論文 97-22-12-25

분산환경에서 Kerberos와 X.509 Protocol을 이용한 인증 메카니즘의 설계

準會員 김 성 진* 正會員 정 일 용*

The Design of Authentication Mechanism Using Kerberos and X.509 Protocol in Distributed Environment

Seongjin Kim* *Associate Member* Ilyong Chung* *Regular Member*

요 약

Kerberos는 분산환경에서 사용되는 대표적인 인증 프로토콜이다. 본 논문에서는 Kerberos를 기반으로 하여 X.509와 연계하여 디렉토리 인증을 통한 영역간의 서비스를 제공하는 인증 방식을 제안하였다. Kerberos에서는 영역간의 서비스에 대한 제안이 없으므로 X. 509를 적용하여 영역간에 연결된 체인을 이용하여 다른 영역과 인증을 수행하도록 한다. 두 개의 프로토콜은 상이한 키관리 방식을 갖고 있는데 Kerberos는 공통키에 기반을 두고 있는 반면에 X.509는 공개키 방식에 기반을 두고 있으므로 이들을 상호 연동시키기 위해 연결 세션은 X.509를 이용하였고, 실제적인 인증관련 세션은 Kerberos를 적용하여 설계하였다.

ABSTRACT

Kerberos is the most used example of authentication technology in distributed enviroment. In this paper, based on this method, a new authentication mechanism associated with X.509 protocol that authenticates services between regions is presented. Since any suggestions to regional services are not described in Kerberos, the authentication between regions is performed via the connected chain obtained from X.509. 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, X.509 is employed on connection part and Kerberos on actual authentication part.

Ⅰ. 서 론

컴퓨터와 정보통신의 발전에 따라서 다양한 응용 서비스가 창출하고 있으며 신뢰성있고 안전하게 서비스들을 제공하기 위해서 해결되어야 할 중요한 문제는 정보보호이다. 정보통신 서비스 사용을 위협하는 대표적인 요소는 합법적인 사용자로 가장, 비인가 자원

*조선대학교 전자계산학과
論文番號:97280-0818
接受日字:1997年 8月 18日

에 대한 접속시도, 서비스 제공의 부인, 자료 수정 등이며 이를 해결하는 정보보안 메카니즘은 다양한 형태로 구현될 수 있다. 해결방안중에서 인증은 여러가지 위험 요소를 해결할 수 있는 관심 분야로 많은 연구가 진행되고 있으며 크게 사용자 인증과 메시지 인증으로 나누어져 사용자를 확인하고 수신된 메시지가 정당한 것인가 확인한다.

Needham과 Schroeder[1]은 사용자 자신의 비밀키와 상대방을 인증하기 위해 사용하는 핸드세이킹 함수를 알고 있다는 가정하에 프로토콜을 설계하였다. 하지만 이 프로토콜은 메시지의 재전송 문제가 발생되는 문제점이 있으며, 이를 해결하기 위해 Denning과 Sacco[2]는 타임 스탬프 개념을 프로토콜에 적용하여 각 사용자의 암호화 키가 누설되지 않았다는 가정하에 핸드세이킹함수를 사용하지 않아도 되는 키분배 프로토콜을 제시하였다. Otway와 Rees[3]는 공통키 암호화 시스템에서의 통신키 분배 및 사용자 인증을 위한 프로토콜로써 Needham과 Schroeder의 프로토콜에 기본을 둔 프로토콜을 제시하였으며 인증 서버를 통한 사용자 상호인증과 메시지 재전송 탐지를 위한 사용자 비밀키로 챌린지(challenge) 암호화 등을 수행하여 전송한다. 위에서 언급한 프로토콜들은 공통키 방식을 사용하든, 공개키 방식을 사용하든 통신키를 인증서버에게서 제공받거나 자신이 직접 관리해야하는 단점이 존재하며 이런 문제를 해결하기위해 Okamoto와 Tanaka[4]는 사용자 ID정보에 의한 통신키 분배 및 사용자 인증 프로토콜을 제안하였다. 사용자는 자신의 ID정보만을 가지고 있다가 통신을 할 때마다 자신이 통신키를 만들어 내고 상대방을 인증할 수 있도록 해준다.

