제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

X.509 공개키 기반구조에서 Kerberos 인증에 관한 연구

김철현*, 김영자*
*홍성기능대학 전자계산기과
e-mail:kch7604@kopo.or.kr,

A study on an Efficient Kerberos Authentication based on X.509

Cheol-Hyun Kim*, Young-Ja Kim*
*Dept. of Computer Science, HongSeong Polytechnic College

요 약

본 논문에서는 IETF CAT Working Group에서 발표한 PKINIT기반의 인증서비스를 향상시킨 Kerberos 인증 메커니즘을 제안한다. PKINIT기반의 X.509, DS/DNS를 적용하여 영역간의 서비스를 제공하는 인증과 키 교환방식으로 DNS를 통해 외부영역의 위치를 탐색하고 X.509 디렉토리 인증 시스템을 적용, 영역간 인증은 DNS 서버로부터 공개키를 획득하여 다른 영역을 인증하도록 하였다. 영역간 인증과 키 교환은 Kerberos의 관용키 암호방식을 사용하고 세션 연결은 X.509 공개키 방식에 기반을 두고 있다. 효율적인 TGT(티켓승인 티켓) 교환과 통신상의 Overload를 감소시키는 효과와 인증절차의 간소화를 가지는 Kerberos시스템을 설계하였다.

1. 서론

분산 환경의 자원보호는 사용자와 서버간의 신원증명과 안전한 비밀키 교환을 필요로 하다. 신원증명과 비밀키 교환이라는 필요성을 만족시키기 위하여 인증, 무결성, 데이터 보안기능이 필요하다. 이러한 환경에서 대표적인 인증 메커니즘으로 Kerberos[1]와 Yaksha 인증방식[2]이 있으며 여러 응용시스템에 호환성을 갖도록 구성된 정보보호 하부구조로써 Kerberos 메커니즘을 확장한 SESAME이 있다. 본 논문에서는 네트웍 상에서 여러 문제점들을 해결할 수 있는 방안들 중 Kerberos 인증에 관해 중점적으로 연구하였다. Kerberos는 통신망 인증시스템의 개념과 모델로 중앙 집중식 인증서버를 제공하는 관용암호방식으로 개발되었다[3,4]. 네트웍 환경에서의 지역을 극복하기 위해 IETF(Internet Engineering Task Force) CAT에서 두 영역과 영역사이, 인증기관과 지역을 공개키로 상호 서비스해 주는 메커니즘으로 PKINIT(Public Key Cryptography for Initial Authentication)/PKCROSS(Public Key Cryptography for Cross-Realm Authentication)를 사용하고 있다[5,6]. PKINIT는 DES뿐 아니라 RSA 등 공개키 암호화와 X.509 인증서 기반구조의 Key 관리를 포함하며 Cross-Realm에 대한 인증으로 DNS[7]사용을 연급하고 있다[8]. 본 논문의 제안은 X.509와 PKCORSS/PKINIT에 기반을 둔 효율적인 Kerberos 인증서비스 교환을 위한 메커니즘을 설계하였다. 본 논문의 구성으로 2장에서 Kerberos 인증메커니즘을 설명하였고 3, 4장에서 효율적인 키 교환과 인증을 위한 메커니즘 설계와 분석을 통하여 제안하고 마지막 장에서 결론을 맺는다.

2. Kerberos 인증 메커니즘

Kerberos 인증 메커니즘[그림 1]은 여러 가지 요소로 구성된 복합시스템으로 Kerberos서버와 TGS, 티켓(Ticket), 인증자로 구성되어 있다. Kerberos 서버와 TGS가 티켓을 생성하여 TGS와 서비스 서버와의 통신에 사용되며 티켓의 구성정보는 서버와 클라이언트 이름, TimeStamp, 유효시간, 세션키를 포함한다. 인증자는 클라이언트에 의해 생성되고 생성된 인증자는 사용을 1회로 제한하고 있으며 인증정보는 클라이언트의 이름과 웍스테이션의 IP 주소, 현재의 시간을 포함하고 있다[9,10].

