제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

효율적인 인증서 관리를 위한 Grid CA 클라이언트 설계 및 구현

이성현*, 박형우**, 이원구*, 이희규*, 이재광*
*한남대학교 컴퓨터공학과
**한국과학기술정보연구원
e-mail:shlee@netwk.hannam.ac.kr

Design and Implementation of Grid CA Client for Efficient Certificate Management

Seoung-Hyeon Lee*, Hyung-Woo Park**, Won-Goo Lee*,
Hee-Gyu Lee*, Jae-Kwang Lee*
*Dept of Computer Science, Hannam University
**KISTI

요 약

그리드 환경(Grid Environment)은 인터넷을 통하여 사용하지 않는 컴퓨팅 자원을 공유하여 활용하고자 하는 의도에서 연구가 진행되었다. 그리드 환경에서는 전 세계에 흩어져 있는 컴퓨팅 자원에 특정 형태의 운영 프로그램을 설치하여, 각각의 자원에 접근하여, 저장 공간을 공유하고 프로세스를 실행 시킬 수 있는 컴퓨팅 통합 환경이다. 이러한 시스템에서는 각각의 자원에 대한 접근 및 프로세스의 생성 및 실행에 있어서 사용자 혹은 프로세스에 대하여 X.509 인증서를 기반으로 구현된 특별한 형태의 인증 메커니즘을 지니고 있다. 본 논문에서는 그리드 환경에서 인증서를 활용한 인증 메커니즘에 대해서 살펴보고, 해당 인증서를 효율적으로 관리할 수 있는 그리드 인증서 관리 모듈을 설계하고 구현한 후, 향후 연구되어야 할 방향을 제시하였다.

1. 서론

컴퓨터 및 네트워크의 성능이 향상됨에 따라 이들 자원을 공유하여 효율적으로 사용하고자 하는 분산 시스템에 대한 논의가 활발히 진행되고 있다. 그리드(Grid) 환경은 이러한 논의를 바탕으로 분산 시스템에서 한 걸음 더 나아가 전 세계에 흩어져 있는 컴퓨팅 자원을 인터넷 망을 통하여 하나의 단일 컴퓨팅 자원처럼 활용할 수 있도록 하자는 개념에서 출발하였다[1][2][9][10].

그리드 환경에서 다른 시스템의 컴퓨팅 자원을 활용하고자 하는 사용자, 호스트 및 프로세스는 각각의 컴퓨팅 자원을 사용하는데 있어서 단 한번의 로그인 후에 다른 컴퓨팅 자원에 접근할 때 추가적인 인증 과정을 거치지 않는 단일 인증(Single Sign-on) 서비스, 인증 받은 사용자의 컴퓨팅 자원의 사용 권한에 대한 접근제어(Access Control) 서비스 등과 같은 보안문제와 관련된 서비스에 대한 기반기술이 뒷받침되어야만 효율적이고 안전한 운영을 할 수 있다[3][4][6][11].

현재 그리드 환경에서 각각의 서비스를 제공하기 위해서 개발된 미들웨어로는 글로버스(Globus)가 있다. 글로버스에서는 컴퓨팅 자원에 대한 인증 서비스를 제공하기 위해서 X.509 기반의 인증서를 적극적으로 활용하고 있다.

X.509 기반의 인증서는 인증과 데이터 무결성, 부인-방지 서비스를 효과적으로 제공할 수 있는 수단이다. 글로버스에서는 이러한 인증서를 통하여 인증 서비스를 제공함으로써 기존의 시스템에 큰 변경 없이 손쉽고 효율적으로 인증 서비스를 제공한다.

본 논문에서는 그리드 환경에서 요구하고 있는 사용자 인증 요구사항과 메커니즘을 살펴보고, 글로버스에서 인증 서비스를 제공하기 위해서 사용하고 있는 X.509 인증서 기반으로의 관리 클라이언트를 설계하고 구현한다.

* 본 연구는 한국과학기술정보연구원 슈퍼컴퓨팅 센터의 "그리드 미들웨어" 과제 지원 및 관리로 수행되었습니다.

본 논문의 구성은 다음과 같다. 2장에서는 그리드 환경에서의 인증 메커니즘에 대해서 살펴보고, 3장에서는 인증서를 효율적으로 관리할 수 있는 클라이언트를 설계한 후, 4장에서 이를 구현한다. 마지막으로 5장에서 연구된 내용에 대한 결론을 맺고 향후 연구방향을 제시한다.

