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

요약
본 논문에서는 IETF CAT Working Group에서 발표한 PKINIT 기반의 인증서비스를 향상시킨 Kerberos 인증 메커니즘을 제안한다. PKINIT 기반의 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(티켓증명 티켓) 교환과 통상상의 Overload을 감소시키는 효과와 인증 전차의 간소화를 가지는 Kerberos시스템을 설계하였다.

1. 서론
본 논문에서는 IETF CAT Working Group에서 발표한 PKINIT 기반의 인증서비스를 향상시킨 Kerberos 인증 메커니즘을 제안한다. PKINIT 기반의 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(티켓증명 티켓) 교환과 통상상의 Overload을 감소시키는 효과와 인증 전차의 간소화를 가지는 Kerberos시스템을 설계하였다.

2. Kerberos 인증 메커니즘
Kerberos 인증 메커니즘은 여러 가지 요소로 구성된 복합시스템으로 Kerberos 서버와 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 티켓이의 IP 주소, 현재의 시간을 포함하고 있다.

3. 효율적인 Kerberos 인증 메커니즘 설계

3.1 IETF의 Kerberos 인증 메커니즘

IETF의 Kerberos 인증 메커니즘에서는 티켓을 발급 받기 위해 원격 Kerberos가 지정 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)를 발급하는 과정의 메커니즘으로 구성되어 있다.

그림 2. IETF의 인증 메커니즘

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

3.2 딥렉토리 시스템(Directory System)

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

[그림 4]는 딥렉토리를 인증하기 위해 X.500의 딥렉토리 시스템을 이용하여 외부영역에 있는 목적지까지 경로를 연결하는 세션과정을 도식한 것이다. 여기에서 X.500의 딥렉토리 시스템의 형식은 Domain, X500, Other 그리고 Reserved로 구성된다.
3.3 승인 티켓을 위한 인증 서비스 교환 메커니즘

Client가 요청한 서비스가 동일한 영역 내에 있는 서비스이면 KDC의 메시지에서 Client의 정보로 인증을 하게 되고 요청한 서비스가 동일 영역 내에 존재하지 않으면 KDC는 Client가 요청한 영역에 액세스하여 다플레이스시스템을 통하여 DNS에게 검색을 의뢰한다. DNS 서비스는 정상적으로 회의영역, 캐시 무단사용을 이용하여 리솔루션 후 캐시영역에 저장한 후 KDC로부터 엑셀이 받은 영역을 검색한 후에 이웃(Pre-authentication)하는 영역을 다플레이스시스템에 전송한다. 클라이언트는 원격 Kerberos에게 X.509를 이용하여 획득한 원격 영역의 공개키로 정보를 암호하여 전송함으로써 클라이언트와 원격 영역간의 통신을 방해하는 3차로부터 보호할 수 있게 한다.

[그림 6]은 서로 다른 영역의 Local Realm(MIT.EDU)과 Remote Realm(IFS.UMICH.EDU)의 환경으로 KDC는 TGS가 사용한 티켓(TicketGSREx)이 받을 유지하는 역할을 하며 티켓에는 발급자, 세션키, 발급대상의 ID와 주소, 발행시간, Reply 받기용 값을 포함한다. TGS는 SGT인 TicketSGREx를 발급하는 서비스를 담당한다.

(2) TGT 서비스
④ EKc.TGSREx(TicketGSREx, KC.TGSREx, TimeStamp, None, Realm.TGSREx)

TicketGSREx = EKc.TGSREx[flags, KC.TGSREx, IDc, Adc, TimeStamp, None]

(3) SGT 서비스
⑤ EKc.SGTREx(IDs, Ac, TicketGSREx)

Exk.SGTREx(TicketGSREx, TimeStamp, PaChecksum, None, Realm.TGSREx)

