論文
2-12-6

PKINIT기반의 향상된 Kerberos 인증에 관한 연구 (A study on advanced Kerberos Authentication between Realms based on PKINIT)

신 광 철* 정 진 욱**
(Kwang-Cheul Shin) (Jin-Wook Chung)

요 약

본 논문에서는 IETF CAT Working Group에서 발표한 PKINIT 기반의 인증서비스를 향상시킨 Kerberos 인증 메커니즘을 제안한다. 서비스를 위한 상호 영역간 인증은 X.509와 DS/DNS를 이용하는 PKINIT를 통한 체인에 의해서 연결하였다. 영역간 서비스를 위해 공통키와 공개키를 사용하며 실제적인 인증은 Kerberos의 공통키에 두고 PKINIT의 X.509는 공개키를 이용하여 세션을 설정하였다. 새로운 메커니즘은 원격영역에서 티켓을 얻기 위하여 KDC의 인증서 사용으로 Client와 원격 KDC간 인증절차를 간소화시킴으로써 통신부담을 줄이고 원격 KDC의 재확인 과정이 생략되었다.

ABSTRACT

In this paper, We propose a new Kerberos certification mechanism that improve certification service based on PKINIT that announce in IETF CAT Working Group. Certification between area connected by chain through PKINIT that use X.509 and DS/DNS mutually for service. In order to provide regional services used private key and public key, X.509 of PKINIT is employed on session part and Kerberos's private key on actual authentication part. New mechanism be reduced communication overload doing to simplify certification formality between Client and remote KDC by KDC's certificate use to get ticket in remote sacred ground and remote KDC's reaffirmation process omitted.

1. 서 론

분산 개방형 시스템인 네트워크 상에서 자원을 가진 많은 컴퓨터(Server)들과 이들 자원을 이용하는 다수의 사용자(Client)들 간에 허락된 사용자만이 자원에 접근하도록 하는 과정과 그룹에서의 외부에 의한 공격뿐만이 아니라 내부 사용자의 공격에 대한 대책이 필요하다. 이 두 가지의 필요성을 만족시키기 위하여 인증(Authentication), 무결성(Identify), 데이터보안(Privacy)를 제공하면서 키 분배 센터(KDC: Key Distribution Center)의 개념을 갖는 메커니즘이 Kerberos이다[1]. IETF(Internet Engineering Task Force) CAT에서 두 영역과 영역사이, 인증기관과 지역을 공개키로 상호 서비스해 주는 메커니즘으로 PKINIT(Public Key Cryptography for Initial Authentication)를 사용하고 있다[2].

Kerberos에서 사용되는 인증서 X.509는 상호인증과 접근제한을 위한 공개키의 암호화와 디지털 서명에 기반을 두고 있으며 디렉토리 서비스를 정의하는 X.500 서비스 권고 안의 일부분으로 사용자에게 디렉토리 인증을 정의하고 있다[3]. IETF의 PKINIT를 이용한 Kerberos 인증 메커니즘에서는 티켓을 얻기 위한 티켓 승인 서비스단계로서 원격 Kerberos가 지역 클라이언트

* 정회원 : 벽성대학 소프트웨어개발전공 교수
** 정회원 : 성균관대학교 전기전자 및 컴퓨터공학부 교수

논문접수 : 2001. 12. 10.
심사완료 : 2001. 12. 15.

에게 티켓발급서버(Ticket Granting Server:이하 TGS)를 접근할 수 있는 티켓과 임의의 난수(Krand)를 전송하여 원격 Kerberos가 지역 클라이언트를 재확인하는 9단계의 메커니즘으로 구성되어 있다[4]. 본 논문에서는 PKINIT 인증 알고리즘을 적용하고 KDC의 인증서(TrustedCertifiers)를 사용함으로써 Client와 원격 KDC간 상호인증절차를 생략하였다. 지역Kerberos와 원격 Kerberos의 상호인증을 위해 DS(Directory server)/DNS (Domain Name Server)를 사용하여 전·후방 선인증(Pre-authentication) 체인으로 연결, 상호인증을 함으로써 7단계의 메커니즘으로 개선하여 설계하였다.

