액티브 노드 보안을 위한 그리드 상에서의 엔티티 상호 인증 기법 적용에 관한 연구

이원구°, 이재광
한남대학교 컴퓨터공학과 네트워크 실험실
e-mail : wglee@netwk.hananm.ac.kr, jklee@netwk.hannam.ac.kr

A Study Applying to Mutual Authentication Mechanism among Entities in Grid to Structure Secure Active Nodes

Won-goo Lee°, Jae-Kwang Lee
Dept of Computer Engineering, Hannam University

요 약

본 논문에서는 그리드 환경에서의 엔터티 상호 인증구조와 추가적으로 제안한 인증구조를 고찰하여, 향후 액티브 네트워크 상에서의 액티브 노드간의 상호인증구조를 구축하기 위한 초석을 다지고자 한다. 추가적으로 현재의 그리드 인가 구조에서 ID 기반이 아닌 인증서 기반의 사용자 인가 시스템을 제안하였으며, 기존의 ID 매핑 방식의 인가 시스템 대신에 인증서내의 확장 필드에 사용자의 권한 등급을 추가하고, 이를 기반으로 자원에 대한 접근 제한 등급을 결정하도록 하였다.

국문 키워드 : 액티브 노드, 그리드, 클라이언트 CA, 인증 서비스, 인가 서비스

1. 서 론[1)]

현재의 액티브 네트워크에서는 도메인마다 하나의 키 분배 서(KDS: Key Distribution Server)가 있다고 가정한다. KDS는 세션키를 생성하여 해당 네트워크 내의 노드들에게 분배한다. 이 때의 세션키는 대칭키이며 암호 통신이 종료하면 폐기된다. KDS와 액티브 노드들은 공개키 기반구조를 사용하여 전당한 노드인지를 확인하여야 한다. 각 노드들은 공개키와 비밀키를 생성하후, 공개키와 신원 정보를 인증기관에게 전송하여 인증서를 발급받는다. 이는 불법적인 노드가 암호 통신에 참여하지 못하도록 불법적인 노드가 생성하는 비정상적인 패킷이 노드를 공격하는 등의 악의적인 행동을 막는다. 단일 네트워크 내의 노드들과 암호 통신을 원하는 노드는 암호 통신 상대자들의 ID를 KDS의 공개키로 암호화한 후 자신의 공개키 인증서와 함 KDS에 전송하게 된다. 이러한 통신 메커니즘은 그리드 상에서 보다 안전하게 구현되어 가고 있다. 이에 본 논문에서는 그리드 환경에서의 엔터티 상호 인증구조와 추가적으로 제안한 인증구조를 고찰하여, 향후 액티브 네트워크 상에서의 액티브 노드간의 상호인증구조를 구축하기 위한 초석을 다지고자 한다. 추가적으로 표준문서[2][3][4]를 바탕으로 그리드에서 요구하고 있는 엔터티 인증 및 인가에 대한 요구사항과 메커니즘을 분석하고, 글로버스에서 인증 서비스를 제공하기 위해서 사용하고 있는 X.509 인증서 기반의 사용자의 권한 부여 항목과 모듈을 추가하였다. 즉, 그리드 CA(Grid CA)와 클라이언트 사이의 안전한 통신을 보장하여 인증서를 효율적이고 안전하게 관리할 수 있는 그리드 환경에서의 엔티티 보안을 위한 그리드 CA 클라이언트에 대해 추가 연구하였다.

※ 본 연구는 한국과학재단 목적기초연구(R01-2002-000-00127-0) 지원으로 수행되었음.

2. 관련연구

2.1 그리드 보안 기반구조

그리드는 어플리케이션과 계산에 사용될 사용자의 데이터를 보호하기 위한 특수한 요구사항을 가지고 있다. 더욱이, 실행 코드가 네트워크 상의 여러 곳에서 시작될 수 있기 때문에, 악의적인 코드가 실행될 수 있는 잠재성, 출처를 검증하기 위한 강력한 방법의 요구, 코드의 인증과 그것의 실행확인 수단이 많이 있다. 그리드 자원들이 많은 기관에 의해 관리되기 때문에, 서로 다른 보안 요구사항과 보안정책의 충돌 가능성을 가지고 있다. 이러한 이유로 그리드 환경에서의 보안 관리는 많은 어려움을 주고있다.

