의 서비스 등급을 판단하는 과정이 필요하다. 그리드 환경에서 컴퓨팅 자원에 이러한 등급을 매김으로써 서비스 요청자는 자신에게 알맞은 서비스 제공자를 믿고 찾을 수 있다.

3.1.4 계정 관리

그리드 환경에서 계정 관리는 컴퓨팅 자원의 사용량을 감시하고, 제한하고 또는 사용량에 따라 요금을 부과하기 위해 필요하다. 계정 관리를 통해 각 계정에 따른 자원의 사용량을 제한하고, 자원 이용에 있어 사용자 별로 우선 순위를 부여할 수도 있다. 그리드 환경에서 계정 관리는 분산된 형태로 이루어지고 확장이 가능해야 한다. 그리드로 연결되어 있는 컴퓨터의 수가 많아질수록 그것을 이용하는 사용자의 수도 많아지므로 일일이 계정을 하나씩 부여한다는 것은 올바른 해결책이 아니다.

3.1.5 감사

감사는 어떤 시스템에서 발생한 중요한 이벤트에 대한 정보를 기록으로 남기는 것이다. 시스템이 다운되거나 문제가 생겼을 경우, 감사 기록을 통해 그 원인을 추측해 볼 수 있다. 그리드 환경은 분산되어 있고, 작업이 여러 곳에 흩어져 수행될 수 있기 때문에 그리드 환경에서 감사 기록 또한 분산되어야 한다. 분산된 감사 기록 시스템은 분산 실행중인 작업에 문제가 발생했을 경우 해결의 실마리를 제공한다.

3.1.6 무결성과 비밀성

일반적인 보안 시스템에서와 마찬가지로 그리드 환경에서도 무결성과 비밀성은 중요하다. 데이터가 저장되거나 네트워크를 통해 다른 곳으로 전송될 때 제 3자에게 노출되거나 공격자에 의해 변경 및 조작되는 것을 방지해야 할 때가 있다. 인

터넷과 같은 외부로 노출되어 있는 네트워크 환경에서 이러한 요구는 더더욱 필요하다. 그리드 미들웨어는 응용 프로그램에서 이러한 기능을 요구할 경우 지정된 데이터에 대해 무결성과 비밀성을 보장해야 한다.

3.2 그리드 보안

그리드의 출현과 전개는 분산 시스템의 보안에 많은 영향을 주었다. 전통적인 시스템에서 보안 메커니즘의 초점은 사용자로부터 시스템을 보호하는 것이었으나 그리드에서는 사용자의 데이터, 네트워크 전반에 산재되어 있는 실행코드에 대한 인증과 실행 확인 수단들도 요구되고 있다. 또한 그리드 자원들은 여러 기관에 의해서 관리되기 때문에 서로 다른 보안 요구사항과 보안 정책의 충돌 가능성을 가지고 있다.

다음은 GSI에서 요구하는 보안 요구사항과 표준 솔루션을 보여준다.[8]

3.2.1 보안 요구 사항

그리드 보안 솔루션은 현재 존재하고 사용 가능한 표준을 토대로 한다. 보안은 매우 복잡한 문제로써 많은 시간동안 뛰어난 개발자들에 의해서 개발 되어왔다.

3.2.1.1 인증 요구사항

o. Single Sign On

사용자는 반드시 단지 한번의 "log on"(인증) 과정만으로 그리드 내의 사용하기로 허가받은 모든 자원에 어떤 개입이나 간섭 없이 접근할 수 있어야 한다.

o. 위임 (Delegation)

사용자는 자신의 권한을 프로그램에게 부여할 수 있어야 한다. 프로그램이 사용자가 인증 받은 자원에 접근할 수 있어야 한다. 또한 프로그램은 다른 프로그램에게 다시 권한을 위임할 수 있어야 한다.

o. 산재되어 있는 로컬 보안 솔루션의 통합

각각의 사이트나 자원 제공자는 커버로스, 유닉스 보안등의 다양한 보안 솔루션을 가지고 있다. 그리드 보안 솔루션은 이러한 다양한 보안 솔루션끼리의 상호운용을 지원하여야한다. 모든 로컬 보안 솔루션을 대처할 수는 없지만 로컬 환경에 맞는 매핑은 제공하여야 한다.

o. 사용자 기반 신뢰 관계

사용자가 다양한 제공자의 자원을 함께 사용하기 위해, 보안 시스템은 각각의 자원 제공자들이 서로 협력하는 것을 요구하거나, 보안 환경 설정 시에 서로 상호 작용하도록 해서는 안 된다. 만일 어떤 사용자가 사이트 A와 B를 사용할 권한이 있다면, 그 사용자는 사이트 A와 B의 보안 관리자들에게 상호 작용하는 것을 요구하지 않고 사이트 A와 B를 사용할 수 있어야 한다.