분산 환경에서 인증 메카니즘에 대한 연구가 활발하게 이루어지고 있으며 대표적인 방법은 MIT의 Athena 계획의 일환으로 개발된 Kerberos[5]이다. 이는 인증 서비스이며 안전한 서버의 서비스를 통하여 사용자들을 인증할 수 있도록 한 시스템/프로토콜이 부가된 네트워크 서비스이다[6, 7, 8]. 상당수 인증 프로토콜이 공개키 암호 방식을 선호하는데 반해 Kerberos는 공통키 암호 방식을 사용하고 있으며[9], 현재 Kerberos V4와 V4의 결함 부분을 수정하여 인터넷 draft 표준(1510)으로 발표된 Kerberos V5의 두가지 버전이 있다[10]. Kerberos에서 제안하고 있는 인증 방식은 영역내에서는 명쾌하게 설명하고 있지만 영역간의 서비스에 대한 부분은 언급하고 있지 않다.

CCITT의 권고안 X.509[11]는 디렉토리 서비스를 정의하는 X.500 시리즈 권고안의 일부분으로 자신의 사용자에게 X.500의 디렉토리에 의한 인증의 준비에 대해 골격을 정의하고 있으며 공개키 암호화 기법의 사용과 디지털 서명에 근거를 두고 있다. 본 논문에서는 사용자의 인증을 위해서 Kerberos를 적용하며, 영역간 서비스 이용 부분에선 X.509를 사용하여 영역 참조하는 인증 메카니즘을 제안한다.

본 논문의 구성은 다음과 같다. 제 2장에서 Kerberos가 인증 서비스를 제공하는 방식과 V4, V5에 대해 설명하였고, 제 3장에서 디렉토리 인증 서비스인 X.509를 고찰하고, 제 4장에서는 Kerberos와 X.509를 결합한 인증 서비스의 설계를 제안하고 결론은 마지막 장에서 한다.

Ⅱ. Kerberos의 인증 방식

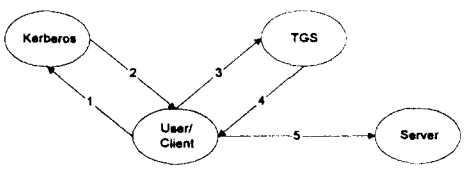
2.1 Kerberos V4 프로토콜

Kerberos은 다양한 요소로 구성된 복잡한 시스템이며 주요한 요소로는 Kerberos 서버, 티켓승인서버(TGS), 티켓, 인증자등이 있으며, 티켓은 Kerberos 서버와 티켓승인 서버가 생성하여 티켓승인 서버와 서비스 서버와의 통신에 이용되며, 티켓의 구성정보는 서버의 이름, 클라이언트의 이름, 클라이언트의 인터넷 주소, 타임스탬프, 유효시간과 세션키를 포함한다. 인증자는 클라이언트에 의해 생성되고, 생성된 인증자는 한 번만 사용될 수 있다. 즉, 새로운 서비스를 요청할 경우 클라이언트는 다시 인증자를 생성해야 한다. 인증자의 구성정보는 클라이언트의 이름, 워크스테이션의 IP 주소, 현재 워크스테이션의 시간을 포함하고 있다. 그림 1에서 Kerberos 인증 프로토콜이 나타나고 있다.

1) Client는 사용자의 ID를 Kerberos에게 보내어 TGS 사용을 승인하는 티켓 승인티켓을 요청한다.
2) Kerberos는 승인티켓을 사용자의 패스워드로부터 얻은 비밀키로 암호화하여 Client에게 전송한다.
3) Client는 승인티켓을 복호화하여 얻은 TGS와의 세션키로 서비스 승인티켓을 TGS에게 요청한다.