이와 같은 문제점을 해결하기 위해서 그리드 환경의 보안을 연구하는 그리드 보안 워킹그룹에서는 GSI(Grid Security Infrastructure) 솔루션에 대해 논의하고 이에 대한 표준화 과정을 진행하고 있다. 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[8].

2.2 그리드 환경에서 필요한 인증

2.2.1 위임

사용자는 자신이 그리드 자원을 활용하기 위해서 획득한 권한을 사용자 프로그램이나 프로세스에 부여할 수 있어야 한다. 그림 2와 같이 사용자 프로그램은 부여받은 권한을 가지고 해당 자원들에 접근할 수 있어야 한다. 또한 사용자 프로그램은 다른 프로그램에게 자신이 위임받은 권한을 다시 위임할 수 있어야 한다.

2.2.2 사용자 기반 신뢰 관계

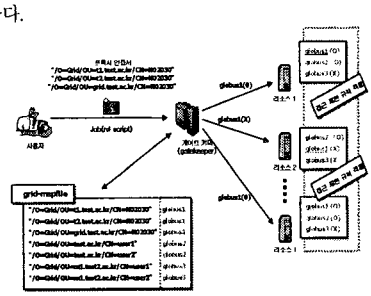
그림 4에서처럼 사용자가 다양한 제공자(Provider)의 자원을 사용하기 위해서는, 보안 시스템이 각각의 자원 제공자들과 서로 협력하는 것을 강요하거나, 보안 환경 설정 시에 상호 작용하도록 해서는 안 된다. 다시 말하면, 어떤 사용자가 사이트 A와 B를 사용할 권한이 있다면, 그 사용자는 사이트 A와 B의 보안 관리자들에게 상호 작용하는 것을 요구하지 않고도 사용자 자신이 인증 받은 권한을 가지고 사이트 A와 B를 함께 사용할 수 있어야 한다.

3. 사용자 등급 기반의 보안 서비스 모델 설계

3.1 인증서 기반의 인가 서비스 모델

3.1.1 단순 ID 기반의 인가 서비스

현재 글로버스에서는 그림 8과 같이 그리드 사용자들의 인증서에서 subject DN(Distinguished Name)을 추출하여 로컬 시스템의 ID와 매핑하여 사용자에게 권한을 부여하고 있다. 사용자가 작업을 그리드 상에서 수행하기 위해서는 작업 파일과 프록시 인증서를 해당 시스템에 전달하게 되는데 해당 시스템에서는 프록시 인증서의 subject DN을 로컬 시스템의 /etc/grid-security/grid-map에서 검색하여, 일치하는 ID를 추출하고 로컬 시스템의 ID에 따라서 로컬 시스템에 대한 자원 접근을 인가한다.



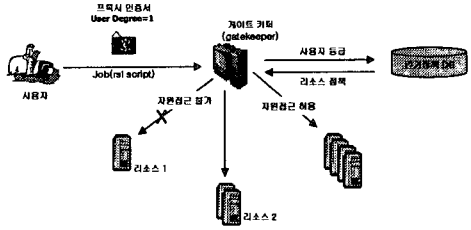
(그림 1) 단순한 ID 기반의 인가 서비스

이러한 자원에 대한 접근은 OS 차원에서의 접근 제한뿐만 아니라 LSF, PBS, LoadLeveler와 같은 작업 관리 프로그램에 의해서도 적용될 수 있다. 작업관리 프로그램에서는 사용자 ID를 기반으로 하여 사용가능한 CPU의 개수, 메모리 용량, 실행 시간등을 제한할 수 있다.

3.1.2 엔티티별 등급 기반의 인가 서비스

기존 글로버스의 사용자 인가 시스템은 해당 로컬 시스템에 접근하는 사용자가 많아지게 되면, 사용자 프록시 인증서의 subject DN과 로컬 시스템의 ID를 1:1로 매핑할 경우, 계정 관리 문제와 메모리 자원, 디스크 자원의 관리에 있어 많은 어려움을 겪게 된다. 이러한 이유로, 기존의 글로버스에서는 여러 subject DN이 하나의 로컬 ID를 공유하는 형태를 띠고 있다.

