論文
2-6-10

X.509기반 PKI의 영역간 상호인증 프로토콜에 관한 연구 (A Study of Cross Certification between Realms in Public Key Infrastructure based on X.509)

신 광 철*
(Kwang-Cheul Shin)

요 약

인터넷의 전자상거래, 응용서비스가 보편화되고 중요문서나 주문정보 등 개인정보가 네트워크상에서 교환되면서 송.수신자의 적법성과 정보의 무결성을 위해 허락된 사용자만이 자원에 접근할 수 있는 절차가 필요하다. 서버자원에 접근하는 사용자를 통제하고 클라이언트들을 식별하기 위해서는 인증서비스를 통해서 가능하다. 특히 분산환경에서는 공개키 암호시스템을 기반으로 구현되어야 여러 사용자들에게 동시에 편리성과 안전성을 보장할 수 있다. 본 논문에서는 PKI기반의 X.509와 DNS를 연관하여 디렉토리 인증을 통한 영역간 서비스를 제공하는 메커니즘을 설계하였다.

ABSTRACT

Electronic commerce and application service is to universal on the internet, and a large quantity information transmitted on the network, It's needs procedure to access only permit objects for the integrity of information. In order to provide regional services is authentication for control resource and client identification. In particular, public key system is to implement in distributed environment, it is able to insurance users convenience and integrity at the same time. In this paper designed mechanism of cross certification between realms in PKI based on X.509 associated with DNS (Domain Name System) that is presented.

1. 서론

인터넷시대의 가상세계를 통해 전자상거래, 응용서비스 등이 현실화되었으며 미래의 생활은 더욱 더 인터넷을 통해 이루어질 것으로 예상된다. 컴퓨터 및 통신망의 보급이 보편화되고 분산처리시스템과 개방형 시스템의 응용이 활발히 진행되고 수많은 정보들이 교환되면서 주체가 되는 송, 수신자가 적합한 상대인지, 전송도중 내용의 변질은 없었는지를 확인하는 인증이 필요하다.

인터넷은 서로를 직접 확인할 수 없는 가상공간의 특성으로 클라이언트와 서버는 서로간에 신뢰를 확보하기 힘들다. 서버의 정보에 접근하는 사용자를 통제하고 클라이언트들을 식별하기 위해서는 인증서비스를 통해서 가능하다[1].

* 정회원 : 벽성대학 소프트웨어개발전공 교수

논문접수 : 2001. 6. 12.
심사완료 : 2001. 6. 22.

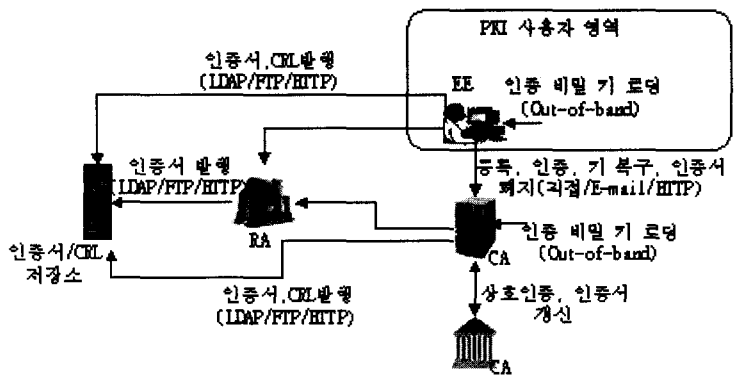
대부분의 시스템에서 패스워드 방식으로 사용자의 이용을 제한하고 있으나 지불정보나 중요한 문서의 경우는 클라이언트와 서버에 대한 각각의 인증과 상호인증 서비스를 제공해야 한다. Kerberos, Otway-Rees 등 서버기반 인증과 키분배 프로토콜의 모태가 되는 Needham과 Schroeder[1]식별 프로토콜은 사용자 자신의 비밀키와 상대방 인증용 핸드쉐이크 함수를 서로 알고 있다고 가정하여 설계한 프로토콜로 개체인증과 키 설정 서비스를 제공하나 메시지의 재전송이라는 안전성문제로 사용되지 않고 있으며 이를 보완하기 위해 Denning과 Sacco[2]는 타임스탬프 개념을 도입하여 핸드쉐이크 함수를 배제한 키 분배 프로토콜을 제시하였다. Otway와 Rees[3]는 Needham과 Schroeder의 식별프로토콜에 기반을 둔 키 분배 및 사용자 인증 프로토콜로 인증서버를 통하여 상호간에 인증이 이루어지고 메시지 재전송 탐지를 위해 사용자의 비밀키로 challenge 암호화를 수행하여 전송한다. 이러한 프로토콜들은 공개키나 개인키를 자신이 보유하거나 서버에 등록하여 제공받아야 하는 문제가 있다. 본 논문에서는 분산, 개방환경에서 PKI 구조의 X.509 디렉토리 인증서비스를 적용하여 해결하고자 한다. X.509는 디렉토리 서비스를 정의하는 X.500 시리즈 권고안의 일부로 공개키 암호화와 디지털서명에 근거를 두고 있다[4].