2. Kerberos와 X.509 디렉토리 인증

Kerberos는 여러 가지 요소로 구성된 복합시스템으로 Kerberos 서버와 티켓승인서버(TGS), 티켓(Ticket), 인증자(Authenticator)로 구성되어 있으며 Kerberos 서버와 TGS가 티켓을 생성하여 TGS와 서비스 서버와의 통신에 사용되며 티켓의 구성정보는 서버와 클라이언트 이름, 티켓생성 시간, 유효시간, 세션키를 포함한다. 인증자는 클라이언트에 의해 생성되고 생성된 인증자는 한번만 사용할 수 있으며 인증정보는 클라이언트의 이름과 워스테이션의 IP 주소, 현재의 시간을 포함하고 있다[5].

버전(Ver)4에서 KDC는 모든 사용자의 ID 및 패스워드를 보유하는 DB와 인증서버(AS :Authentication Server)를 사용하며 각 응용서버와 고유의 비밀키를 물리적으로 안전하게 분배하여 공유하도록 설계되었다. Client가 서버접근 티켓을 요청하기 위해 로그인하고 서버 V에 접속하기 위한 요구정보(IDC, PC, IDV)을 전송하여 AS에 의해 인증이 되면 Ticket를 생성하여 Client에게 보냄으로써 서버에게 Client가 허가를 받았다는 사실을 확인시켜야 한다. 문제는 패스워드가 평문으로 전송되며 서버에 접근이 필요할 때마다 티켓을 발급받기 위해 패스워드를 입력해야 하는데 이러한 문제를 해결하기 위하여 AS와 함께 티켓-승인서버(TGS)를 사용한다. 사용자는 티켓을 보관하여 서비스에 접속할 때마다 이 티켓을 이용하여 TGS에게 접속한다. AS는 자신의 DB에 저장되어 있는 Client의 패스워드로 암호키(KC)를 생성하여 티켓을 발급한다. 패스워드의 입력 시기는 Ticket이 도착한 후에 자신의 패스워드를 입력하여 키를 생성하고 티켓을 복호화한다. 또한 티켓의 가로채기를 부인하기 위해 티켓이 발행된 시간과 유효시간을 포함하고 있다. 문제는 티켓-승인 티켓과 관련된 유효시간의 문제로 어떤 네트웍 서비스(TGS 또는 응용서버)는 티켓을 사용하고 있는 사람이 티켓이 발행된 사람과 같다는 것을 증명할 수 있어야 한다. AS가 C와 TGS간, C와 서버 V간에 세션키(KC,TGS , KC,V)를 제공하여 신원을 확인시켜 주고 유효시간(Lifetime)을 짧게 인증자(Authenticatorc)에게 두어 가로채기의 위험을 방지하고 있다.

Ver 5[그림 1]에서 Ver 4와 다른 점은 realm(영역), Options(플래그 값), Times(티켓에 시간설정), Nonce(Replay를 방지)가 추가되었고 Subkey와 Seq#는 실제 통신상에서 별도의 세션키로 사용하고 메시지에 순서를 부여하여 재전송이 아님을 보증하도록 한다.

Version	Client	Kerberos		Server	표 기
		AS	TGS		
V5	① ● ····▶ ● Options, RealmC, IDC, ID_{TGS}, Times, Nonce1, AD_C ② ● ◀···· ● $Realm_C$, ID_C, $Ticket_{TGS}$, $E_{Kc}[K_{C,TGS}$, nonce1, Flag, Times1, $Realm_{TGS}$, ID_{TGS}, $AD_C]$ ③ ● ····▶ ● options, ID_V, Times2, nonce2, $Ticket_{TGS}$, $Authenticator_C$ ④ ● ◀···· ● $Realm_C$, ID_C, $Ticket_V$, $EK_{C,TGS}[K_{C,V}$, nonce2, Flag, Times2, $Realm_V$, ID_V, $AD_C]$ ⑤ ● ···· options, $Ticket_V$, $Authenticator_C$ ····▶ ● ⑥ ● ◀···· $EK_{C,V}$[TS2, Subkey, Seq#] ···· ●			$Ticket_{TGS}=EK_{TGS}$[Flag, $K_{C,TGS}$, $Realm_C$, ID_C, Times1, AD_C] $Ticket_V=EK_V$[Flag , $K_{C,V}$, $Realm_C$, ID_C, Times2, AD_C] $Authenticator_C=EK_{C,V}$[ID_C, $Realm_C$, TS2, Subkey, seq#]