하나의 로컬 ID를 공유할 경우에 발생하는 문제는 수많은 그리드 사용자의 모든 요구사항을 적용하는데 있어서 불합리한 면을 지닌다. 이에 본 논문에서는 ID 기반이 아니라, 그림 9에서 보는 바와 같이 인증서 기반의 사용자 인가 시스템을 제안하였다. 앞서 설명한 기존의 ID 매핑 방식의 인가 시스템 대신에 인증서 내의 확장 필드에 사용자의 권한 등급을 추가하고, 이를 기반으로 자원에 대한 접근 제한 등급을 결정하도록 하였다.

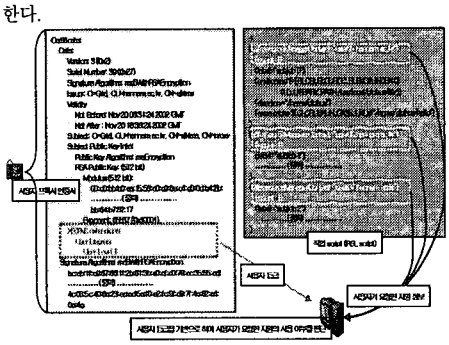


(그림 2) 인증서를 이용한 사용자 등급 기반의 인가 서비스

3.1.3 엔티티 등급별 필드 적용

본 논문에서 제안된 인증서 기반의 사용자 인가 시스템은 사용자의 프록시 인증서 내에 사용자 등급을 표시 할 수 있는 필드를 인증서 확장 영역내에 추가하였다. 사용자가 작업을 실행하기 위해서 로컬 시스템으로 작업파일과 프록시 인증서를 전송하게 되면 로컬 시스템에서는 프록시 인증서에서 사용자 등급을 추출해낸다. 이를 미리 정의된 로컬의 인가 정책 데이터베이스를 검색하여 사용자가 접근 가능한 자원과 정책에 의해서 정의된 각종 시스템 리소스 사용량을 검사하여 제출한 작업파일이 정당히 실행할 수 있는지를 검사하고 작업의 실행여부를 결정하게 된다. 그림 3은 인증서의 확장 필드에 사용자의 등급과 관련된 사항을 추가한 것이다.

또한, 인증서내의 사용자 등급을 포함하고 있는 확장 필드를 추가하기 위해서는 글로버스에서 인증서버로 사용하고 있는 SimpleCA의 openssl.conf 파일에 다음과 같은 항목과 값을 추가해야 한다.



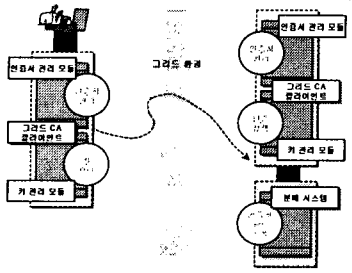
(그림 3) 인증서내의 사용자 등급 사항

3.2 그리드 CA 클라이언트의 인증서비스 모델

그리드 CA 클라이언트는 그리드 CA와의 연동을 통해서 사용자의 인증관련 요구를 받아들여, 요청 메시지를 만든 후에 그리드 CA에 전송하여 처리하는 것과, 요청에 응답된 그리드 CA의

메시지를 받아들여, 사용자에게 전달하는 역할을 담당한다.

그리드 CA 클라이언트는 그림 4와 같이 크게 인증서 관리 모듈, 키 관리 모듈로 구성되며, 그리드 CA 클라이언트와 그리드 CA의 메시지 교환은 다음과 같은 과정을 거치게 된다.

