PKINIT 기반 새로운 커브로스 인증 메커니즘의 설계

(Design of a New Kerberos Authentication Mechanism based on PKINIT)

김 철 현 † 정 일 용 ††
(Cheolhyun Kim) (Ilyong Chung)

요 약 본 논문에서는 X.509와 DNS를 연관하여 새로운 Kerberos 인증 메카니즘을 제안한다. Kerberos에서는 영역간의 서비스에 대하여 언급을 하지 않았기 때문에 영역간 인증은 X.509와 DNS(Domain Name System)를 사용하여 얻을 수 있는 체인에 의해서 수행하는 PKINIT를 통하여 이루어진다. 두 개의 프로토콜은 상이한 키관리 방식을 갖고 있는데 Kerberos는 공통키에 기반을 두고 있는 반면에 X.509는 공개키 방식에 기반을 두고 있다. 따라서 본 논문에서는 이들을 상호 연동시키기 위해 연결 세션은 DS(Directory Service)를 이용하였고, 실제적인 인증을 위해서는 Kerberos를 적용하였다. 새로운 프로토콜은 통신복잡도의 관점에서 고찰하면 IETF CAT 작업반(Working Group)에서 제안한 인증 메커니즘보다 개선되었다.

Abstract In this paper, a new Kerberos authentication mechanism associated with X.509 and DNS(Domain Name system) is presented. Since any suggestion to regional services are not described in Kerberos, authentication between regions is performed via PKINIT, which can be accomplished by the connected chain obtained from X.509 and DNS. These two protocols have distinguished key management systems. X.509 is designed using an asymmetric method, while Kerberos using a symmetric method. In order to provide regional services, DS(Directory Service) is employed on connection part and Kerberos on actual authentication part. The new protocol is better than the authentication mechanism proposed by IETF CAT Working group in terms of communication complexity.

1. 서 론

컴퓨터와 정보통신의 발전에 따라서 다양한 응용 서비스가 창출하고 있으나 신뢰성있고 안전한 서비스들을 제공하기 위해서 해결되어야 할 중요한 문제는 정보보호이다. 정보통신 서비스 사용을 위협하는 대표적인 요소는 합법적인 사용자로 가장, 비인가 자원에 대한 접속시도, 서비스 제공의 부인 및 자료 수정 등이며 이를 해결하는 정보보안 메커니즘은 다양한 형태로 구현될 수 있다. 본 논문에서는 네트워크 상에서 여러 가지 문제점들을 대처하는 방안들 중 인증에 대해 중점적으로 다루고자 한다. 네트워크 상에서 사용권한이 없는 사용자가 실제 사용자인 것처럼 위장을 하여 서버에 접속, 위조한 메시지의 재전송 등을 통한 서비스를 요청할 경우 인증을 통하여 적법한 사용자만이 서비스를 사용할 수 있도록 하고 또한 사용자가 사용하려고 하는 영역 및 서버 확인과 같은 상호확인 과정을 통하여 소중한 정보가 제3의 사용자에게 유출되지 않도록 방지할 수 있도록 한다.

분산 환경에서 개발된 대표적인 인증 메커니즘으로 Kerberos[1]와 SESAME[2]가 있다. Kerberos는 MIT의 Athena 계획의 일환으로 개발된 인증 서비스로서 안전한 서비스를 통하여 사용자들을 인증 할 수 있도록 한 인증 메커니즘이며 키 분배 센터(KDC: Key Distribution Center)[3,4]의 개념을 적용하고 있다.

· 이 논문은 리눅스시스템 보안연구센터에서 지원받아 연구되었음.
† 비 회 원 : 조선대학교 컴퓨터공학부
chkim@mina.chosun.ac.kr
†† 종신회원 : 조선대학교 컴퓨터공학부·정보통신보안시스템 연구센터 교수
iyc@mina.chosun.ac.kr
논문접수 : 2000년 7월 27일
심사완료 : 2001년 1월 10일