[그림 1] 커버러스 V5

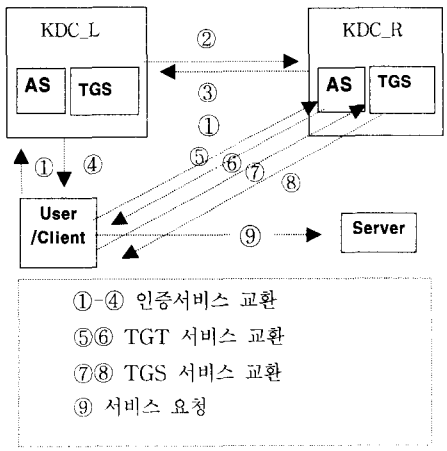
[Fig. 1] Kerberos V5

또한 Ticket에 대한 이중암호화가 제거되었고 임의 암호형식을 사용할 수 있으며 여러 영역간에 상호동작을 가능하도록 확장성을 더욱 용이하게 개선되었다[6]. X.509는 디렉토리 서비스를 구성하는 X.500계열의 일부로 사용자들에 대한 정보를 담고 있는 일종의 서버인 X.500 디렉토리를 통해서 제공되는 인증서비스의 구성을 명시하고 있으며 PKI(Public Key Infrastructure) 구조를 제공한다[7]. X.500 디렉토리는 DIT (Directory Information Tree)로 구성되며 각 엔트리는 유일한 이름(DN : Distinguished Name)을 가진다. Root를 정점으로 각 국가를 나타내는 RDN(: Relative Distinguished Name)이 할당되고 각 조직들은 그에 속한 모든 엔트리를 구성한다. X.509 인증서는 인증서 취소목록(CRL : Certificate Revocation List)과 인증서를 정의하는 다양한 환경에 맞는 조건과 서명 알고리즘의 선택이 가능하도록 확장영역이 추가되었다. 본 논문에서 디렉토리 인증 프로토콜인 X.509를 이용하며 연결, 외부 영역에 있는 서비스를 얻는다. 디렉토리 서버는 클라이언트들에게 인증서를 획득하는데 쉽게 접근할 수 있는 경로를 제공하며 DNS와 X.500을 기반으로 도메인을 갖는 한 단위조직의 검색엔진이면서 통합저장소이다. 또한 영역 내의 객체에 대한 속성을 가지며 Kerberos 내의 위치정보를 DNS, SRV(Service Resource Records), RR[RFC2052]를 사용하여 저장한다.[8] DNS는 호스트명과 IP 어드레스를 서로 매핑시키고 E-mail의 라우팅 정보를 제공하기 위하여 TCP/IP 어플리케이션에 의해 사용되는 기반 서비스이자 프로토콜로 호스트 이름에 대한 분산된 데이터베이스라고 할 수 있다. 즉 계층적 이름을 인터넷의 주소로 또는 그 반대로 변환하는 것을 의미한다[9].