4) TGS는 들어온 티켓을 복호화하고 정당한 메시지인가를 확인하고 서비스 승인티켓을 세션키로 암호화하여 Client에게 전송한다.

5) Client는 승인티켓을 복호화하여 서비스 서버와의 세션키를 얻는다. 그리고 서비스를 이 세션키로 암호화하여 서비스 서버에게 요청한다.



1. Request for TGS ticket
2. Ticket for TGS
3. Request for Server ticket
4. Ticket for Server
5. Request for service

그림 1. Kerberos 인증 프로토콜

2.2 Kerberos V5 프로토콜

Kerberos V4는 환경적인 문제점과 구현기술상의 문제점이 나타나는데 첫 번째 범주에 해당되는 문제점으로는 표준화된 DES 알고리즘을 이용하지 않으며 IP 주소의 사용을 권장하지 않고 있다. 티켓 유효시간도 최대 유효시간이 1280분으로 고정되어 장시간 실행되는 시뮬레이션에는 부족하며 인증서에 관한 문제에서는 한 번 발행된 인증서가 다른 영역의 호스트에서는 인증이 되지 않는 점이 있다. 특히 상호 영역의 인증에 있어서도 n영역 사이의 상호 운영 능력이 $O(n^2)$의 Kerberos대 Kerberos관계를 요구한다[12].

구현기술상의 문제점으로는 Kerberos에서 Client로 되돌아오는 메시지를 보면 이중 암호화되어 $\{K_{c,tgs}$, $\{T_{c,tgs}\}K_{tgs}\}K_c$ 처럼 되어있고 TGS에서 Client로 되돌아오는 메시지에서도 $\{\{T_{c,s}\}K_s$, $K_{c,s}\}K_{c,tgs}$처럼 이중 암호화[13]가 되어있는데 이는 암호화 절차만 복잡한 불필요한 과정이다. 제 3자의 공격은 상당히 심각할 수 있는데 특정한 서버로부터 서비스를 받기위해 세션키를 연속 사용하여 침해자에게 사용당할 우려, 패스워드에 대한 공격등이 문제가 된다.

Kerberos V5에서는 언급된 V4의 문제점들을 해결하고 있다. 수신자가 메시지를 번역하기위해 적절한 복호 알고리즘을 식별하도록 식별자를 붙여주고, 네트워크 주소에는 형태와 길이 field를 덧붙이고, 수신자가 적절히 주소들을 번역할 수 있게한다. 네트워크 메시지는 Abstract Syntax Notation One(ASN.1)을 이용하고 기본적인 암호화 규칙 [ISO8825]에 따라 메시지를 암호화한다. V4에서의 Kerberos 영역은 N 대 N의 관계로 키 교환의 수가 $O(n^2)$이었는데, V5는 그림 2와 같이 영역의 이름에 근거한 계층 구조를 이용하며 키 교환의 수를 O(log(n))으로 감소시킨다[12].

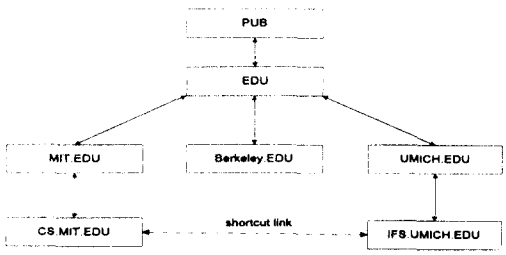


그림 2. V5의 영역 계층

Ⅲ. X.509 프로토콜

본 논문에서 영역간 연결은 디렉토리 인증 프로토콜인 X.509를 이용하며 V5에서 외부 영역에 있는 서비스를 얻기 위해서 이름에 근거한 계층구조를 사용한다. X.509 스키마의 핵심은 각 사용자에게 연관된 공개키 인증서이다. 이 사용자 인증자들은 어떤 신뢰할 수 있는 인증 기관 CA에 의하여 생성되어 CA 또는 사용자가 디렉토리에 배치하는 것으로 가정된다. 그리고 디렉토리 서버(Direcory Server:DS) 자체는 공개키의 생성이나 인증 기능에 대한 책임이 없으며 단지 사용자에게 인증서를 획득하는데 쉽게 접근할 수 있는 장소를 제공한다. X.509 인증서의 구성[14, 15]은 다음과 같다.