2. X.509 PKI의 구성요소

PKI(Public Key Infrastructure) 관리를 위해 IETF (Internet Engineering Task Force)의 PKIX(Public Key Infrastructure)분과의 Draft에 의해 정의되고 있는 X.509기반 PKI에 대해 살펴본다.

2.1 PKI의 구성요소와 기능

PKI는 공개키 암호를 기반으로 하고 있는 전자서명 어프리케이션에서의 무결성(Integrity), 송신 부인봉쇄(source non-repudiation), 인증(Authentication) 등의 보안서비스가 효율적이고 안정적으로 제공될 수 있도록 함을 주요 목적으로 하고 있으며 PKI가 제공해야하는 가장 기본적인 기능은 인증기능으로 각 개인 또는 기관들과 같은 개체들과 그들이 소유하고 있는 공개키 값(Public Key Value)을 공식적으로 연결(binding)하는 행위와 검증(validation)기능으로 인증내용이 여전히 유효한지를 확인하는 행위이다. [그림 1]에서와 같이 PKI 관리모델은 최종개체와 다른 CA들에게 인증서를 발행하는 인증기관(CA : Certification Authority)과 CA역할을 대신하여 사용자의 신분을 확인하고 토큰분배, 취소보고, 이름할당, 키 생성 및 키 쌍 기록 등을 수행하는 등록기관(RA : Registration Authority)이 있으며 이름과 개인키, CA의 이름 및 공개키의 정보를 안전하게 저장하고 이에 대해 접근을 통제하는 최종개체(End Entity), 저장소(Repository)로 구성된다[5].



[그림 1] 인증서 관리를 위한 PKI의 구성요소

[Fig.1] Elements of PKI

인증서/CRL 저장소는 디렉토리 서버로 각 서버에 의해 발행된 인증서와 취소된 인증서리스트(CRLs)에 대한 보관 및 정보제공을 위한 정보저장소로 CA가 담당 관리한다. 최종개체인 클라이언트는 공개키 기반의 어프리케이션을 이용하는 사용자 및 관련 응용 시스템을 통칭하며 자신의 공개키에 대한 인증서의 요청과 획득, 자신 및 다른 사용자의 공개키 인증서의 검증기능을 수행할 수 있어야 한다. 이 PKI 구성 요소들 간에는 온라인으로 상호 지원해야 하며 CA와 EE, 두 CA 간에 이용이 가능해야 한다. 이와같이 PKI의 기능은 공개키를 개인이나 조직, 또는 다른 개체에 묶어주는 인증과정과 인증의 유효성을 검증하는 과정으로 구성된다.