3.2.1.2 통신상의 요구사항

o. 유연한 메시지 보호

응용프로그램은 서비스 프로토콜을 메시지 보호를 위한 여러 가지 수준, 즉 보호를 안 한다거나 무결성만을 제공하거나 무결성과 기밀성을 동시에 제공하는 여러 수준으로 설정할 수 있고 그 설정을 변경할 수 있어야 한다.

o. 다양한 신뢰성 있는 통신 프로토콜 지원

TCP가 인터넷에서 가장 널리 사용되는 신뢰성 있는 통신 프로토콜이지만, 다른 프로토콜의 신뢰성을 높이기 위해 보안 메커니즘을 적용할 수 있어야 한다. TCP를 지원하지 못하는 특별한 환경이 있을 수도 있다.

o. 독립적인 데이터 단위 지원

어떤 응용프로그램은 다른 데이터 단위의 보호 여부와는 무관하거나, 지정된 수신자의 연결여부와 무관하게 스트리밍 미디어, 이메일과 신뢰성 없는 UDP에서의 일반적인 데이터 단위의 보호를 필요로 한다.

3.2.1.3 권한 부여 요구사항

o. 제 3자에 의한 인증

자원 소유자 또는 제 3자들은 사용자가 적당한 조건이 되면 자원에 접근할 수 있도록 인증하여야 한다.

o. 제한 위임

손상되거나 오용된 위임된 인증서로 인하여 발생할 수 있는 취약성을 최소화하기 위해, 위임되는 인증 권한을 제한하기 위한 많은 정책을 가지고

있는 것이 바람직하다.

3.2.2 관련 표준안

현재 다양한 종류의 보안 표준이 존재하지만 앞서 기술한 모든 요구사항을 만족하는 표준은 없다. 아래에서는 현재 존재하는 표준과 요구사항간의 관계를 기술한다.

3.2.2.1 커버로스[9]

커버로스는 대칭키 기반의 메시지 암호화, 무결성, 인증 기능을 수행하는 표준이다. 커버로스는 Single Sign On, 위임, 유연한 메시지 보호 등의 그리드 요구사항을 지원한다. 그러나 아래와 같은 사항은 지원하지 않는다.

o. 산재되어 있는 로컬 보안 솔루션의 통합

o. 사용자 기반 신뢰 관계

3.2.2.2 TLS(Transport Layer Security)[10]

TLS는 공개키 기반의 메시지 암호화, 무결성, 인증 기능을 수행하는 표준이다. 커버로스와는 달리 사용자 기반 신뢰관계는 만족시키지만 Single Sign On과 위임은 지원하지 않는다.

3.2.2.3 PKIX(Public Key Infrastructure eXtension)[11]

PKIX는 공개키 기반 구조에서 X.509 인증서 기반의 표준이다. X.509 표준은 TLS 같은 다른 보안 통신 표준과의 연동되어 사용된다.

3.2.2.4 암호 메시지 구문(CMS : Cryptographic Message Syntax)[12]

CMS는 디지털 서명, 다이제스트, 인증, 메시지의 암호화에 대한 표준이다. 이는 독립적인 데이터 단위(IDUs)를 보호하는 표준이다.

3.2.2.5 GSS-API(Generic Security Service API)[13][14]

GSS-API는 인증, 메시지 무결성, 기밀성을 제공하기 위한 API를 정의한 표준이다. GSS-API에서는 두 상대방이 서로 신뢰성이 있고, TCP/IP 같은 연결 지향 토인 프로토콜을 사용한다고 가정하고, 다양한 보안 메커니즘을 활용할 수 있기 때문에 그리드 보안 요구사항의 대부분을 지원한다.

3.2.2.6 IDUP-API(Independent Data Unit Protection GSS-API)[15]

독립 데이터 단위의 보호를 지원하는 GSS-API의 확장판이다. IDUP-GSS-API는 신뢰성이 없거나 순서가 없거나, 멀티캐스트, 비 연결 지향적인 통신에서의 보호를 지원한다.

3.2.2.7 SPKM(Simple Public Key GSS-API Mechanism)[16]

SPKM은 인증, 메시지의 무결성 및 기밀성을 제공하기 위해 간단한 공개키 메커니즘을 사용하여 GSS-API를 구현할 때 사용하는 프로토콜 절차와 규정을 정의한 프로토콜이다.

3.3 그리드 보안 기반 구조(GSI : Grid Security Infrastructure)

GSI 프로토콜, API들과 서비스들은 가능한 현존하는 표준들의 개정을 통하여, 앞서 기술한 요구사항들을 만족하도록 조합되고 개발된다. GSI는 그리드의 구성원 사이트들에서 서로 다른 로컬 보안 서비스들 간의 차이를 연결해주는 도메인 상호 보안 프로토콜을 제공한다

.GSI 서비스의 특징은 다음과 같다.