버전 (V)	일련번호 (SN)	알고리즘 고유 식별자 (AI)	발행자 (CA)	유효기간 (T_A)	주체 (A)	주체 공개키 (A_P)	서명

그림 3. X.509의 인증서

CA≪A≫는 인증기관 CA에 의해 발행된 사용자 A의 인증서이며 CA{V, SN, AI, CA, TA, A, AP}로 정의된다. 사용자 A, B가 있고 인증기관 X1, X2가 있는 계층구조의 예를 그림 4에 표현하였다.

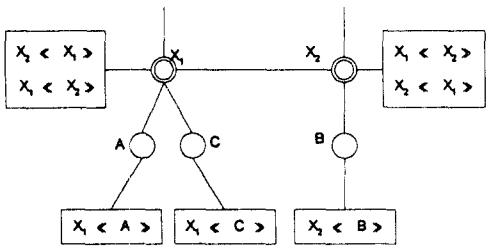


그림 4. X.509 CA 계층 구조의 가상 예

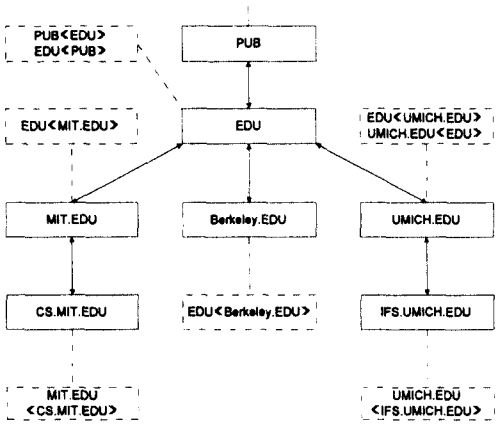


그림 5. 디렉토리와 해당 디렉토리의 인증서

A는 B의 공개키를 획득하기 위하여 인증서의 체인 $X_1≪X_2≫X_2≪B≫$을 사용하고 동일한 방법으로 B는 역방향 체인 $X_2≪X_1≫X_1≪A≫$을 이용하여 A의 공개키를 획득한다. 이러한 체인은 두 개의 인증서에 제한되는 것이 아니고 다음과 같이 N개 요소로 구성된 체인 $X_1≪X_2≫X_2≪X_3≫ \cdots ≪XB≫$을 형성할 수 있다.

이 경우에 체인 (X_i, X_{i+1})의 각 CA쌍은 서로가 인증서를 갖고 있어야 한다. 이와 같이 CA에 의한 모든 CA의 인증서들은 디렉토리에 표현될 필요가 있으며 사용자는 각 인증서들이 다른 사용자의 공개키 인증서 경로를 따라서 어떻게 연결되어 있는지 알 필요가 있다. X.509는 진행 과정이 직선적으로 이루어지도록 CA를 계층적으로 정렬하도록 제시하고 있다. 연결된 원은 CA들 사이의 계층적 관계를 나타내며, 연관된 네모 상자들은 각 CA 엔트리에 대하여 디렉토리에 유지되고 있는 인증서들을 나타낸다. CA X에 대한 디렉토리 엔트리는 2가지 타입의 인증서를 포함하고 있는데 다른 CA에 의해 생성된 X의 인증서인 전방 인증서와 X가 생성한 다른 CA의 인증서인 후방 인증서이다. CA에 의하여 생성된 사용자 인증서는 CA이외의 어느 누구도 검출되지 않고 인증서를 수정할 수 없다는 특성을 갖는다. 그리고 인증서는 위조할 수 없기 때문에 인증서를 보호하기 위한 특별한 노력없이 디렉토리에 배치될 수 있다.