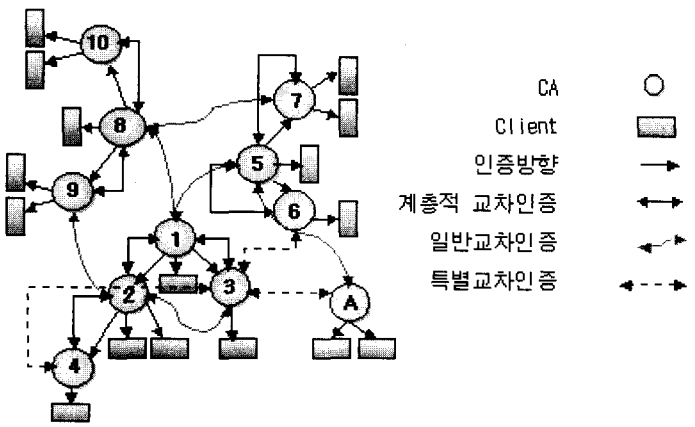
2.2 PKI의 혼합형 인증구조

PKI는 CA들에 대한 구성체계를 통하여 인증서와 CRL 등에 대한 관리의 최적화를 추구하고 CA간 신뢰고리를 어떻게 형성하느냐에 따라 해당 PKI의 특성을 결정지을 수 있다. 가장 기본적인 인증체제로는 체계성과 정렬성에 초점을 두고 있는 계층적구조(Hierarchical structure)를 들 수 있고 이와는 대조적으로 체계의 자율성에 초점을 두고 있는 네트워구조(Network structure)가 있다. 또한 이 두 구조의 장단점을 수용할 수 있는 혼합형구조(Hybrid Structure)[그림 2]가 제시되고 있다. 본 논문에서는 계층적 구조와 네트워구조가 혼합된 형태의 구조로 단위 어프리케이션은 조직별 계층적 구조의 형성과 이들간에 교차인증을 하는 네트웍 구조 형태인 혼합형구조를 제시했다. 특정 도메인별로 여러 개의 Root CA를 둘 수 있으며 이들 Root CA들은 자신의 하위 CA에 대한 인증과 다른 도메인의 Root CA 등과 교차인증을 수행하여 신뢰고리를 형성한다.

- 계층적 교차인증(Hierarchical cross-certificate) : 상.하위 CA들간의 인증경로
- 일반 교차인증(general cross-certificate) : 서로 다른 도메인의 Root CA들간의 교차인증
- 특별 교차인증(Special cross-certificate) : 인증계층의 최하위 CA들간의 교차인증

2.3 X.509 디렉토리 인증서비스

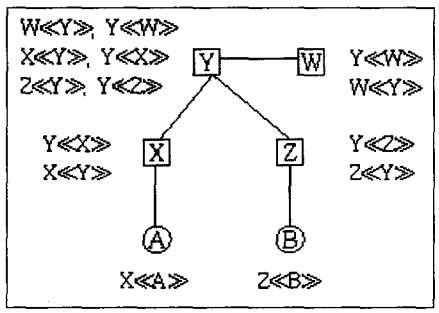
디렉토리 서비스란 사용자들이 네트워크 상에서 필요한 객체를 찾아 사용할 수 있도록 디렉토리 정보를 생성하고 유지, 관리하는 서비스이다[6]. X.500 표준은 대규모 네트웍에 디렉토리 서비스에 대한 호환을 제공하기 위해 ITU(International Telecommunications Union)에서 고안되었으며 정의된 디렉토리 정보는 다음과 같다.