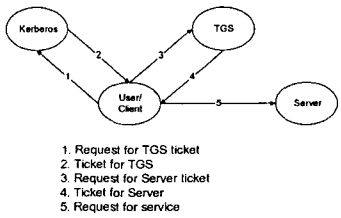

그림 1. Kerberos 인증메커니즘

3. 효율적인 Kerberos 인증 메커니즘 설계

3.1 IETF의 Kerberos 인증 메커니즘

IETF의 Kerberos인증 메커니즘에서는 티켓을 발급 받기 위해 원격 Kerberos가 지역 클라이언트를 확인하는 과정을 갖는다. 지역 Kerberos를 통하여 TGS(Ticket Granting Server)를 접근할 수 있는 티켓과 원격 TGS가 서버에 접근할 수 있는 티켓인 SGT(Server Granting Ticket)을 발급하는 과정의 메커니즘으로 구성되어 있다.

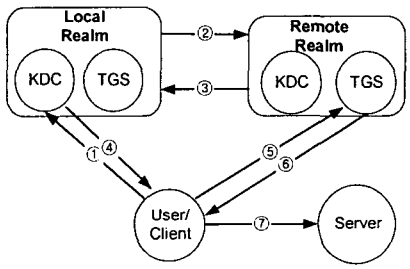

그림 2. IETF의 인증 메커니즘

[그림 2]는 IETF의 영역간 Kerberos 인증절차로써 상호간 인증서와 암호알고리즘 등 인증서비스를 교환하고 원격 TGS 접근을 위한 티켓과 세션키를 교환하는 TGT 서비스 교환(①-④), 서버 접근용 티켓과 세션키를 교환하는 TGS 교환(⑤-⑥), 세션키에 의한 서비스 요청과정(⑦)으로 원격 KDC가 지역 KDC의 정보를 인증한 후 티켓을 발급하고 있다.

3.2 디렉토리 시스템(Directory System)

모든 Kerberos의 공개키는 디렉토리시스템에서 획득하게 된다. 저장되는 KDC의 공개키는 디렉토리시스템에 의해 데이터 무결성과 데이터의 인증을 보장받는다. 이 공개키 인증서는 PKCROSS/PKINIT에 의한 초기 인증을 목적으로 원격 KDC의 공개키를 획득하기 위해 디렉토리시스템을 이용한다. 디렉토리 서비스는 데이터베이스, 파일, 호스트 연결, 사용자 서비스 등 모든 자원에 대한 관리를 허용하고 위치 서비스로써 인터넷 DNS[11]을 사용하여 여러 도메인을 트리구조로 연결시킨다[12,13]. 지역 Kerberos는 지역 클라이언트가 요청한 영역이 동일영역이 아닐 경우에는 DNS를 사용하여 외부 영역의 경로를 찾는다. 디렉토리 서버는 클라이언트들에게 인증서를 획득하는데 쉽게 접근할 수 있는 경로만을 제공하며, 인증과 키 교환을 위한 디렉토리 시스템의 구조는 [그림 3]와 같다. 구성은 DNS와 디렉토리 서비스에 접근하기 위한 인터넷 표준(RFC1777) 프로토콜인 LDAP, 인증과 키 교환을 실현할 Kerberos, Database로 되어있다.

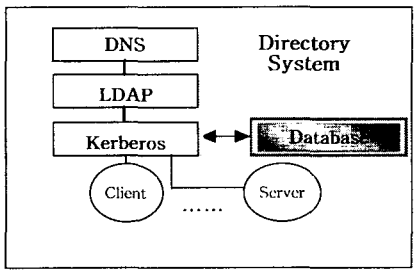

그림 3. 디렉토리 서비스의 구조

[그림 4]은 디렉토리를 인증하기 위해 X.500의 디렉토리 시스템을 이용하여 외부영역에 있는 목적지까지 경로를 연결하는 세션과정을 도식한 것이다. 여기에서 X.500의 디렉토리 시스템의 형식은 Domain, X500, Other 그리고 Reserved로 구성된다.