3. 영역간 새로운 Kerberos 인증 메커니즘 설계

3.1 개요

본 논문에서 제시한 인증 메커니즘은 영역(Realm)과 영역간 서비스를 위한 인증으로 기본 환경은 KDC(AS)와 티켓을 발행하는 TGS, 영역 내 객체의 위치를 제공하기 위해 DNS를 사용하기 위한 디렉토리 서버(DS), 비밀키의 생성 및 분배를 위한 키 관리센터(KMC), End User의 ID와 패스워드를 저장한 중앙DB, 자원서비스를 위한 서버, 서버를 사용할 Client가 하나의 도메인으로 구성되어 있다. 인증서는 인증기관(CA)이 전자서명을 통하여 전자서명 공개키와 이를 소유하는 자연인 또는 법인과의 귀속관계를 확인, 증명하는 전자적 정보로써 본 논문에서는 Kerberos의 KDC(AS)가 인증기관의 역할과 키분배 센터의 역할을 담당하며 상호 신뢰성을 확인하는데 사용한다. 각 영역의 Client와 자원(Server)들은 KDC(AS)에게 ID와 패스워드를 Install 때 등록하여 AS의 데이터베이스에 저장되며 이는 동일영역에서의 인증을 위해 사용하고 영역간에는 KDC가 Client를 인증하고 KDCLOC가 인증서(KDCLOC≪C≫)를 발행하여 Client를 보증해 준다. 다수의 워스테이션들이 서비스를 받기 위해서는 티켓발급 서버(TGS)로부터 받은 티켓을 사용하여 서버에게 인증 받는다. 이 티켓은 그 사용시간이 서비스의 종류나 클라이언트의 권한에 따라 제한되어 있으며 티켓을 사용하는 클라이언트의 신분을 증명해 주기 위해 여러 가지 인증정보를 포함하고 있다. Kerberos의 보안정도는 티켓발급서버가 얼마나 확실하게 보호되는지에 달려있으며 Kerberos를 사용하는 서버와 클라이언트들은 티켓발급서버를 신뢰함을 전제로 한다. 본 논문에서는 IETF Draft에서 제시한 PKINIT 기반의 Kerberos 인증 프로토콜에 인증정보를 추가하여 영역간 새로운 Kerberos 인증프로토콜을 제시한다.



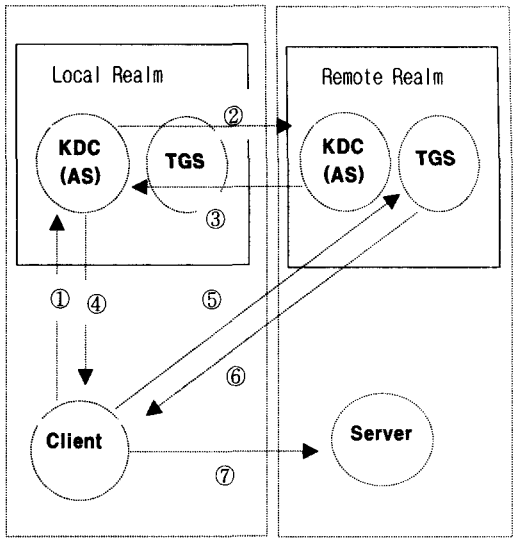
[그림 2] IETF의 인증 메커니즘

[Fig. 2] Authentication mechanism

[그림 2]에서와 같이 IETF의 인증절차는 상호간 인증서와 암호알고리즘 등 인증서비스(①-④)를 교환하고 원격 TGS 접근을 위한 티켓과 세션키를 교환하는 TGT 서비스 교환(⑤-⑥), 서버 접근용 티켓과 세션키를 교환하는 TGS 교환(⑦-⑧), 세션키에 의한 서비스 요청 과정(⑨)으로 원격 KDC가 지역 KDC의 정보를 인증한 후 티켓을 발급하였으나 수정된 Kerberos 메커니즘은 원격 Kerberos(KDC_R)가 인증과 동시에 티켓을 Client에게 발급함으로써 통신부담이 줄어들게 되었으며 임의 난수(Krand)에 의한 공통키의 생성이 불필요하게 되었다.