2. 관련 연구

그리드 환경에서 컴퓨팅 자원에 접근하여 사용하고자 하는 사용자, 호스트 및 서비스는 그들에 대한 사용자 인증을 필요로 한다. X.509 인증서는 이러한 인증 문제를 해결하기 위해 제안된 표준의 한 방법이다. X.509 인증서는 신원을 증명하기 위해서 필요한 공개키와 인증서 소유자가 속한 그룹의 고유한 이름, 인증서 유효 기간과 인증서 폐지 목록 등을 포함하고 있다. 본 장에서는 그리드 환경에서 요구하고 있는 사용자 인증에 대한 요구사항과 인증서를 활용한 인증 메커니즘에 대해서 살펴본다.

2.1 사용자 인증 요구사항

그리드 환경에서 각각의 컴퓨팅 자원을 사용하기 위해서 사용자가 접근하는 경우의 인증 요구사항은 다음과 같다[3][4].

- 단일 인증(Single sign-on)

사용자는 추가적인 인증과정 없이 단 한번의 인증을 통하여 그리드 환경에서 자원을 얻고, 자원을 사용하고, 남은 자원을 반환하며, 내부 통신을 수행할 수 있어야 한다. 추가적인 자원에 대해서는 인증을 요구하지 않는다[3][4][6].

- 위임(Delegation)

사용자는 인증을 거친 후에 그리드 환경으로부터 얻은 권한을 수행하는 프로그램에 부여해 각 컴퓨팅 자원들에 접근할 수 있어야 한다[3][4][6].

- 다양한 지역 보안 솔루션 통합(Integration with various local security solutions)

사용자는 그리드 환경에서 인증 받은 권한에 대해서 다른 형태의 로컬 보안 솔루션과 관계없이 컴퓨팅 자원에 대한 권한을 행사할 수 있어야 한다[3][4][6].

- 사용자 기반 신뢰 관계(User-based trust relationships)

사용자가 그리드 환경의 다양한 컴퓨팅 자원을 사용하기 위해서, 인증 시스템은 각각의 자원 제공자들이 서로 협력하는 것을 요구하거나, 상호 작용하는 것을 허용하지 말아야 한다. 즉, 어떤 사용자가 그리드 환경 A와 B를 사용할 권한이 있다면, 그 사용자는 A와 B의 보안 관리자들에게 상호 작용하는 것을 요구하지 않고도 A와 B를 함께 사용할 수 있어야 한다[3][4][6].

2.2 사용자 인증 메커니즘

이전 절에서 살펴본 바와 같이 그리드 환경에서의 사용자 인증은 많은 요구사항을 포함하고 있으며, 현재까지 모든 요구사항을 수용할 수 있는 관련 기술이 존재하지 않기 때문에 각각의 요구사항을 만족하는 기존 기술을 개선하고 통합하여 사용하고 있다.

사용자 인증 뿐만 아니라 그리드 환경에서의 다른 서비스의 보안요소도 많은 요구사항을 포함하고, 서로 다른 보안 기술의 복합적인 적용을 필요로 한다. 이와 같은 문제점을 해결하기 위해서 그리드 환경의 보안을 연구하는 GSI 워킹그룹에서 GSI(Grid Security Infrastructure) 솔루션에 대해 논의하고 이에 대한 표준화 과정을 진행하고 있다[3][4][6].

GSI 솔루션은 가능한 현존하는 표준들의 개정을 통하여, 앞에서 설명한 사용자 인증과 통신 보안 요구사항을 만족하도록 조합되고 개발되며, 그리드 환경의 구성원 사이트들의 서로 다른 지역 보안 솔루션들 간의 차이를 연결해 주는 도메인 상호 보안 프로토콜을 제공한다. GSI에는 [그림 1]과 같은 사용자 인증 메커니즘을 제시하고 있다.

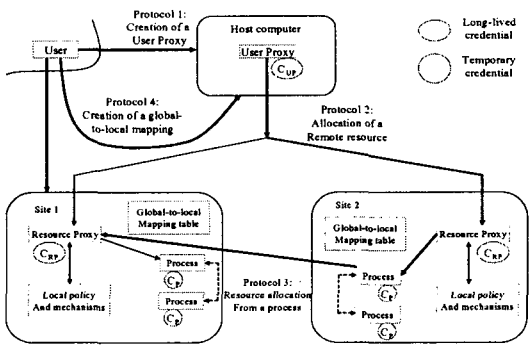

그림 3 GSI에서의 사용자 인증 메커니즘

• SSL-K5 and PKINIT

SSL-K5는 SSL 프로토콜에 기반을 두고, 커버러스에서 인증 티켓을 발행하는 도메인 컨트롤러(KDC : Key Distribution Center)를 사용할 수 있는 간단한 버전이다. PKINIT는 KDC에서 인증 티켓을 발행하는 SSL-K5를 대신하여 제정된 IETF 표준이다[4][6].