Domain	: host.subdomain.domain
X500	: C=US/O=OSF
Other	: NameType
Reserved	: reserved

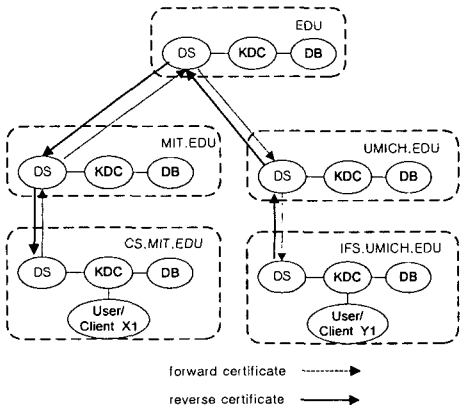

그림 4. 디렉토리 서버인증

문제는 침해자가 서비스를 요청한 클라이언트처럼 가장하여 서비스를 가로채거나 변경시킬 수 있기 때문에 상호 영역간에 있어서 클라이언트를 인증하는 절차를 필요로 하게 된다. 클라이언트는 원격 Kerberos에게 X.509[14]를

이용하여 얻은 원격 영역의 공개키로 정보를 암호화하여 전송함으로써 클라이언트와 원격 영역간의 통신을 방해하는 침입자로부터 보호할 수 있게 한다[15]. 디렉토리 시스템이 진·후방 인증서를 통하여 체인으로 연결되면 KDC는 Kerberos Ticket을 발행한다. KDC는 하나의 Master와 여러 개의 Slave로 구성되며 각각Kerberos 데이터베이스를 보유한다. Slave KDC는 데이터베이스의 복사본들을 유지하며 데이터베이스의 추가나 변경 삭제 등은 Master KDC에서만 가능하다.

```
AHTENA.MIT.EDU = {
database-name = /usr/local/var/krb5kdc/principal
admin_keytab = /usr/local/var/krb5kdc/kadm5.keytab
        }
key_stash_file= /usr/local/var/krb5kdc/.k5.ahtena.mit.edu
kadmin_port = 749
max_life = 10h 0m 0s
max_renewable_life = 7d 0h 0m 0s
master_key_type = des-cbc-crc
supported_enctypes = des-cbc-crc:normal
                    }
```

그림 5. Kerberos의 도메인영역

즉 Salve KDC는 Ticket만을 발급해 주는 역할만 하고 경로를 설정하는 것은 Master KDC의 역할이다. [그림 5]은 루트 도메인 EDU와 최상위 도메인 MIT, 그리고 서브 도메인 AHTENA를 갖는 도메인 이름구조를 AHTENA.MIT.EDU라는 [Realms]에 생성하고 데이터베이스에 저장한다.

3.3 승인 티켓을 위한 인증 서비스 교환 메커니즘

Client가 요청한 서비스가 동일한 영역 내에 있는 서비스이면 KDC의 데이터베이스에서 Client의 정보로 인증을 하게 되고 요청한 서비스가 동일 영역 내에 존재하지 않으면 KDC는 Client가 요청한 영역이 어디에 존재하는지 디렉토리시스템을 통하여 DNS에게 검색을 의뢰한다. DNS 서버는 정방향 조회영역, 캐쉬 루트서버를 이용하여 리졸빙 후 캐쉬영역에 저장 한 후 KDC로부터 의뢰를 받은 영역을 검색한 후에 이웃(Pre-authentication)하는 영역을 디렉토리시스템에게 전송한다. 클라이언트는 원격 Kerberos에게 X.509를 이용하여 획득한 원격 영역의 공개키로 정보를 암호화하여 전송함으로써 클라이언트와 원격 영역간의 통신을 방해하는 제3자로부터 보호할 수 있게 한다.

[그림 6]은 서로 다른 영역의 Local Realm(MIT.EDU)과 Remote Realm(IFS.UMICH.EDU)의 환경으로 KDC는 TGS가 사용할 티켓($Ticket_{TGSREM}$) 만을 발급하는 역할을 하며 티켓에는 발급자, 세션키, 발급대상의 ID와 주소, 발행시간, Reply 방지용 값을 포함한다. TGS는 SGT인 $Ticket_{SGTREM}$를 발급하는 서비스를 담당한다.