IETF CAT 작업반에서 KDC 기반 인증 메커니즘을 설계하고 있는데 영역과 영역사이, 인증기관과 지역사이에 서비스를 수행하기 위하여 PKINIT(Public Key Cryptography for Initial Authentication)를 이용하고 있다. 현재의 IETF CAT 작업반에서 사용하고 있는 메커니즘을 살펴보면 Kerberos를 기반으로 하여 공통키를 사용하고 있으며 PKINIT[5]를 기반으로 두 영역과 영역사이를 공개키로 상호 서비스해주는 메커니즘[6,15]을 사용하고 있다. X.509[14]는 디렉토리 서비스를 정의하는 X.500[13,16] 서비스 권고 안의 일부분으로 자신의 사용자에게 X.500의 디렉토리에 의한 인증의 준비에 대해 골격을 정의하고 있으며 공개키 암호화 기법의 사용과 디지털 서명에 근거를 두고 있다. 지역 Kerberos는 클라이언트와 서버의 환경에서 인증서버 및 티켓 승인 서버를 두어 다단계 인증 서비스를 제공하는 메커니즘을 제공하고 있다. 승인 티켓을 얻기 위한 인증 서비스 단계에서는 클라이언트가 지역 Kerberos에게 인증을 받고 지역 Kerberos는 원격 Kerberos에게 클라이언트 및 자신의 인증을 받기 위한 과정을 도식하였다. 즉 지역 Kerberos는 클라이언트가 요청한 영역이 자신의 영역에 없으므로 DNS에게 원격 Kerberos 영역 검색을 의뢰함으로써 각각 Kerberos는 영역을 기억하지 않아도 될 뿐만 아니라 지역 Kerberos와 원격 Kerberos의 상호인증을 위하여 DS(Directory server)를 사용하여 지역 Kerberos과 원격 Kerberos에 전·후방 선인증(Pre-authentication) 체인으로 연결하여 상호인증을 할 수 있도록 설계하였다. 티켓을 얻기 위한 티켓 승인 서비스단계로서 원격 Kerberos가 지역 Kerberos에게 자료를 전송시 지역 클라이언트에게 티켓발급서버(TGS)와 사용 가능한 티켓을 전송하여 원격 Kerberos(AS)가 지역 클라이언트를 재확인 과정이 생략됨으로서 시간을 절약할 수 있고, 원격 Kerberos(AS)가 지역 클라이언트를 확인하기 위한 임의적인 난수(K_{rand})를 생성하지 않기 때문에 DES로 암호화하는 과정을 줄일 수 있다. 그러므로 클라이언트는 원격 Kerberos(AS)와의 확인 과정에 필요한 임의적인 난수(K_{rand})를 보관하지 않아도 되므로 난수보관에 대한 부담을 줄일 수 있다. 서버용 티켓을 얻기 위한 과정은 티켓을 사용하며, 티켓은 TGS의 키로 암호화(K_{TGS})되어 있으므로 변조가 불가능할 뿐만 아니라 클라이언트와 TGS사이의 세션키($K_{C,TGS}$)로 암호화, TGS가 발행한 티켓을 이용하는데 메시지 내에 클라이언트와 서버의 세션키($K_{C,S}$)를 서버의 비밀키(K_S)로 재 암호화하므로 제 3자가 티켓을 이용할 수 없다. 티켓 내에도 클라이언트와 서버사이의 세션키($K_{C,S}$)를 포함시킴으로써 티켓 소유자가 정당한 사용자임을 증명한다. 서버 인증 교환 과정은 지역(지역) 클라이언트와 원거리(원격) 서비스 인증 서비스 과정이다.

본 논문의 구성은 다음과 같다. 제2장에서는 기본적인 Kerberos 인증 절차에 대하여 설명하고, PKINIT를 실제로 구현하기 위해서 필요한 DNS와 X.509를 제3장과 제4장에서 논의한다. 제5장은 본 논문의 핵심적인 부분으로 클라이언트 인증을 위해서 Kerberos를 적용하고, 영역간의 서비스 부분에서는 PKINIT를 기반으로 하여 영역을 참조하는 인증 메커니즘을 제안하고 이를 분석하였다. 마지막 장에서는 결론을 맺는다.

2. Kerberos 인증 절차

Kerberos은 다양한 요소로 구성된 복잡한 시스템이며 중요한 요소로는 Kerberos 서버, 티켓승인서버(TGS), 티켓, 인증자 등이 있다. 티켓은 Kerberos서버와 티켓승인 서버가 생성하여 티켓승인 서버와 서비스 서버와의 통신에 이용되며, 티켓의 구성정보는 서버의 이름, 클라이언트의 이름, 클라이언트의 인터넷 주소, 타임스탬프, 유효시간과 세션키를 포함한다[1,4]. (그림 1)는 Kerberos 인증 프로토콜에 관한 개괄적인 그림을 표현하고 있다. Kerberos 프로토콜의 특징을 살펴보면 다음과 같다.