그림2는 그리드 보안 기반구조에서 제공하는 기본 동작을 개념적으로 보여준다.

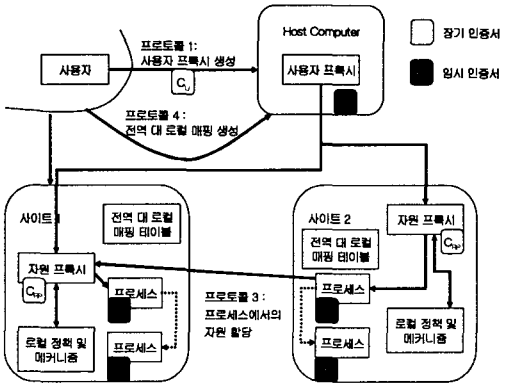

그림 2 그리드 보안 기반구조 기본 동작

먼저 공개키 메커니즘을 이용하여 사용자의 인증서 Cu를 생성한 후 호스트 컴퓨터에서 사용자의 프록시 임시 인증서 Cup를 생성한 후 사이트 2의 자원이나 프로세스를 사용하기 위해서 로컬의 보안 정책과 메커니즘을 적용하여 자원

프록시 인증서 C_{RP}에서 사용자에게 위임된 임시 인증서 Cp를 생성한다.

이 경우에 각 사이트의 자원에 접근하기 위해서 각 사이트의 전역 대 로컬 매핑 테이블을 이용하여 접근에 필요한 위임된 임시 인증서 Cp를 생성하게 된다. 결과적으로 위임된 임시 인증서 Cp를 이용하여 사이트2에 원격 프로세스를 생성하게 된다.

생성된 위임된 임시 인증서 Cp를 이용하여 사이트1과 같은 다른 사이트에서 위의 과정을 반복하여 사이트1을 위한 위임된 인증서를 다시 생성할 수도 있고 만약 사이트1과 사이트2가 신뢰 관계에 있다면 직접 사이트1에서 프로세스를 생성할 수도 있다.[17]

IV. 결론

IT분야에서 미래를 예측하는 것은 아주 어려운 일이다. 하지만 현재 프로세서 기술의 발전과 네트워크 속도의 발전을 기반으로 IT분야를 예측해 본다면 그리드 기술이 대세를 이룰 것으로 전망된다. 하지만 구현측면에서 볼 때 많은 보안상의 허점이 존재하는 것도 사실이다. 이에 본 논문에서는 Grid Security Infrastructure를 구현하기 위해 적용될 수 있는 보안적 요소를 살펴보았고, 어떻게 적용할 것인가에 대해 제시하였다.

참고문헌

[1] 안현수 "차세대 인터넷 기반구조로서의 그리드(GRID)에 관한 고찰", TTA 저널 제 80호

[2] Realizing the Information Future : The Internet and Beyond. National Academy Press, 1994. http://www.nap.edu/readingroom/book/rtif

[3] Ian Foster, Carl Kesselman, Gene Tsudik, Steven Tuecke, "The Anatomy of the Grid"

[4] Ian Foster and Carl Kesselman (eds.) "The Grid : Blueprint for a new Computing Infrastructure" Morgan Kaufmann Publishers, 1998

[5] 조금원, "그리드 응용과 전산 유체역학", 슈퍼컴퓨팅소식 5권 36-40페이지 2001년 6월

[6] 이식, "인터넷 컴퓨팅의 생물학 응용 및 BioGrid의 동향", 슈퍼컴퓨팅소식 5권 41-45 페이지 2001년 6월

[7] www.gridforumkorea.org

[8] Steven Tuecke, "Grid Security Infrastructure(GSI) Roadmap

[9] Kohl, J. and C. Neuman, "The Kerberos Network Authentication Service(V5)," RFC1510, September 1993.

[10] Dierks, T. and C. Allen, "The TLS Protocol, Version 1.0," RFC 2246, January 1999.

[11] Arsenault, A. and S. Turner, "Internet X.509 Public Key Infrastructure, PKIX Roadmap," Internet Draft, March 1999.

[12] Housley, R., "Cryptographic Message Syntax," RFC 2630, June 1999.

[13] Linn, J., "Generic Security Service Application Program Interface, Version 2, Update 1, " RFC 2743, January 2000.

[14] Wray, J., "Generic Security Service API Version 2, C-bindings," RFC 2744, January 2000

[15] Adams, C,. "Independent Data Unit Protection Generic Security Service Application Program Interface (IDUO-GSS-API),"RFC 2479, December 1998.

[16] Adams, C., "The Simple Public-Key GSS-API Mechanism(SPKM), "RFC 2025, October 1996.

[17] Ian Foster, Carl Kesselman, Gene Tsudik, Steven Tuecke, "A Security Architecture for Computational Grids"