그림 5는 CS.MIT.EDU에서 IFS.UMICH.EDU의 서비스를 사용하기위해 인증서의 체인을 사용하면 다음과 같다.

① forward certificate : MIT.EDU≪EDU≫EDU≪UMICH.EDU≫UMICH.EDU≪IFS.UMICH.EDU≫

② reverse certificate : UMICH.EDU≪EDU≫EDU≪MIT.EDU≫MIT.EDU≪CS.MIT.EDU≫

Ⅳ. Kerberos와 X.509를 결합한 인증메카니즘 설계

사용자가 서비스를 요청할때 Kerberos는 원하는 서비스의 영역을 파악한 후에 영역간 연결이 필요시에 X.509를 이용하여 서비스를 제공하는 과정을 살펴보도록 한다. 먼저 CS.MIT의 영역에서 사용자가 그 영역의 Kerberos에게 인증을 받아야 하며 사용자의 유효시간이라든가 가로채기에 의한 침입 혹은 재전송의 여부를 조사한다. 그림 6은 사용자가 소속해 있는 영역에서 우선적인 접속이 이루어진 과정을 표현한 것이다. 이 과정에서는 서비스를 필요로하는 사용자의 신분 인증에 관한 사항만을 Kerberos가 입증하는 절차이므로 Kerberos 공개키로 암호화하여 전송할 필요는 없다. 이 부분부터 암호화한다면 수없이 접속해오는 모든 사용자들에 대해 Kerberos가 비밀키로 해독해야하므로 시스템에 과부하를 초래할 수 있다.

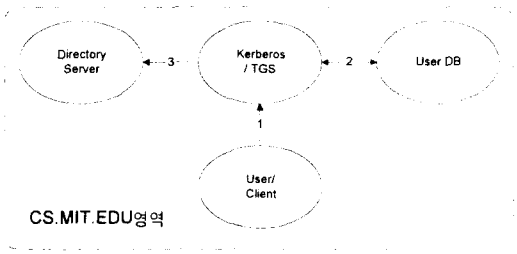


그림 6. CS.MIT.EDU에서의 연결

사용자가 Kerberos에게 자신의 ID와 원하는 서비스에 관한 내용을 전송하게 된다. Kerberos는 사용자에 관한 정보들을 데이터베이스에서 탐색하여 인증하며, 요청한 서비스가 위치한 영역을 검색한다. 만약 동일한 영역내에 있는 서비스라면 영역간 인증은 필요가 없다.

그림 7은 사용자가 원하는 서비스가 외부영역에 있을 경우 이를 원하는 목적지까지 경로를 연결하는 사항을 나타내고 있다. CS.MIT.EDU 영역에 있는 사용자가 IFS.UMICH.EDU 영역에 있는 서비스를 사용하기 위한 내용으로 CS.MIT.EDU 영역의 사용자는 그와 이웃해 있는 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 있는 Directory server는 단지 연결 설정의 역할만 있을뿐 인증의 기능은 갖지 못한다. 인증에 관한 제반 사항은 Kerberos에서 전담하기 때문이다.

그림 7은 CS.MIT.EDU와 MIT.EDU 연결, MIT.EDU영역과 EDU영역 연결, EDU영역과 UMICH.EDU영역 연결, 그리고 UMICH.EDU영역과 IFS.UMICH.EDU 영역 연결을 한다. 그리고 CS.MIT.EDU의 사용자는 IFS.UMICH.EDU에 있는 서비스를 사용하기 위한 전방 인증서와 후방 인증서는 다음과 같다.