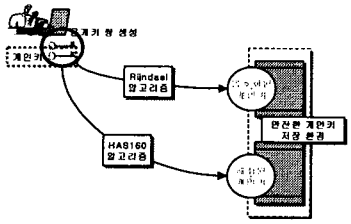


(그림 4) 그리드 CA 클라이언트 구조

위와 같은 Grid CA 클라이언트는 인증 시스템 구축에 있어서 현재 글로버스에서 사용하고 있는 인증서버와 비교하여, 기존에 없었던 인증서 관리 클라이언트를 확장함으로써, 그리드 사용자가 자신이 소유하고 있는 인증서의 관리를 보다 편안히 수행하고, 전체적인 인증서 관련 업무를 간소화시킬 수 있는 장점이 있다.

4.2.1 암호화 저장 모델

인증 시스템에서 전자서명 및 수신된 문서에 대한 암·복호화에 사용되는 개인키를 보관하는 것은 매우 중요한 문제이다. 개인키가 유출된다면 인증 시스템에 근본적인 신뢰도가 붕괴되므로 해당 인증서를 사용할 수 없으며, 추후 발생할 문제의 여지가 남아 있다. 본 논문에서는 개인키 보관에 대한 취약한 보안 강도를 높이기 위해, 최근에 가장 안전하다고 알려진 라이젠델 알고리즘을 이용하여 암·복호화를 수행하고, PKCS #5 v2.0 표준에 정의되어 있는 해쉬 알고리즘인 SHA-1을 이용하여 해쉬 값을 출력하게 된다. 이러한 개인키 저장 모듈을 구현한 모델은 그림 12와 같다.



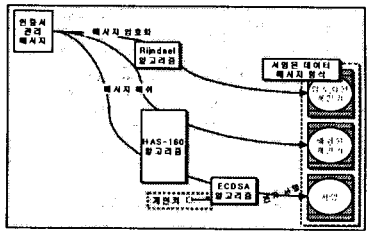
(그림 5) Rijadael을 이용한 개인키 저장

개인키를 전자서명 및 수신된 암호화 문서를 복호화 하는데 사용하기 위해서는 암호화되어 저장되어 있는 개인키를 복호화해서 사용한다. 개인키의 복호화는 암호화 모델의 역순으로 진행된다.

4.2.2 암호 메시지 교환 모델

그리드 CA 클라이언트와 그리드 CA가 공개된 네트워크 상에서 메시지를 교환하게 되면, 제 3자의 도청에 의한 메시지 유출 및 변경과 같은 보안 위협 요소에 당면하게 된다. 인증서와 관련된 메시지는 RFC 2511, RFC 2797과 PKCS #7 표준에 정의된 암호화된 메시지의 형식을 지녀, 안전한 메시지를 그리드 CA 클라이언트와 그리드 CA 사이에서 교환할 수 있다.

인증서 관리 메시지 암호화는 그리드 CA 클라이언트 또는 그리드 CA에서 생성하는 관리 메시지를 암호화하여 전송하는 과정을 포함한다. 그리드 CA 클라이언트 또는 그리드 CA에서 생성하는 메시지는 암호화된 메시지 부분과 서명 부분으로 구성된다. 그림 6은 다음에 기술한 메시지 암호화 과정을 거쳐 암호화된 메시지를 생성하는 과정을 보여준다.



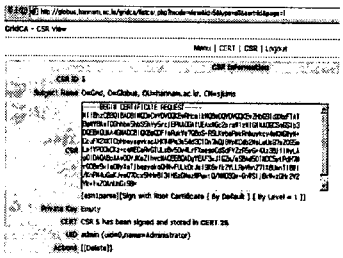
(그림 6) Rijadael을 적용한 인증서 관리 메시지 암호화

메시지 암호화 모델에서 Rijndael 알고리즘의 키 값은 커버러스 인증 과정을 거친 후 교환된 비밀키를 사용함으로써 안전한 채널에서 메시지를 교환할 수 있다. 또한 역순으로 복호화를 수행할 수 있다.