① 클라이언트는 클라이언트의 ID와 TGS 사용에 대한 요구를 의미하는 TGS ID를 AS에 보내는 것으로 클라이언트의 편에서 티켓-승인 티켓을 요구한다.

② AS는 클라이언트의 패스워드로부터 알아낸 키를 가지고 암호화된 티켓으로 응답한다. 이 응답이 클라이언트에 도착했을 때, 클라이언트는 클라이언트에게 패

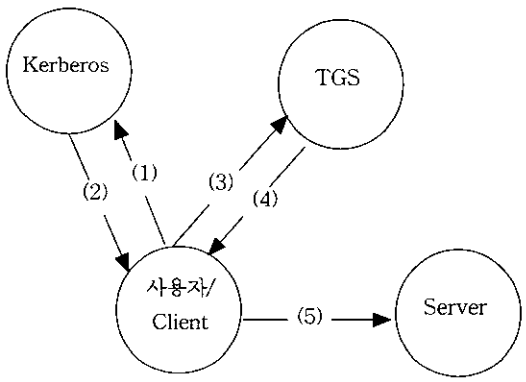

그림 1 Kerberos 인증 절차

스워드를 입력하라고 요구하고, 키를 생성한 다음, 들어온 메시지를 복호화한다. 정확한 패스워드가 입력되었으면 티켓은 성공적으로 만들어진다.

③ 클라이언트는 서비스-승인 티켓을 클라이언트의 편에서 요구한다. 이런 목적으로 클라이언트는 클라이언트의 ID, 요구하는 서비스의 ID 그리고 티켓-승인 티켓을 포함하고 있는 메시지를 TGS로 전송한다.

④ TGS는 들어온 티켓을 복호화하고 그 ID가 존재하는가에 의해 복호화의 성공 여부를 결정한다. 유효시간이 넘지 않았는지 점검한다. 그런 다음 클라이언트의 ID와 네트워크 주소를 클라이언트의 확인을 위해 들어온 정보와 비교한다. 끝으로, 요구한 서비스에 접속을 승인하는 티켓을 발행한다.

⑤ 클라이언트는 클라이언트의 편에서 서비스에 접속을 요구한다. 이 목적을 위하여 클라이언트는 서버에게 클라이언트의 ID 그리고 서비스-승인 티켓이 포함된 메시지를 보낸다. 서버는 메시지의 내용을 이용하여 승인한다.

3. DNS(Domain Name System)

DNS서버는 (그림 2)과 같이 연산 인터페이스와 관리 인터페이스의 두 인터페이스를 가진다. 연산 인터페이스를 사용하여 DNS 클라이언트는 DNS 서버에 질의를 보내고 DNS서버도 연산인터페이스를 통하여 응답을 한다[6]. 관리 인터페이스는 CA가 인증서와 CRL을 등록하기 위해 사용된다. 클라이언트나 관리자가 DNS서버에 요청을 보내고자 할 때는 적절한 매개 변수를 사용한다[8,9].

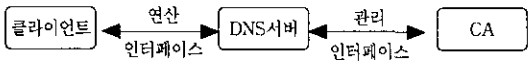

그림 2 DNS 서버의 인터페이스

먼저 X.509 인증서를 DNS서버에서 가져오는 과정을 설명한다. (그림 3)은 일곱 개의 DNS서버들의 계층구조를 보여주고 있다. 두 클라이언트 A와 B가 U,V,X의 범위에 등록되어 있고 클라이언트 C는 Z,Y,X의 범위에 등록되어 있다고 가정하자. 만약 클라이언트 A가 B의 인증서를 원한다면 질의는 DNS서버 U에 전달되고 U는 CA_U의 개인키로 서명된 B의 인증서를 받을 것이다. 클라이언트 A는 CA_U로부터 B의 공개키를 받아 인증서를 확인할 수 있다. 만약 클라이언트 A가 다른 범위에 있는 C의 인증서를 요청하면 이 요청은 반복적인 방법[11,12]이나 순환적인 방법으로 처리된다. 그러나 클라이언트 A는 CA_Z의 공개키를 가지고 있지 않으므로 C의 공개키 인증서를 확인할 수 없다. 따라서 클라이언트 A는 C의 인증서를 확인할 수 있기 위해서는 DS를 이용하여 전방인증서와 후방인증서를 연결하는 인증서 경로가 필요하게 된다. 전방인증서(A≪CA_U≫CA_U≪CA_V≫CA_V≪CA_X≫CA_X≪CA_Y≫CA_Y≪CA_Z≫CA_Z≪C≫)와 후방인증서(C≪CA_Z≫CA_Z≪CA_Y≫CA_Y≪CA_X≫CA_X≪CA_V≫CA_V≪CA_U≫CA_U≪A≫)는 다음과 같이 표현할 수 있다.