- 전방인증서 : CS.MIT.EDU≪MIT.EDU≫MIT.EDU≪EDU≫EDU≪UMICH.EDU≫UMICH.EDU≪IFS.UMICH.EDU≫
- 후방인증서 : IFS.UMICH.EDU≪UMICH.EDU≫UMICH.EDU≪EDU≫EDU≪MIT.EDU≫MIT.EDU≪CS.MIT.EDU≫CS.MIT.EDU≪X1≫

CS.MIT.EDU 영역과 IFS.UMICH.EDU 영역간 연결이 직접적으로 이루어지므로 상호영역간에 있어서 사용자를 인증하는 절차를 필요로 하게 된다. 그 이유는 침해자가 서비스 요청 사용자처럼 가장하여 서비스를 가로채거나 변경시킬 수 있기 때문이다. 공개키 $PK_{IFS.UMICH.EDU}$를 $Client_{X1}$이 알고 있으므로 공개키로 자신이 보내고자 하는 내용을 암호화하여 통신을 하게 된다. 그림 8는 IFS.UMICH.EDU로부터 CS.MIT.EDU로 공개키 $PK_{IFS.UMICH.EDU}$가 전송된 다음 직접적으로 두 영역간 통신이 이루어지는 모습을 그려본 것이다. CS.MIT.EDU를 X, IFS.UMICH.EDU

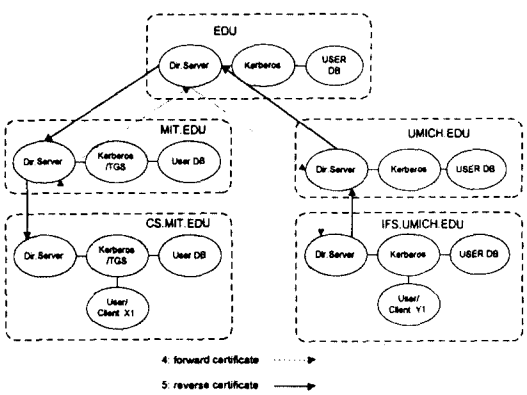


그림 7. 디렉토리간의 인증

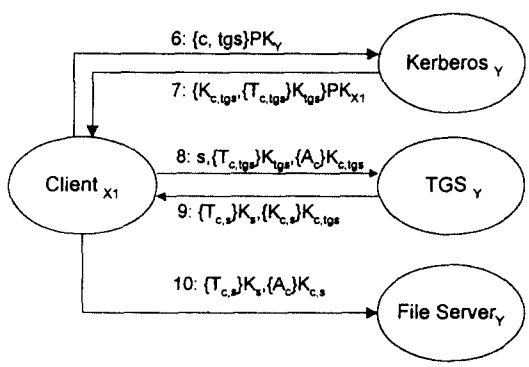


그림 8. 두 영역간 통신

를 Y, 그리고 서비스를 제공할 서버는 File Server로 가정하였다.

그림 8에서 $Client_{X1}$은 $Kerberos_Y$에게 X.509를 이용하여 얻은 Y영역의 공개키 PK_Y로 인증정보를 암호화하여 전송함으로써 송신측과 수신측의 통신을 방해하는 침해자로부터 보호할 수 있게 한다. $Kerberos_Y$는 자신의 비밀키로 수신된 메시지를 복호화한 후에 다시 $Client_{X1}$에게 공개키 PK_{X1}로 메시지를 암호화하여 전송한다. $Client_{X1}$은 자신의 비밀키로 메시지를 복호화하여 TGS_Y와 통신에 필요한 세션키와 티켓을 알아낸 후 이제부터는 해당 세션에 맞는 공통키를 사용하게 된다.

Kerberos와 X.509를 이용하여 그림 6~8에서 다룬 내용을 기반으로하여 $Client_{X1}$이 Y영역에 위치한 서비스를 제공받기 위해서 필요한 인증정보가 교환되는 알고리즘은 다음과 같다.