5. 사용자 등급기반의 보안 서비스 모델 구현

5.1 CA 클라이언트의 인가 서비스 구현

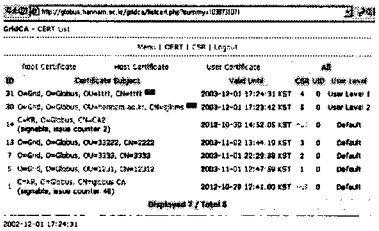
본 그리드 CA 보안 서비스 모듈의 구현 환경은 IBM 호환 PC를 사용하였으며, 운영체제로는 MicroSoft사의 Windows 2000 Professional과 Redhat사의 리눅스 커널 버전 2.4.18을 사용하였다. 또한, JDK1.3.1과 Kawa, JBuilder를 사용하여 사용자 인터페이스 및 인증 클라이언트인 그리드 CA 클라이언트 프로그램을 작성하였으며, 인증서 기반의 인가 시스템은 글로버스에서 제공하는 SimpleCA와 JSP(Java Serve Page)를 이용하여 프로그램을 작성하였다.



(그림 7) 새로운 인가 서비스를 적용한 인터페이스 화면

그림 15는 슈퍼컴퓨터연구실에서 개발·배포한 인증서 발급 시스템(GridCA V1.0)을 제안된 시스템에 맞게 변경한 화면이다. 위의 화면은 사용자의 인증서 발급 요청에 대하여 실제 인증서를 생성해주는 화면이며, 인증서 발급자(관리자)가 사용자의 인증서 요청을 확인한 후에 미리 정의한 정책에 따라 등급이 부여된 인증서를 사용자에게 발급할 수 있다.

본 논문에서 구현된 현재까지의 사용자 등급은 간단히 Default와 Level=1로 구분하고 있으나 이것은 인증서 발급 정책에 의해서 보다 세분화가 가능하다. 다음 그림 16은 수정된 인증서 발급 시스템을 통하여 등급을 부여하여 발급한 인증서들의 목록을 표시하는 화면이다. 인증서에 등급에 대한 확장 필드가 있다면 등급을 표시하며, 만일 정의하지 않았다면 Default로 표시하도록 구성되어져 있다.



(그림 8) 사용자 등급 부여 인증서 목록

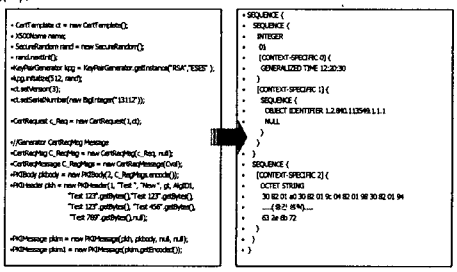
인증서 내에 추가된 사용자 등급 정보를 확인하기 위해서 openssl의 소스코드를 수정하여 policy라는 파라미터를 추가하였다. 이를 이용하여 다음과 같이 명령어 라인 상에서도 인증서내의 사용자 등급을 확인할 수 있다.

5.2 CA 클라이언트의 인증 서비스 구현

본 논문에서 구현된 인증서 기반의 인가 시스템과 그리드 CA 클라이언트의 핵심은 인증서 관리 프로토콜(Certificate Management Protocol ; CMP)을 준수하는 인증서의 관리 모듈, 개인키 저장 모듈, 그리고 안전한 메시지 교환을 위한 암호화 및 메시지 전송 모듈이다.

5.2.1 인증서 관리 클래스에 의한 ASN.1 모듈

그리드 CA 클라이언트에서 그리드 CA로 인증서 관리와 관련한 메시지를 전송하고, 이를 처리하기 위해서는 국제 표준규약에 맞추어진 인증서 요청 메시지 형식을 생성해야 한다. 그림 18은 클라이언트에서 초기 인증서를 요청하기 위한 ASN.1 구문으로, 클라이언트에서 전송되는 모든 메시지는 이와 같은 형태를 지니고 있다.



(그림 9) 인증서 요청 메시지의 ASN.1 형식

5.2.2 암호화 모듈

문서에 대한 서명 또는 수신된 문서를 복호화하기 위해서 사용되는 개인키는 안전하게 보관되어야 한다. 개인키의 저장은 일반적으로 안전한 이동 저장 매체 또는 디렉토리와 데이터베이스를 지정하여 저장하게 된다. 또한, 그리드 CA 클라이언트와 그리드 CA 사이에 교환되는 관리 메시지도 암호화되어 외부의 보안 위협으로부터 보호되어야 한다.