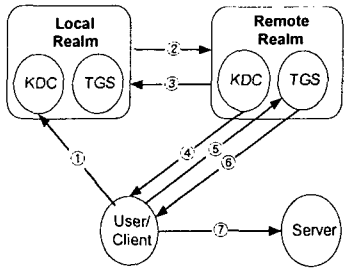

그림 6. 승인 티켓을 위한 메커니즘

Kerberos는 인증과 KDC의 역할을 하며 Local Client가 Remote Server의 서비스를 받기 위한 메시지 교환 내용은 다음과 같다.

(1) 인증 서비스

① ID_C, $Realm_S$

② E_{KDC_rPK}[SignedAuthPack, TrustedCertifiers, CertPath]

③ E_{KDC_lPK}[KDC_r 《KDC_l》 ,KDC_r 《C》]

(2) TGT 서비스

④ E_{PKC}[$Ticket_{TGSREM}$, $K_{C.TGSREM}$, TimeStamp, Nonce, $Realm_{TGSREM}$,

E_{KDC_rSK}[$Ticket_{TGSREM}$, TimeStamp, PaChecksum, Nonce, $Realm_{TGSREM}$]]

$Ticket_{TGSREM}$ = EK_{TGSREM}[flags, $K_{C.TGSREM}$, ID_C, AD_C, TimeStamp, Nonce]

(3) SGT 서비스

⑤ $EK_{C.TGSREM}$[ID_S, A_C, $Ticket_{TGSREM}$,

E_{KDC_rSK}[$Ticket_{TGSREM}$, TimeStamp, PaChecksum, Nonce, $Realm_{TGSREM}$]]

⑥ $E_{KC.TGSREM}$[$K_{C.SGTREM}$, $Ticket_{SGTREM}$, TimeStamp, Nonce, $Realm_{SGTREM}$, ID_S,

EK_{SGTREM}[$K_{C.SGTREM}$, ID_C, AD_C, ID_S, TimeStamp, nonce]]

A_C = $EK_{C.TGSREM}$[ID_C, AD_C, $Realm_{TGSREM}$, TimeStamp, Nonce]

$Ticket_{SGTREM}$ = EK_{SGTREM}[flags, $K_{C.SGTREM}$, $Realm_{SGTREM}$, ID_C, AD_C, TimeStamp, Nonce]

(4) 서비스 요청

⑦ $EK_{C.SGTREM}$[$Ticket_{SGTREM}$, Ac, EK_{SGTREM}[$K_{C.SGTREM}$, ID_C, AD_C, ID_S, Nonce]]

A_C = $EK_{C.TGSREM}$[ID_C, AD_C, $Realm_{TGSREM}$, TimeStamp, Nonce]

$Ticket_{SGTREM}$ = EK_{SGTREM}[flags, $K_{C.SGTREM}$, $Realm_{SGTREM}$, ID_C, AD_C, TimeStamp, Nonce]

4. 메커니즘 분석 및 효과

IETF CAT Working Group에서 사용하고 있는 Kerberos 메커니즘은 PKINIT의 기반의 PKIX로 공개키와 공통키를 사용하여 인증정보에 대한 무결성을 보장하고 있으나 도메인간 연결정보에 대해서는 DNS방법을 언급만 하고 있다. 본 논문에서 제시된 알고리즘은 Kerberos을 기반으로 IETF Working Group에서 사용하고 있는 PKCROSS/PKINIT 메커니즘이며, Kerberos와 X.509에서 보장해 주는 안전성과 DS/DNS에 의한 경로에 대하여 인증서 체인(*CertPath : Domain Value*)으로 보관하기 때문에 원격 Kerberos에서 Client로 TGT를 직접 전송할 수 있다. 즉 Client는 KDC_r에 TGT를 획득하기 위한 별도의 요청을 필요로 하지 않는다. 서버용 티켓은 TGS의 키로 암호화(K_{TGSREM})되어 있으므로 변조가 불가능할 뿐만 아니라 Client의 공개키로 재 암호화하므로 제 3자가 티켓을 이용할 수 없다. 티켓 내에도 Client와 TGS_{REM}, Client와 서버사이의 세션키($K_{C,TGSREM}$, $K_{C,SGTREM}$)를 포함시킴으로써 티켓 소유자가 정당한 사용자임을 증명한다.