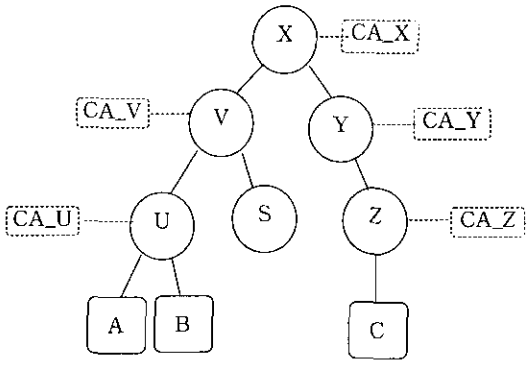

그림 3 DNS서버의 계층적인 구조

4. X.509 프로토콜

본 논문에서 영역간 연결은 디렉토리 인증 프로토콜인 X.509를 이용하며 외부 영역에 있는 서비스를 얻기 위하여 이름에 근거한 계층구조[10]를 사용한다. X.509[13,14]의 핵심은 각 클라이언트에게 연관된 공개키 인증서이다. 이 클라이언트 인증자들은 어떤 신뢰할 수 있는 인증기관 CA에 의하여 생성되어 CA 또는 클라이언트가 디렉토리에 배치하는 것으로 가정된다. 디렉토리 서버는 공개키의 생성이나 인증 기능에 대한 책임이 없으며, 클라이언트에게 인증서를 획득하는데 쉽게 접근할 수 있는 경로만을 제공한다. X.509 인증서의 구성은 다음과 같다.

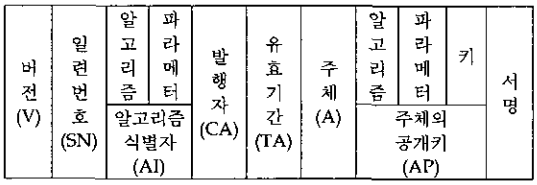

그림 4 X.509의 인증서

CA ≪ A ≫는 인증기관 CA에 의해 발행된 클라이언트 A의 인증서이며 CA{V, SN, AI, CA, TA, A, AP}로 정의된다. 클라이언트 A,B가 있고 인증기관 X1,X2가 있는 계층구조의 예를 (그림 5)에 표현하였다.

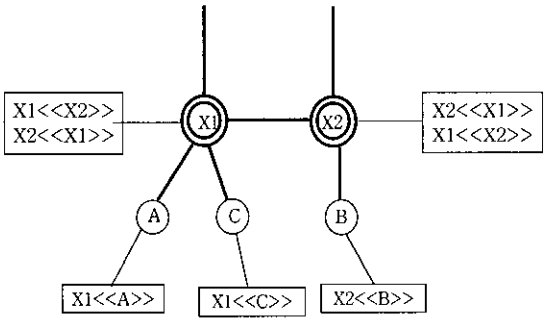

그림 5 인증기관의 계층 구조 예

A가 B의 공개키를 획득하기 위하여 인증서의 체인 X1≪X2≫X2≪B≫를 사용하고 동일한 방법으로 B는 역방향 체인 X2≪X1≫X1≪A≫를 이용하여 A의 공개키를 획득한다. 이러한 체인은 두 개의 인증서에 제한되는 것이 아니고 다음과 같이 N개 요소로 구성된 X1≪X2≫ X2≪X3≫…X_N≪B≫ 체인을 형성할 수 있다. 이 경우에, (Xi, Xi+1)연결에 있는 CA의 각 쌍은 서로가 인증서를 갖고 있어야한다. 이와 같이 CA에 의한 모든 CA의 인증서들은 디렉토리에 표현될 필요가 있으며 클라이언트는 각 인증서들이 다른 클라이언트의 공개키 인증서 경로를 따라서 어떻게 연결되어 있는지를 알 필요가 있다. X.509는 진행과정이 직선적으로 이루어지도록 CA를 중심으로 계층적으로 정렬하도록 제시하고 있다. 연결된 원은 CA들 사이의 계층적 관계를 나타내며, 연관된 사각형은 각 CA 엔트리에 대하여 디렉토리에 유지되고 있는 인증서들을 나타낸다. CA X에 대한 디렉토리 엔트리는 2가지 타입의 인증서를 포함하고 있는데 다른 CA에 의하여 생성된 클라이언트 인증서는 CA 이외의 누구도 검출되지 않고 인증서를 수정할 수 없다는 특성을 가지고 있다. 그리고 인증서는 위조할 수 없기 때문에 인증서를 보호하기 위한 특별한 노력없이 디렉토리에 배치될 수 있다[10].