KerbX_Authentication Algorithm

1) $Client_{X1}$은 $Kerberos_X$에게 Client의 ID, 사용할 서비스, 그리고 송신시간을 담고있는 timestamp를 전송하여 $Client_{X1}$이 TGS와의 사이에서 사용할 티켓을 요청한다.
   $Client_{X1} \rightarrow Kerberos_X$: ID, service, timestamp
2) $Kerberos_X$는 $Client_{X1}$이 현재 유효한 사용자인지 데이터베이스 검색하여 적법성을 조사한다.
3) $Kerberos_X$는 $Client_{X1}$이 요청한 서비스가 어느 영역에 있는지 Directory $Server_X$(DS_X)에서 조사한다.
4) DS_X는 원하는 서비스를 제공하는 영역 Y와 전방 인증체인을 생성한다.
5) DS_Y는 공개키 PK_Y를 포함하는 후방 인증체인을 DS_X로 전송한다.
6) $Client_{X1}$은 $Kerberos_Y$에게 자신의 이름과 티켓을 승인할 TGS이름, 서비스 그리고 송신메시지의 시간을 담고 있는 timestamp를 PK_Y로 암호화하여 전송한다.
   $Client_{X1} \rightarrow Kerberos_Y$:{ID, TGS_Y, service, timestamp}PK_Y
7) $Kerberos_Y$는 $Client_{X1}$과 TGS_Y사이에서 사용할 세션키 $K_{C,TGS}$ 그리고 TGS의 키로 암호화된 티켓을 PK_{X1}로 암호화하여 $Client_{X1}$에게 전송한다.
   $Kerberos_Y \rightarrow Client_{X1}$: {K_{C,TGS_Y}}, {T_{C,TGS_Y}} K_{TGS_Y}}PK_{X1}
8) $Client_{X1}$은 부호화하여 얻은 세션키로 자신이 생성한 인증자를 암호화하고 승인티켓, Y 영역에서 서비스를 제공할 서버이름을 TGS_Y에게 전송한다.
   Client $X1 \rightarrow TGS_Y$: {A_C} K_{C,TGS_Y}, {T_{C,TGS_Y}} K_{TGS_Y}, S_Y
9) TGSY는 $Client_{X1}$에게 $Client_{X1}$과 서비스 서버 사이에 사용할 세션키를 K_{C,TGS_Y}로 암호화하고, 서버 사용승인 티켓을 전송한다.
   $TGS_Y \rightarrow Client_{X1}$: {K_{C,S_Y}} K_{C,TGS_Y}, {T_{C,S_Y}} K_{S_Y}
10) $Client_{X1}$은 서버 S_Y에게 사용승인 티켓과 K_{C,S_Y}로 암호화된 ClientX1의 인증자를 전송한다.
   $Client_{X1} \rightarrow Server_Y$: {A_C} K_{C,S_Y}, {T_{C,S_Y}} K_{S_Y}

V. 결 론

정보통신망에서 정보보안 메카니즘의 구현은 중요한 과제이며 이를 위해 대표적인 분산인증 프로토콜인 Kerberos V4와 V5를 연구하였고, 디렉토리 인증 시스템인 X.509를 고찰하였다. 본 논문에서는 Kerberos를 기반으로 하여 X.509를 적용하여 영역간의 서비스를 제공하는 인증 방식을 제안하였다. Kerberos는 동일영역에서 다양한 정보보안 서비스를 제공하지만 실환경에서 요구되는 외부 영역에서의 서비스에 대한 제안이 없다. 이를 보완하기 위해서 X.509를 적용하여 영역간에 연결된 체인을 이용하여 다른 영역을 인증할 수 있는 공개키를 얻어서 서비스를 제공받도록 한다.