• K5Cert

K5Cert는 커버러스 인증 프로토콜을 사용하는 서비스로 클라이언트가 GSI 인증서를 생성하기 위하여 커버러스를 이용하여 사용자를 인증하는 것을 허용하며, GSI 프로토콜을 사용하여 사용자들이 쉽게 그리드 환경의 컴퓨팅 자원에 접근할 수 있도록 한번 사용자가 지역 커버러스 영역에서 인증받으면, 사용자는 그리드 환경의 컴퓨팅 자원을 사용하기 위한 GSI 프록시 인증서를 얻는 것이 용이하다[4][6].

• MyProxy

MyProxy는 클라이언트를 인증하기 위해서 커버러스를 사용하는 대신에, 클라이언트와 서버가 TLS를 사용하여 신뢰할 수 있는 채널을 만든 후에, 클라이언트가 서버에게 아이디와 패스워드를 보내면, 서버에서 저장소의 이름과 비밀번호를 비교하고, 일치여부를 확인한 후에 사용자 프록시를 위임하여 클라이언트에게 되돌려 보낸다. 사용자는 서비스 저장소에 프록시를 저장하기 위해서 MyProxy 클라이언트를 사용할 수 있다[4][6].

3. Grid CA 인증서 관리 클라이언트 설계

3.1 기본 구조

그리드 환경에서의 Grid CA의 인증서를 관리하는 클라이언트는 [그림 2]와 같이 인증서 관리 모듈과 키 관리 모듈로 구성된다.

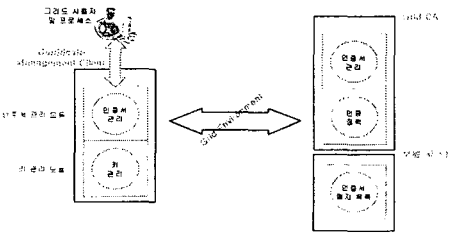

그림 4 인증서 관리 클라이언트의 기본 구조

3.2 인증서 관리 모듈

인증서 관리 모듈은 그리드 환경에서 사용자, 호스트 및 프로세스 인증을 위해서 사용되는 인증서를 관리하기 위한 모듈이다.

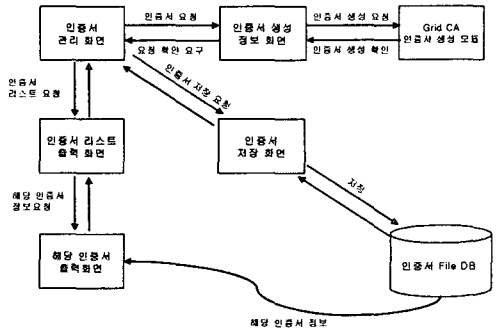

그림 5 인증서 관리 모듈

[그림 3]과 같이 인증서 관리 모듈은 Grid CA와 연계하여 인증서의 생성을 요청하고, 생성된 인증서를 관리할 수 있는 인터페이스를 제공한다.

3.3 키 관리 모듈

인증서 생성에 사용되는 공개키, 개인키 중에서 전자서명 및 공개키로 암호화된 문서의 복호화에 사용되는 개인키를 저장하는 것은 매우 중요한 문제이다. 개인키가 유출되면, 인증 시스템의 신뢰성이 무너지게 된다.

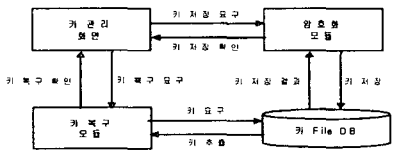

그림 6 키 관리 모듈

[그림 4]와 같이 키 저장 모듈은 개인키를 암호화하여 저장하며, 이를 다시 복원할 수 있는 암호화 모듈과 키 복구 모듈로 구성되어 있다.

4. Client 구현

4.1 인증서 관리

인증서는 그리드 환경에서 인증서는 사용자, 호스트 및 프로세스의 컴퓨팅 자원 접근을 인증해주는 매체로써 매우 중요하게 사용된다.

이러한 인증서 관리 모듈은 인증서를 편리하고, 효율적으로 관리하기 위한 모듈이다. [그림 5]의 메뉴와 같이 인증서 관리 모듈은 인증서 생성 요청, 인증서 저장, 인증서 검증, 인증서 가져오기와 내보내기 모듈로 구성되어 있다.