5. PKINIT 기반 새로운 Kerberos 인증 메커니즘의 설계

5.1 Kerberos 인증메커니즘의 설계

IETF CAT 작업반의 인증 메커니즘은 PKINIT에 의해서 지역 영역 과 원격 영역을 상호 연결하는 인증 메커니즘이다. (그림 6)은 지역 클라이언트와 원격 서버간의 서비스과정을 나타낸 것이다. 지역 클라이언트가 서비스를 요청할 때 지역 Kerberos는 원하는 서비스의 영역을 파악한 후에 영역간 연결이 필요시 PKINIT에 포함된 X.509를 이용하여 서비스를 제공하는 과정을 살펴보도록 한다.

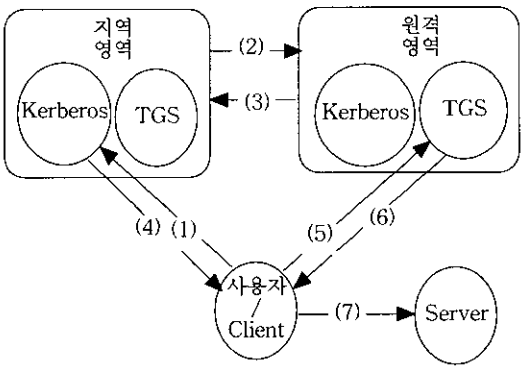

그림 6 클라이언트와 원격 서버간의 절차

지역 Kerberos는 지역 클라이언트가 요청한 영역이 동일한 영역내에 있는 서비스라면 영역간의 인증은 필요가 없다. 그러나 원하는 서비스가 동일영역이 아닐 경우에는 DNS를 사용하여 외부 영역의 경로를 찾는다. (그림 7)은 DS를 이용하여 외부영역에 있는 목적지까지 경로 연결 세션 과정을 도식한 것이다. 즉, CS.MIT.EDU 영역에 있는 클라이언트가 IFS.UMICH.EDU 영역에 있는 서비스를 사용하기 위한 내용으로 CS.MIT.EDU 영역의 클라이언트는 그와 선인증하여 MIT.EDU 영역과 연결을 한 후 다시 EDU 영역과 연결을 하게 된다. 다시 EDU 영역은 UMICH.EDU 영역과 연결을 설정한 후 UMICH.EDU의 서브 영역인 IFS.UMICH.EDU와 연결을 하게된다. 그리고 각 영역마다 Directory server는 단지 연결 설정의 역할만 있을 뿐 인증의 기능은 갖지 않는다. 인증에 관한 제반 사항은 Kerberos에서 전담하기 때문이다. 즉, CS.MIT.EDU와 MIT.EDU 연결, MIT.EDU영역과 EDU영역 연결, EDU영역과 UMICH.EDU영역 연결, 그리고 UMICH.EDU영역과 IFS.UMICH.EDU 영역 연결한다. 그리고 CS.MIT.EDU의 클라이언트는 IFS.UMICH.EDU에 있는 서비스를 사용하기 위해 전방 인증서와 후방 인증서는 다음과 같다.

• forward certificate : MIT≪EDU≫EDU≪UMICH.EDU≫UMICH.EDU≪IFS.UMICH.EDU≫

• reverse certificate : UMICH.EDU≪EDU≫EDU≪MIT.EDU≫MIT.EDU≪CS.MIT.EDU≫

이제 클라이언트가 있는 영역 즉, CS.MIT.EDU 영역과 IFS.UMICH.EDU간 연결이 직접적으로 이루어지므로 상호영역간에 있어서 클라이언트를 인증하는 절차를 필요로 하게 된다. 그 이유는 침해자가 서비스를 요청한 클라이언트처럼 가장하여 서비스를 가로채거나 변경시킬 수 있기 때문이다.