두 개의 프로토콜은 상이한 키관리 방식을 갖고 있는데 Kerberos는 공통키에 기반을 두고 있는 반면에 X.509는 공개키 방식에 기반을 두고 있으므로 두 개의 프로토콜을 상호 접목시키기 위해 연결 세션은 X.509를 적용하는 공개키 방식에 기반을 두었고, 실제적인 인증관련 세션은 Kerberos를 적용하고 있는데 서비스를 제공하는 해당 영역의 Kerberos가 실제로 인증을 담당하는 방식으로 설계하였다.

참 고 문 헌

1. R. M. Needham and M. D. Schroeder, "Using Encryption for Authentication Large Networks of Computers," Comm. of ACM, Vol. 21, No. 12, pp. 993-999, Dec. 1978.
2. E. D. Dorothy and G. M. Sacco, "Timestamps in

Key Distribution Protocols," Comm. of ACM, Vol. 24, No. 8, pp. 533-536, Aug. 1981.
3. D. Otway and O. Rees, "Efficient and Timely Mutual Authentication," Operation System Review, Vol. 21, No. 1, pp. 8-10, Jan. 1987.
4. E. Okamoto and K. Tanaka, "Identity-Based Information Security Management System for Personal Computer Networks," IEEE J. on Selected Areas in Commun., Vol. 7, No. 2, pp. 290-294, Feb. 1989.
5. Jennifer G. Steiner, Clifford Neuman and Jeffrey I. Schiller, "Kerberos: An Authentication Service for Open Network Systems," In proceedings of the Winter 1988 Usenix Conference. Feb. 1988.
6. 모영범, 송주석, "반복 인증을 고려한 인증 프로토콜 제안 및 분석," 통신정보보호학회논문지, 제5권 제2호, pp. 45-60, 1995. 6.
7. Warwick Ford, Computer Communications Security, Prentice-Hall, pp. 131-137, 1994.
8. http://www.byte.com/art/9406/sec8/art.htm
9. B. C. Neuman and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks," IEEE Commun. Mag., pp. 33-38, Sep. 1994.
10. 이권일, "전자도서관 시스템에서 Kerberos를 이용한 사용자 인증 방법," 한국통신정보 보호학회 종합학술발표회논문집, 제6권 제1호, pp. 13-18, 1996.
11. 최용락, 강창구, 김대호, "디렉토리 모델과 정보보호 서비스," 통신정보보호학회지, 제5권 제3호, pp. 49-68, 1995. 9.
12. John T. Kohl, B. Clifford Neuman and Theodore Y. Ts'o, "The Evolution of the Kerberos Authentication Service," Proceedings of EurOpen Conference, pp. 1-15, 1991.
13. Simon Garfinkel and Gene Spafford, Practical UNIX Security, O'Relly & Associates, 1991.
14. 최용락, 소우영, 이재광, 이임영, 통신망 정보 보호, 그린출판사, pp. 342-371, 1996.
15. Christopher Mitchell, Michael Walker, and David Rush, "CCITT/ISO Standards for Secure Message Handling," IEEE J. on Selected Areas in Commun., Vol. 7, no. 4, pp. 517-524, May 1989.

김 성 진(Seongjin Kim) 준회원
1996년 2월 : 조선대학교 전자계산학과 졸업(이학사)
1996년 3월~현재 : 조선대학교 대학원 전자계산학과 석사과정
※주관심분야 : 컴퓨터 네트워크, 네트워크 보안시스템, 분산시스템

정 일 용(Ilyong Chung) 정회원
1983년 : 한양대학교 공과대학 졸업(공학사)
1987년 : 미국 City University of New York 전산학과(전산학석사)
1991년 : 미국 City University of New York 전산학과(전산학박사)
1991년~1994년 : 한국전자통신연구소 선임연구원
1994년~현재 : 조선대학교 전자계산학과 조교수
※주관심분야 : 네트워크 관리, 분산시스템 보안, 코딩이론, 병렬 알고리즘