3.2 원격영역 Kerberos 인증 프로토콜 설계

Client가 요청한 서비스가 동일한 영역 내에 있는 서비스이면 KDC(AS)의 데이터베이스에서 Client의 정보로 인증을 하나 요청한 서비스가 동일 영역 내에 존재하지 않으면 KDC(AS)는 Client가 요청한 영역이 어디에 존재하는지 DS를 통하여 DNS에게 검색을 의뢰한다. DNS 서버는 정방향 조회영역, 캐쉬 루트서버를 이용하여 리졸빙 후 캐쉬영역에 저장 한 후 KDC(AS)로부터 의뢰를 받은 영역을 검색한 후에 이웃(Preauthentication)하는 영역을 DS에게 전송한다. DS는 각각의 영역을 상호인증하기 위한 전·후방 인증 체인을 생성하여 서비스 받을 Remote Realm의 공개키를 획득한다. 즉, DS는 인증의 기능이 없이 세션을 설정한 다음 KDC(AS)가 인증을 하는 수행 절차를 가지며 이제 클라이언트가 있는 영역과 서버간 연결이 직접적으로 이루어지므로 상호 영역간에 있어서 클라이언트를 인증하는 절차를 필요로 하게 된다. 그 이유는 침해자가 서비스를 요청한 클라이언트처럼 가장하여 서비스를 가로채거나 변경시킬 수 있기 때문이다. 클라이언트는 원격 Kerberos에게 X.509를 이용하여 얻은 원격 영역의 공개키로 정보를 암호화하여 전송함으로써 클라이언트와 원격 영역간의 통신을 방해하는 제3자로부터 보호할 수 있게 한다.



[그림 3] 수정된 Kerberos 메커니즘

[Fig. 3] Advanced Kerberos mechanism

본 논문에서는 DNS서버를 두고 다른 영역의 서버를 탐색할 때 질의, 연산을 통해 위치를 확인한다. X.509 프로토콜을 사용하여 전.후방 체인으로 원격 영역의 공개키를 획득함으로써 비밀키를 교환하는 번거로움을 배제한 PKINIT기반의 Kerberos 서버 상호지원 메커니즘이다.

[그림 3]은 서로 다른 영역의 Local Realm과 Remote Realm의 환경으로 원격 KDC는 TGS가 사용할 티켓(TicketTGS) 만을 발급하는 역할을 하며 티켓에는 발급자, 세션키, 발급대상의 ID와 주소, 발행시간, Reply 방지용 값을 포함한다. TGS는 서버승인 티켓(SGT : Server Granting Ticket)인 TicketSGT를 발급하는 서비스를 담당한다. Kerberos는 인증과 KDC(Key Distribution Center)의 역할을 하며 Local Client가 Remote Server의 서비스를 받기 위한 메시지 교환 내용은 다음과 같다.

인증 및 TGT 서비스 교환

(1) ID_C, $Realm_S$

(2) E_{KDC_PK}[SignedAuthPack, TrustedCertifiers, KdcCert, CertPath]

(3) $E_{[KDC\_PK}$: $Ticket_{TGS}$, $K_{C,TGS}$, TimeStamp, Nonce, $Realm_{TGS}$, $E_{[KDC\_RSK}$: $Ticket_{TGS}$, TimeStamp, PaChecksum, Nonce, $Realm_{TGS}$]]

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

(4) EK_C[$Ticket_{TGS}$, $K_{C,TGS}$, TimeStamp, Nonce, $Realm_{TGS}$, $EKDC\_rSK$[$Ticket_{TGS}$, TimeStamp, PaChecksum, Nonce, $Realm_{TGS}$]]

SGT 서비스 교환

(5) $EK_{C,TGS}$[ID_S, A_C, $Ticket_{TGS}$, $EKDC\_rSK$[$Ticket_{TGS}$, TimeStamp, PaChecksum, Nonce, $Realm_{TGS}$]]

(6) $EK_{C,TGS}$[$K_{C,SGT}$, $Ticket_{SGT}$, TimeStamp, Nonce, $Realm_{SGT}$, ID_S, EK_{SGT}[$K_{C,SGT}$, ID_C, AD_C, TS, ID_S, nonce]]