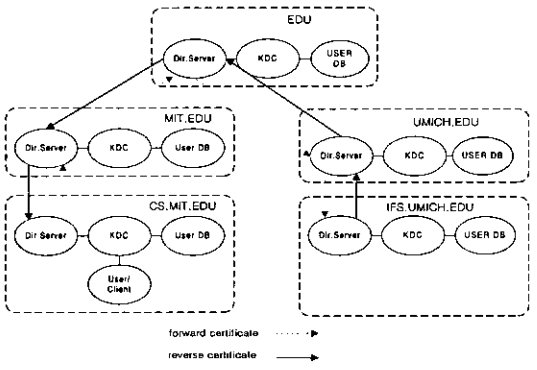

그림 7 디렉토리간의 인증

클라이언트는 원격 Kerberos에게 X.509를 이용하여 얻은 원격 영역의 공개키로 정보를 암호화하여 전송함으로써 클라이언트와 원격 영역간의 통신을 방해하는 침입자로부터 보호할 수 있게 한다. 클라이언트가 원격 영역의 서비스를 제공받기 위해서 필요한 정보 교환 알고리즘은 다음과 같다.

5.1.1 표기법

PK_C : C의 공개키
K_C : C의 개인키
CS : 증명서 일렬번호
A_P : 인증서 주체의 공개키(알고리즘, 파라메터, 키)
A_I : 알고리즘 식별자(알고리즘, 파라메터)
ID_C : C에 있는 클라이언트의 식별자(C의 ID)
AD_C : C에 있는 Address값(C의 IP)
KDC≪C≫ : Kerberos로 발행된 C의 인증서

5.1.2 제안된 알고리즘

① 클라이언트는 원격 영역의 서비스를 요청한다.

$C \rightarrow Kerberos_{LOC}$: ID_C, R

② 지역은 자신의 정보(Auth-Pack, SigAuth- Pack), Certificate의 형식(User-type), 클라이언트의 인증서, CS(CertificateSerialNumber)를 전방체인으로 획득한 원격 Kerberos의 공개키(PK_{KDC_REM})으로 암호화하여 전송한다. 클라이언트가 요청한 서비스가 동일한 영역 내에 있는 서비스라면 영역간 인증이던가 외부 영역에 있는 서버들의 공개키를 얻는 과정은 필요가 없게 된다. 만약 동일 영역 내에 존재하지 않으면 Kerberos는 클라이언트가 요청한 영역이 어디에 존재하는지 DNS에게 검색한 후에 선인증하는 영역을 전·후방 인증 체인을 생성하여 원격 영역의 공개키를 획득한다.

$Kerberos_{LOC} \rightarrow Kerberos_{REM}$:{Auth-Pack, {SigAuth-Pack} PK_C, User-type, KDC_{LOC} ≪C≫, CS}PK_{KDC_REM}

SigAuth-Pack : {A_I, PK_C}
Auth-Pack : {Kerberos, 영역, cusec, ctime, nonce, A_I, A_P}
cusec : INTEGER (for replay prevention as in RFC1510)
ctime : KerberosTime(for replay prevention as in RFC1510)
nonce : INTEGER (binds responce to the request)
User-type : X.509V3 (DER encoding)
PGP (PGP specification)
PKIX (PKCS #6)

③ 원격 Kerberos는 원격 TGS와 클라이언트사이에 사용할 정보를 지역 Kerberos의 공개키로 암호화(PK_{KDC_LOC})하여 전송한다.

$KDC_{REM} \rightarrow$ KDC_{LOC} : {V, KDC-cert, nonce, kdc PublicValue, {$K_{C,TGS}$, TGS, TS, nonce}PK_C, {$K_{C,TGS}$, ID_C, AD_C, TGS, TS, nonce}K_{TGS}, User-Type}PK_{KDC_LOC}

kdcPublicValue : {A_I, A_P}
User-type : X.509V3 (DER encoding)
PGP (PGP specification)
PKIX (PKCS #6)
KDC-cert : Issuer (인증서를 발행하고 서명한 CA)
SerialNumber (인증서 일련번호)

④ 지역 Keberos는 정보를 클라이언트의 개인키로 암호화하여 전송한다. 이 정보는 지역 클라이언트와 원격 TGS의 세션키($K_{C,TGS}$)및 원격 TGS Ticket을 포함하고 있다.