⑥ EKc.TGTREx(Kc.SGtrex, TicketsGTREx, TimeStamp, None, Realm.TGTREx, IDs, EKc.TGTREx[Kc.SGtrex, IDc, Adc, IDs, TimeStamp, None]

Ac = EKc.TGTREx[IDc, Adc, Realm.TGTREx, TimeStamp, None]

TicketsGTREx = EKc.TGTREx[flags, KC.SGtrex, Realm.TGTREx, IDc, Adc, TimeStamp, None]

(4) 서비스 요청
⑦ EKc.SGTREx(TicketSGREx, Ac, EKc.SGTREx[Kc.SGtrex, IDc, Adc, IDs, None])

Ac = EKc.TGTREx[IDc, Adc, Realm.TGTREx, TimeStamp, None]

TicketsGTREx = EKc.TGTREx[flags, KC.SGtrex, Realm.TGTREx, IDc, Adc, TimeStamp, None]
4. 메커니즘 분석 및 효과

IETF CAT Working Group에서 사용하고 있는 Kerberos 메커니즘은 PKINIT의 기반인 PKIX의 공통적인 메커니즘을 사용하여 인증정보에 대한 무결성을 보장하고 있으나, 도메인간 연결정보에 대해서는 DNS패턴을 기반으로 하고 있다. 본 논문에서 제시한 알고리즘은 Kerberos를 기반으로 IETF Working Group에서 사용하고 있는 PKCROSS/PKINIT 메커니즘이다. Kerberos와 X.509에서 보장해 주는 안전성과 DS/DNS에 의한 경로에 대하여 인 증서 체인(CertPath : Domain Value)으로 보관하기 때문 에 원격 Kerberos에서 Client로 TGT를 직접 전송할 수 있다. 즉 Client는 KDC로 TGT를 획득하기 위한 별도 의 요청을 필요로 하지 않는다. 서비스 터켓은 TGS의 키 로 암호화(KgsBrem)되어 있으므로 변조가 불가능한 뿐만 아니라 Client의 공개키로 해 암호화하기로 제 3자가 터켓 을 이용할 수 없다. 터켓 내에도 Client와 TGSBrem, Client와 서버사이의 세션키(KcTgsBrem, KcSgBrem)를 포함 심시에 서비스가 정상적인 사용자를 인증한다.

본 논문에서 제시한 알고리즘은 원거리 통신에서의 보안 성을 보장하기 위해서 인증정보를 전달할 때 Kerberos의 비밀키와 PKCROSS/PKINIT을 이용한 공개키를 사용하였고 상호인증을 위해 X.509에 디렉토리시스템을 이용한 정인방식으로 원거리 통신을 보다 안전성이 보장되는 Kerberos시스템을 설계하였다.

5. 결 론

정보보호 기반기술의 중요성에 인증 메커니즘과 만 둔 암호방식을 사용하는 Kerberos는 정보보안에서 최적의 상호인증 알고리즘으로 분산 네트워크에서 통신하고자 하는 다수의 네트워크시스템과 사용자의 인증은 위해서 Kerberos는 X.509 공개키 기반구조를 갖는 PKINIT을 통해 공개키와 비밀키를 제공하여 안전한 서비스를 지원한다. 본 논문에서는 인증 메커니즘이 Kerberos와 초기 인 증과정에서 공개키 암호 사용에 대한 정의를 기술한 PKINIT/PKCRASS와 PKIX의 인증시스템인 X.509를 고 찰하였다. 경로(CertPath)는 DNS를 통해 외부영역의 위치를 탐색하여 데이터베이스에 저장한 공개키 허득은 X.509 디렉토리 인증 시스템인 디렉토리시스템을 사용하였으며 엉망한 체인을 통해 나온 엉망을 인증하도록 하였다. Local Kerberos를 겪지 않게 Client로 직접 터켓을 전송함으로써 통신상의 Overload를 감소시키는 효과와 인증절차의 간소화를 가져오는 Kerberos 시스템을 설계하였다.

참고 문헌