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

서비스 요청

(7) $EK_{C,SGT}$[$Ticket_{SGT}$, A_C, EK_{SGT}[$K_{C,SGT}$, ID_C, AD_C, TS, ID_S, Nonce]]

AC = $EK_{C,TGS}$[ID_C, AD_C, $Realm_{TGS}$, TimeStamp, Nonce]

메시지(1)에서 Client는 자신의 ID와 서비스를 원하는 영역을 자신의 영역에 있는 Local KDC에게 보내 서비스를 요청한 Client가 정당한 사용자인지를 Database에서 검색하여 유효성과 적법성을 검토하도록 한다. 서비스 영역이 다를 경우 DNS를 통하여 검색을 의뢰하고 해당영역의 DS는 DNS로부터 받은 서비스 영역(Remote 영역)에 관하여 상호인증을 하기 위한 전·후방 인증 체인을 생성하여 Remote 영역의 공개키를 획득한다. 메시지(2)에서 Local KDC는 Client와 자신의 정보(SignedAuthPack, TrustedCertifiers), KdcCert, CertPath를 전송하여 신원확인 및 티켓승인 티켓을 요청한다. 이 메시지에는 KDC_L과 Client에 대한 시간, 암호알고리즘, 유형, 인증서, 자신의 위치를 확인시키기 위하여 URL 값을 갖는 CertPath를 포함하고 있다. 메시지(3)에서 KDC_R은 kdcCert로 Client를 인증하고 KDC_R 영역의 TGS에게 Client의 인증을 확인시키기 위해 공유키(ESK)로 티켓과, 티켓발행시간, 암호알고리즘, 임의의 수, TGS의 영역을 공통키로 암호화하고 세션키와 티켓을 KDC_L의 공개키로 전송한다. 이때 KDC_R은 임의의 수를 자신 영역의 TGS에게 전송함으로써 Client로부터 전송될 내용과 비교하여 허가된 자라는 것을 확신시킨다. 메시지(4)는 KDC_L이 Client의 비밀키를 생성하여 KDC_L로부터 수신된 메시지를 보낸다. Client는 이제 티켓과 세션키(KC,TGS)를 가지면 TGS에 접근할 준비가 된다. 메시지(5)에서 Client는 TGS에게 티켓과 인증자, 서비스를 요청할 서버의 ID를 포함한 메시지를 보낸다. 부가적으로 Client는 인증자를 보내는데 여기에는 ID와 Client의 주소, Timestamp, 임의의 수가 포함되어 있다. 재사용할 수 있는 티켓과는 다르게 인증자는 한번만 사용되기 때문에 짧은 유효시간을 갖는다. TGS는 KDC_R의 공유키와 세션키, 자신의 비밀키를 가지고 티켓을 복호할 수 있다. 이 티켓은 Client에게 세션키(KC,TGS)가 제공되었음을 가리키기 때문에 KC,TGS을 사용하는 사람은 Client 뿐이다. 원격 TGS는 Client로부터 전송된 인증자와 티켓의 정보와 비교하여 일치하면 티켓을 보낸 사람은 실제 티켓의 소유자라고 인증할 수 있다. 메시지(6)는 서버를 사용할 수 있는 티켓(TicketSGT)과 세션키(KC,SGT)를 생성하고 원격 TGS는 서버의 비밀키(KSGT)로 티켓과, 유효시간, 임의의 수, 영역을 암호화하고 Client와 TGS 간의 세션키로 암호화하여 Client에게 전송한다. Client는 서버의 비밀키(KSGT)로 된 내용을 확인할 수 없다. 메시지(7)에서 Client는 서버를 사용하기 위한 요청으로 서버용 티켓(TicketSGT)과 인증자, 원격 TGS로부터 전송된 내용을 보냄으로써 서버로 하여금 인증자와 TGS로부터 온 내용을 비교하여 인증하고 세션키(KC,SGT)로 송수신할 수 있다.

3.3 Kerberos 프로토콜 주요 요소에 대한 이론적 해석

ID_C : 사용자의 식별자(C의 ID)로 신원을 KDC(AS)에게 알린다.