KDC_{LOC} -> C : {Auth-Pack, V, A_I, User-type, TGS, TS, nonce, $K_{C,TGS}$}K_C, {$K_{C,TGS}$, ID_C, AD_C, TGS, TS, nonce}K_{TGS}

⑤ 클라이언트자신이 사용할 서버와 TGS용 티켓, 자신의 인증서를 세션키($K_{C,TGS}$)로 암호화 한 후 서버용

비교 / 과정	IETF CAT 작업반	제안된 알고리즘
지역 Kerberos ⇔ 원격 Kerberos	- 지역 Kerberos는 클라이언트가 서비스를 받고자 하는 원격 영역에 존재하는 Kerberos에게 자신과 클라이언트의 정보를 암호화한 후 PKINIT를 사용하여 전송한다. - 원격 영역에 위치한 Kerberos는 자신의 정보와 클라이언트를 인증할 수 있는 난수값을 발생하여 지역 영역에 위치한 Kerberos에 전송한다.	- 원격 영역에 존재하는 Kerberos의 위치탐색을 위하여 DNS를 적용했고, 상호 인증을 위해 X.509의 디렉토리 인증 시스템인 디렉토리 서버DS를 적용하여 영역간에 연결된 체인을 이용하여 다른 영역을 인증할 수 있도록 하였다. - 원격 영역에 위치한 Kerberos는 자신의 정보와 지역 영역에 존재하는 클라이언트가 사용할 수 있는 원격 TGS 티켓 및 세션키를 지역 영역에 위치한 Kerberos에 전송한다.
지역 Kerberos ⇔ 지역 클라이언트	- 지역 Keberos는 원격 Kerberos에게 전송 받은 정보를 해독한 후 원격 Kerberos의 정보 및 난수값을 클라이언트에게 전송한다.	- 지역 Keberos는 원격 Kerberos에게 전송 받은 정보를 해독한 후 원격 영역에 존재하는 TGS용 티켓 및 세션키를 클라이언트에게 전송한다.
지역 클라이언트 ⇔ 원격 Kerberos	- 원격 Kerberos는 자신이 발행한 난수값과 클라이언트가 보내온 난수값이 동일한가를 확인 후 클라이언트가 요청한 TGS용 티켓 및 세션키를 전송한다.	- 확인과정 불필요
지역 클라이언트 ⇔ 원격 TGS	- 지역 클라이언트는 원격 TGS로 받은 티켓 및 세션키로 원격 영역에 존재하는 서버용 티켓 요청한다.	- 동일

그림 8 알고리즘의 비교 분석

티켓을 요청한다.

C -> TGS_{REM} : S, {$K_{C,TGS}$, ID_C, AD_C, TGS, TS, nonce}K_{TGS}, {ID_C, AD_C, TS }$K_{C,TGS}$

⑥ 원격 TGS는 클라이언트와 서버가 사용할 세션키($K_{C,S}$)등을 포함한 정보를 클라이언트와 TGS용 세션키($K_{C,TGS}$)로 암호화하고, 클라이언트와 서버사이에 사용할 서버용 티켓을 서버의 개인키(K_S)로 암호화하여 클라이언트에게 전송한다.

TGS_{REM} -> C : {$K_{C,S}$, S, TS, nonce}$K_{C,TGS}$, {Kc,s, ID_C, AD_C, TS, S, nonce}K_S

⑦ 클라이언트는 서버용 티켓 그리고 자신의 인증서를 서버와 사용될 세션키($K_{C,S}$)로 암호화하여 서버에게 서비스를 요청한다.

C -> S : {Kc,s, ID_C, AD_C, TS, S, nonce}K_S {ID_C, AD_C, TS}$K_{C,S}$

5.2 프로토콜 알고리즘의 분석

현재의 IETF CAT 작업반에서 PKINIT기반의 공개키와 공통키를 모두 사용하여 Kerberos인증 시스템을 설계하고 있다. 클라이언트가 원격 영역 서비스를 받기 위해서는 먼저 자신의 영역에서 인증을 받은 후 원하는 서비스가 외부영역에 있는 경우 지역 영역에 위치한 Kerberos와 원격 영역에 있는 Kerberos사이에 PKINIT를 이용하여 정보를 송·수신한다. 지역 영역에 위치한 Kerberos에게 전송된 정보 속에는 지역 영역에 존재하는 클라이언트를 인증할 수 있는 난수값이 포함되어 있다. 지역 영역에 존재하는 클라이언트는 이 난수값을 보관해야 하며, 이 키로 원격 영역에 위치한 Kerberos에게 서비스를 요청할 수 있다. 본 논문에서는 Kerberos을 기반으로 IETF CAT 작업반에서 사용하고 있는 PKINIT에 포함된 X.509 프로토콜을 적용하였으며, X.509에 포함된 디렉토리 인증 시스템인 DS를 적용하여 영역간에 연결된 체인을 이용하여 다른 영역을 인증할 수 있는 공개키를 얻어서 서비스를 제공할 수 있도록 한다. (그림 8)은 IETF CAT 작업반과 제안된 알고리즘을 비교 분석한 것을 도식하였다.