본 논문에서 제시된 알고리즘은 원거리 통신에서의 보안성을 보장하기 위해서 인증정보를 전달할 때 Kerberos의 비밀키와 PKCROSS/PKINIT를 이용한 공개키를 사용하였고 상호인증을 위해 X.509와 디렉토리시스템을 이용한 체인방식으로 원거리 통신을 보다 더 안전성이 보장되는 Kerberos시스템을 설계하였다.

5. 결 론

정보보호 기반기술의 중요요소인 인증 메커니즘으로 관용 암호방식을 사용하는 Kerberos는 동일영역에서 최적의 상호인증 알고리즘이다. 분산 네트워환경에서 통신하고자 하는 다수의 윅스테이션들과 응용서버의 인증을 위해서 Kerberos는 X.509 공개키 기반구조를 갖는 PKINIT를 통해 공개키와 비밀키를 제공하여 안전한 서비스를 지원한다. 본 논문에서는 인증 메커니즘인 Kerberos와 초기 인증과정에서 공개키 암호 사용에 대한 정의를 기술한 PKINIT/PKCROSS와 PKIX의 인증시스템인 X.509를 고찰하였다. 경로(CertPath)는 DNS를 통해 외부영역의 위치를 탐색하여 데이터베이스에 저장하고 공개키 획득은 X.509 디렉토리 인증 시스템인 디렉토리시스템을 적용하였으며 영역간 체인을 통하여 다른 영역을 인증하도록 하였다. Local Kerberos를 경유하지 않고 Client로 직접 티켓을 전송함으로써 통신상의 Overload를 감소시키는 효과와 인증절차의 간소화를 가지는 Kerberos 시스템을 설계하였다.

참고 문헌

[1]B.C.Neuman, Theodore Ts'o. Kerberos,"An Authentication Service for computer Networks", IEEE Communications, 32(9):33-38.September 1994.

[2]J. G. Steiner, B. C. Neuman, and J. I. Schiller, " Kerberos: An Authentication Service for Open Network System," pp. 191-202 in Usenix Conference Proceedings, Dallas, texas (Feb, 1988)

[3]최용락, 소우영, 이재광, 이임영 "통신망 정보보호", 그린출판사, pp.343-393, 2001.

[4]B.Tung,C.Neuman, M. Hur, A. Medvinsky, S. Medvinsky, J. Wray, J. Trostle, "Public Key Cryptography for Initial Authentication in Kerberos". draft-ietf-cat-kerberos-pk-init-15.txt

[5]http://www.ietf.org/internetdraft-ietf-dnsop/keyhand-00.txt, IETF, 1999.

[6]B. Tung, B.C. Neuman, M. Hur, A. Medvinsky, S. Medvinsky "Public Key Cryptography for Cross-Realm Authentication in Kerberos". draft-ietf-cat-kerberos-pk-cross-08.txt

[7]K. Hornstein, J.Altman,"Distributing Kerberos KDC and Realm Information with DNS".draft-ietf-krb-wg-krb-dns-locate-02.txt

[8]J. Kohl, C. Neuman, "The Kerberos Network Authentication Service (V5)", draft-ietf-cat-kerberos-revisions-10.txt

[9]M. Hur, J. Salowey, " Kerberos Cipher Suites in Transport Layer Security (TLS)", draft-ietf-tls-kerb-01.txt

[10]A. Medvinsky, M. Hur, S. Medvinsky, C. Neuman. "Public Key Utilizing Tickets for Application Servers (PKTAPP)".

[11]K. Hornstein, J.Altman,"Distributing Kerberos KDC and Realm Information with DNS".draft-ietf-krb-wg-krb-dns-locate-02.txt

[12]A. Gulbrandsen, P. Vixie, " A DNS RR for specifying the location of services (DNS SRV)", RFC2052, October 1996.

[13]P. Mockapetris, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION",RFC1035, November 1987.

[14]IETF Draft, "Internet X.509 Public Key Infrastructure Certificate and CRL profile," 1998

[15]K. Raeburn,"Encryption and Checksum Specifications for Kerberos 5", draft-ietf-krb-wg-crypto-00.txt