RealmS : 서비스 받을 서버가 위치하는 영역을 지정한다.

EKDC_Rpk : PKINIT 체인에 의해 획득한 원격영역의 공개키로 보호한다.

SignedAuthPack : 지역영역의 신원인증에 필요한 정보로 PkAuthenticator, ClientPublicValue의 값을 가진다.

- PkAuthenticator : 지역영역의 KDC(AS)의 정보로 cusec, ctime, nonce, PaChecksum으로 구성된다.
  - cusec : Client의 인증자를 발행한 시간을 알린다.
  - ctime : KDC_L의 인증자를 발행한 시간을 알린다.
  - Nonce : Reply가 아니라는 정당한 데이터의 무결성을 보장한다.
  - PaChecksum : ASN.1에서 정의한 암호화 알고리즘의 종류로 cksumtype과 checksum을 포함한다.
    - cksumtype : 암호 알고리즘 유형을 선택하는 정수 값이다.
    - checksum : 암호 알고리즘으로 crc32, rsa-md4, rsa-md4des, rsa-md5, rsa-md5des,des-mac이다.
- ClientPublicValue : Client의 공개정보로 SigAuth-Pack과 User-Type를 갖는다.
  - SigAuth-Pack : 암호Algorithm과 Parameter 값을 갖는다.
  - User-Type : 인증서 형식으로 X.509v3, PGP, PKIX를 갖는다.

'TrustedCertifiers : $KDC_{_L}$의 인증서로 principalName, caName, issuerAndSerial, userCert 값을 갖는다.

- principalName : KerberosName
- caName : X.500, X.509 검증을 거친 Name
- issuerAndSerial : Client 및 KDCs가 신뢰할 수 있는 CA의 번호
- UserCert : Client의 RSA암호화 증명서

KdcCert : $KDC_{_L}$이 발행한 Client의 인증서

CertPath : DNS를 통하여 세션이 설정된 주소를 갖는 인증서 체인 값이다.

E_{KDC_Lpk} : 지역 KDC의 공개키

$Ticket_{TGS}$: $KDC_{_R}$이 발행하여 TGS가 사용할 티켓

$Ticket_{SGT}$: TGS가 발행한 서버용 티켓

$K_{C,TGS}$: Client 와 TGS(Ticket Granting Server)간의 세션키

AD_C : Client에 있는 Address값(C의 IP)

ID_S : Remote Server에 있는 Server의 식별자(S의 ID)

$K_{C,SGT}$: Client 와 SGT(Server Granting Ticket)간의 세션키

A_C : Client의 인증자

4. 메커니즘 분석

IETF의 Working Group에서 사용하고 있는 Kerberos 메커니즘은 PKINIT의 기반의 PKIX(Public Key Infrastructure)로 공개키와 공통키를 사용하여 인증정보에 대한 무결성을 보장하고 있다. 또한 도메인간 연결정보에 대해서는 DS와 DNS에 대한 언급만 했을 뿐 구체적인 사용방법에 대해서는 기술되지 않고 있다. 본 논문에서 제시된 알고리즘은 Kerberos을 기반으로 IETF 그룹에서 사용하고 있는 PKINIT와 동등한 메커니즘이며, Kerberos(KDC)와 X.509에서 보장해 주는 안전성과 DS/DNS에 의한 경로에 대하여 인증서 체인(CertPath:Domain value)으로 보관하기 때문에 원격 Kerberos에서 Client로 TGT를 전송할 수 있다. 즉 Client는 $KDC_{_R}$을 경유하지 않아도 되며 Client가 TGT를 얻기 위한 별도의 요청을 필요로 하지 않는다. 또한 $KDC_{_R}$에서 상호인증을 위해 생성한 임시난수(K_{rand})값을 Client와 원격 TGS에서 암.복호화하는 과정이 생략되었으며 이로 인해 이중 암호화와 통신부담이 감소되었다. 서버용 티켓은 TGS의 키로 암호화(K_{TGS})되어 있으므로 변조가 불가능할 뿐만 아니라 Client의 공개키로 재 암호화하므로 제 3자가 티켓을 이용할 수 없다. 티켓 내에도 Client와 서버사이의 세션키($K_{C,S}$)를 포함시킴으로써 티켓 소유자가 정당한 사용자임을 증명한다.