6. 결 론

분산환경에서 대표적인 인증 메커니즘인 Kerberos와 PKINIT에 포함된 디렉토리 인증 시스템인 X.509를 고찰하였다. 본 논문에서는 Kerberos를 기반으로 하여 IETF CAT 작업반에서 사용하고 있는 PKINIT에 포함된 X.509를 적용하여 영역간의 서비스를 제공하는 인증 방식을 제안하였다.

Kerberos는 동일 영역에서는 다양한 정보보안 서비스를 제공하지만 외부 영역에서의 서비스에 대한 제안이 없다. 이를 보완하기 위해서 외부영역의 위치탐색을 위한 DNS를 적용하였고, PKINIT에 포함된 X.509를

적용하여 영역간에 연결된 체인을 이용하여 다른 영역을 인증할 수 있는 공개키를 얻어서 서비스를 제공받도록 한다.

두 개의 프로토콜은 상이한 키 관리 방식을 가지고 있는데 Kerberos는 공통키에 기반을 두고 있으며, PKINIT에 포함된 X.509는 공개키 방식에 기반을 두고 있으므로 상호 접목시키기 위해 연결 세션은 X.509 디렉토리 인증 시스템인 DS를 적용하는 공개키 획득할 수 있게 하였다. 이때 클라이언트는 난수값을 보관하지 않아도 되며 원격 영역에 위치한 Kerberos와의 재확인 절차과정을 배제하였으며 지역클라이언트와 원격 TGS 세션은 이전 세션 방식을 사용하여 공개키 방식과 비밀키 방식이 상호 충돌하는 문제점이 없도록 설계하여 IETF CAT 작업반에서 제시한 방법보다도 통신 복잡도를 감소하였다.

참 고 문 헌

[1] Steiner, J., Neuman, C. and Schiller, J., "Kerberos: An Authentication Service for Open Network Systems", *Proc. of the Winter 1988 Usenix Conference*, Feb. 1988.

[2] http://www.cosic.esat.kuleuven.ac.be/scsame

[3] http://cd.donga.ac.kr/~shwan/doc/data/kerberos/kerberos.html

[4] http://netsec.ajou.ac.kr/~gonswing/main/research/kerberos.html

[5] http://www.ietf.org/internet-draft-ietf-cat-kerberos-pk-init-09.txt

[6] 심회원, 김진성, 심영철, 임찬순, 변옥환, "확장된 DNS 보안 메커니즘의 설계 및 구현", 한국정보처리학회지, 제6권, 제1호, pp.134-147, 1999.

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

[8] 모영범, 송주석, "반복 인증을 고려한 인증 프로토콜 제안 및 분석", 통신정보보호학회논문지, 제5권, 제2호, pp.45-60, June 1995.

[9] http://www.ietf.org/interner draft-ietf-dnsop/key-hand-00.txt

[10] 최용락, 소우영, 이재광, 이임영, 통신망 정보 보호, 그린출판사, pp.204-211, 342-371, 1996.

[11] http://www.ietf.org/interner draft-ietf-dnsop/keyhand-00.txt

[12] http://www.nic.or.kr/data/report/DNSBIND/dns_binds.html

[13] http://www.opendiroectory.com/whitepapers/x500tut.html

[14] http://www.opendiroectory.com/whitepapers/x509tut.html

[15] Warwick Ford, *Computer Communications Security*, New Jersey, Prentice-Hall, 1994

[16] http://sorec.chungnam.ac.kr/~CALS/directory/dirstd.htm

김 철 현

1996년 광주대학교 공과대학 졸업(공학사). 2000년 조선대학교 교육대학원 졸업(교육학 석사). 주관심분야는 네트워크 보안, 전자상거래, 분산시스템 관리.

정 일 용

1983년 한양대학교 공과대학 졸업(공학사). 1987년 City University of New York 전산학과(전산학석사). 1991년 City University of New York 전산학과(전산학박사). 1991년 ~ 1994년 한국전자통신연구소 선임연구원. 1994년 3월 ~ 현재 조선대학교 컴퓨터공학부 부교수. 2001년 1월 ~ 현재 조선대학교 정보통신보안시스템 연구센터 소장. 관심분야는 네트워크 보안, 전자상거래, 분산시스템 관리, 코딩이론, 병렬 알고리즘