6. 비교분석 및 성능평가

본 논문에서는 공개키 기반의 인증서버 클라이언트는 네트워크 상에서 다양한 사용자의 신분을 인증하기 위한 시스템의 확장 시스템으로 현재까지 많은 업체에서 다양한 제품들이 개발되어 왔다.

본 논문에서 설계하고 구현한 그리드 CA 클라이언트는 기존의 상용화 업체에서 제공하는 클라이언트 시스템들과 같이 인증서를 관리하기 위한, 인증서 신청, 인증서 갱신, 인증서 검증, 개인키 저장 기능을 제공하며, 더불어 각 요청을 전달하는 메시지를 암호화하고 검증하는 모듈에 보안강도가 높은 타원곡선을 적용한 알고리즘을 적용함으로써 높은 보안 요구사항을 달성할 수 있다. 표 2는 본 논문에서 구현한 그리드 CA 클라이언트 시스템과 다른 상용제품의 클라이언트의 기능과 적용 알고리즘을 비교·분석하였다.

(표 1) 제안된 그리드 CA 클라이언트와 상용 소프트웨어와의 비교

비교대상 \ 제품군		제안된 시스템	B사	V사	E사	M대학
인증서 관리 기능	신청	제공함	제공함	제공함	제공함	제공하지 않음
	갱신	제공함	제공함	제공함	제공함	제공하지 않음
	검증	제공함	제공함	제공함	제공함	제공함
	보관	제공함	제공함	제공함	제공함	제공함
	열람	제공함	제공함	제공함	제공함	제공함
알고리즘	키 저장	Rijndael	3-DES	3-DES	3-DES	DES
	메시지 암호화	Rijndael	RSA	RSA	RSA	RSA
	메시지 해쉬	SHA-1	SHA-1	SHA-1	SHA-1	SHA-1
	메시지 서명	ECDSA	ECDSA	ECDSA	DSA	DSA

7. 결론 및 향후 연구

본 논문에서는 그리드 환경에서의 엔터티 상호 인증구조와 추가적으로 제안한 인증구조를 고찰하여, 향후 액티브 네트워크 상에서의 액티브 노드간의 상호인증구조를 구축하기 위한 초석을 다지고자 그리드의 보안 요구 사항과 인증과 권한 부여를 연구하고, 이를 바탕으로 그리드 보안에서 발생할 수 있는 인증 및 인가 서비스에 대한 문제를 해결할 수 있는 방안으로 공개키 인증시스템의 보안 기술 요소를 살펴보고, 이를 적용한 Grid CA 클라이언트를 설계하고, 구현하였다. 또한, 기존의 그리드 미들웨어인 글로버스의 인증 시스템에서 사용자의 권한을 부여해주는 모듈을 ID 기반에서 인증서 기반으로 확장함으로써 추후 발생할 수 있는 자원에 대한 권한 부여 문제를 해결하였다.

추후 연구과제는 CA 클라이언트를 바탕으로 추가적인 보안 모듈의 확장 및 기능 확장을 통하여, 액티브 네트워크 상에서 액티브 노드간의 상호인증에 활용 할 수 있는 통합 인증서 관리 도구를 개발하는 방안을 연구하는 것이다.

[참고문헌]

[1] IETF, "GSS-API EXtensions", Internet Draft, February 2002

[2] IETF, "Internet X.509 Public Key Infrastructure Proxy Certificate Profile", RFC 2459, August 2001

[3] IETF, "Internet X.509 Public Key Infrastructure Certificate Management Protocol", RFC 2510, March 1999

[4] Czajkowski, K., Fitzgerald, S., Foster, I. and Kesselman, C. "Grid Informat

[5] 윤찬현, 심은보, "그리드 구조 및 연구동향", 한국정보과학회지, 제 20권 제2호 pp.13, 2002.2

[6] 김학두, 김진석, "그리드 미들웨어 : 자원 관리 및 원격 데이터 접근 기술 동향", 한국정보과학회지, 제20권 제2호 pp.35~39, 2002.2

[7] http://www.kisa.or.kr/technology/sub1/current_bca.htm

[8] http://csrc.nist.gov/CryptoToolkit/aes/