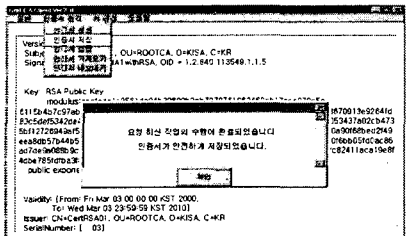

그림 7 인증서 저장

4.2 키 관리

키 관리 모듈은 그리드 환경에서 인증서를 생성할 때 사용되는 개인키를 관리하는 모듈이다. 그림에서와 보는 바와 같이 개인키 관리는 안전한 저장을 위해서 해당키를 암호화하여 지정한 장소에 저장하는 모듈과 전자서명등에 개인키를 사용하기 위해서 암호화된 키를 복호화하는 모듈로 구성되어 있다.

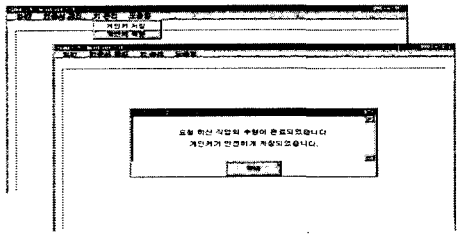

그림 8 개인키 저장

5. 결론

본 논문에서는 그리드 환경에서 각각의 컴퓨팅 자원을 사용하기 위해서 사용자가 인증을 얻는데 필요한 요구사항과 관련 기술을 살펴본 후 현재 가장 널리 사용되고 있는 인증서를 활용한 인증 메커니즘을 살펴보고, 이를 분석한 후 인증서를 효율적으로 관리할 수 있는 Grid CA 인증서 관리 클라이언트를 설계하고 구현하였다.

그리드 환경은 급격히 발전하고 있는 컴퓨팅 자원과 네트워크 성능을 접목시켜 이들을 하나의 단일 컴퓨터 시스템처럼 사용하는 것이기 때문에, 그리드 환경에서의 사용자 인증 메커니즘은 지금까지 구현된 서비스들과 다른 측면을 지니게 된다. 그리도 환경에서 안전한 사용자 인증을 거쳐 시스템을 제공하는 것은 앞에서 언급한 사용자 인증 요구사항을 고려한 후에 이를 바탕으로 효율적인 사용자 인증 메커니즘을 설계하는 것이 매우 중요하다. 본 논문에서 구현한 인증서 관리 클라이언트는 그리드 환경을 지원하기 위한 미들웨어에서 가장 활발히 논의되고 있는 인증서를 통한 인증시스템에서 각각의 인증서를 관리할 수 있는 응용 프로그램이다. 이러한 응용 프로그램이 증가할수록 그리드 환경을 효율적으로 운영할 수 있으며, 이용의 편의성으로 인하여 많은 어려움을 해결할 수 있을 것으로 본다.

향후 본 논문의 연구사항으로는 지속적으로 발전하고 있는 사용자 인증 메커니즘을 면밀히 분석한 후 국내의 실정에 맞는 인증 서비스를 제공하기 위한 응용 프로그램을 설계하고 구현하는 것이다.

참고문헌

[1] 윤찬현, 심은보, "그리드 구조 및 연구동향", 「한국정보과학회 정보과학회지」 제 20권 2호, 2002. pp.11-15

[2] 강 경우, 박형우, "그리드 연구개발 동향", 「한국정보과학회 정보과학회지」 제 20권 2호, 2002. pp.26-33

[3] Randy Butler Von Welch, Douglas Engert, Ian Foster, Steven Tuecke, John Volmer, Garl Kesselman, "A National-Scale Authentication Infrastructure", IEEE, December. 2000. pp.60-66

[4] Ian Foster, Carl Kesselman, Gene Tsudik, Steven Tuecke, "A Security Architecture for Computational Grids", 5th ACM Conference on Computer and Communication Security. 2000.

[5] Gary Tagg, "Implementing a Kerberos Based Single Sign-on Infrastructure", Information Security Bulletin, CHI Publishing Ltd. November. 2001. pp.23-36

[6] S. Tuecke., "Grid Security Infrastructure(GSI) Roadmap", Internet Draft, July. 2001.

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

[8] 이재광외 3인, 컴퓨터 통신 보안, 도서출판 그린, 2001.

[9] http://bluekim.hihome.com/subject/grid/grid_2.htm

[10] http://www.clickunikorea.com/grid.html

[11] http://www.gridforum.org/2_SEC/SEC.htm