본 논문에서 제시된 알고리즘은 원거리 통신에서의 보안성을 보장하기 위해서 정보를 전송시 Kerberos의 비밀키, PKINIT의 공개키로 암호화하였고 상호인증을 위해 X.509와 DNS를 이용한 체인(Directory System)방식으로 원거리 통신을 보다 더 안전성이 보장되는 Kerberos 시스템을 설계하였을 뿐만 아니라 Client가 Remote TGS에 서버용 티켓을 요청시 Remote KDC(AS)의 재확인 과정을 생략함으로 인한 임의의 공통키와 통신 복잡도를 감소하였다.

5. 결 론

분산환경에서 통신하고자 하는 다수의 웍스테이션들과 응용서버의 인증을 위해서 인증 메커니즘인 Kerberos와 초기 인증과정에서 공개키 암호 사용에 대한 정의를 기술한 PKINIT, PKIX의 인증시스템인 X.509를 고찰하였다. 본 논문에서는 Kerberos를 기반으로 하여 PKINIT에 포함된 X.509를 적용하여 영역간의 인증과 서비스를 제공하는 인증 방식을 제안하였다. DNS를 통해 외부영역의 위치를 탐색하고 X.509 디렉토리 인증 시스템인 DS를 적용한 영역간 체인을 통하여 공개키를 획득, 다른 영역을 인증하도록 하였다. PKINIT를 이용하여 두 영역의 Kerberos(KDC)를 연결하여 서비스를 하며 이때 영역의 공개키를 획득하기 위하여 X.509 프로토콜을 사용하여 공개키를 획득할 뿐만 아니라 원거리 통신에서의 보안성을 보장하기 위해서 정보를 전송시 상대방의 공개키와 비밀키를 암호화하였고 상호인증을 위해 체인(CertPath)을 이용하여 원거리 통신을 보다 더 안전성이 보장되는 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] 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-14.txt

[3] Y. Choi, C. Kang, D. Kim, "The Models and security Services for Directory System," Korea Inst. Info. Secu. & Crypt., vol. 5, no. 3, pp. 49-68, May 1995

[4] RFC 1510, Public Key Cryptography for Initial Authentication in Kerberos, draft-ietf-cat-kerberos-pk-init-09.txt, IETF, 1999

[5] J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.

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

[7] 김상균, 백종현, 이강석, 이석준, "공개키인증 기반구조로서의 X.509에 대한 연구", 통신정보보호학회지, 제8권, 제3호, pp.33-46, 1998.

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

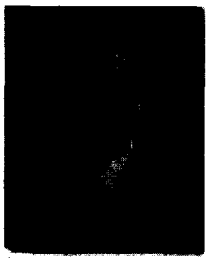
[9] http://www.kr.freebsd.org/doc/PoweredByDNS/resolving.html

[10] A. Medvinsky, M. Hur, S. Medvinsky, C. Neuman. "Public Key Utilizing Tickets for Application Servers (PKTAPP)". draft-ietf-cat-kerberos-pk-tapp-04.txt

신 광 철

1991년~1995년 전쟁연습
프로그램관 및 전산실장
(육군대학)
1995년~1999년 성균관 대학원
정보공학과 수료
1996년~현재 벽성대학
소프트웨어개발전공 교수
관심분야 : 정보보호기술, 객체
지향 분석/설계, 전자상거래
응용, Visual Programming

정 진 욱



1973~1985 한국과학기술
연구소 실장
1991년 서울대학교 대학원
계산통계학과 (이학 박사)
1998.3~1999.2 성균관대학교
정보통신대학원장
현재 성균관대학교 전기전자
및 컴퓨터공학부 교수