[그림 2] 혼합형구조(Hybrid Structure)
[Fig.2] Structure of Hybrid

- 디렉토리 정보는 정보에 대한 객체, 객체에 대한 속성, 속성의 타입과 값이 구성되어야 한다.
- 디렉토리 서비스를 이용하여 객체의 정보를 쉽게 검색할 수 있도록 체계적이고 계층적인 이름 구조를 가지고 저장되어야 한다.
- 사용자들이 디렉토리 내의 정보를 생성, 수정하고 사용할 수 있는 기능을 제공하여야 하며 인증된 사용자만이 디렉토리 정보를 사용할 수 있는 인증서비스 기능을 제공해야 한다.
- 지속적으로 서비스 할 수 있는 분산처리능력을 가져야 한다.

X.500은 디렉토리에 각 정보를 생성, 저장 및 정보에 대한 Access 방식을 정의한 표준 디렉토리 서비스 프로토콜로 디렉토리는 객체와 속성들로 구성된 엔트리로 국제적으로 유일한 이름(DN : distinguished Name)을 가지며 DIT(Directory Information Tree)로 구성된다. 디렉토리 서비스는 X.500 디렉토리 서비스를 준수하며 디렉토리 서버에 접근하기 위한 프로토콜로는 DAP(Directory Access Protocol)와 LDAP(Lightweight DAP, RFC1777)가 가장 많이 활용되고 있으며 이밖에 FTP, HTTP 등을 이용할 수도 있다. 즉 DNS와 LDAP를 기반으로 구현되며 검색엔진과 통합저장소 역할을 한다. X.509는 X.500서비스를 인증하기 위한 PKI 구조를 제공한다. CA가 발행하는 인증서는 특정개체를 확인하고 특정한 활동과 권한, 능력을 허가하기 위한 정보로 구성되어 있는 CA의 서명문이다. 표준화된 인증서는 X.509 신분확인용 인증서로 X.509는 디렉토리 서비스를 규정하는 X.500 시리즈 권고안 계열의 일부분으로써 사용자들에 대한 정보를 담고 있는 일종의 서버인 X.500 디렉토리를 통해서 제공되는 인증 서비스의 구성을 명시하고 있다[7]. 공개키 암호와 전자서명에 기반을 두고 있는 X.509는 특정한 암호나 서명의 사용을 명시하고 있지는 않지만 RSA 공개키 암호의 사용을 권고하고 있다[8]. X.509 표준인증서의 표현형식은 $CA\langle\langle A\rangle\rangle = CA\{V, SN, AI, CA, T_a, A, A_p\}$으로 여기서 $CA\langle\langle A\rangle\rangle$는 인증기관 CA에 의해 발행된 사용자 A의 인증서이고 $CA\{V,...Ap\}$는 CA에 의한 $\{V,...Ap\}$의 서명이다. 서명된 사용자 인증서는 모든 사용자가 접속할 수 있도록 디렉토리에 저장된다. 사용자의 인증서 획득은 상대방의 공개키를 얻기 위해 인증서의 연결(Chain)을 사용하며 이 방법은 두 개의 인증서를 연결하는데 제한될 필요가 없다. 임의로 된 CA의 긴 경로를 따라가면 연결을 생성할 수 있다. 인증기관 X1...Xn이 있고 A와 B간의 인증서획득을 위한 N개의 요소를 가진 연결 표현은 $X_1\langle\langle X_2\rangle\rangle X_2\langle\langle X_3\rangle\rangle \cdots X_n\langle\langle B\rangle\rangle$과 같다. 이 경우 (X_i, X_{i+1}) 연결에 있는 각 쌍은 각각에 대한 인증서를 생성해야 한다. CA ≪A≫는 인증기관 CA(X)에 의해 발행된 클라이언트 A의 인증서이며 CA{버전, 일련번호, 알고리즘 식별자, 발행자, 유효기간, 주체(A), 주체의 공개키}로 정의된다. 클라이언트 A, B가 있고 인증기관 X, Y, Z가 있는 계층구조의 예를 [그림 3]에 표현하였다. 연결된 원은 CA들 사이의 계층적 관계를 나타내며, 연관된 사각형은 각 CA 엔트리에 대하여 디렉토리에 유지되고 있는 인증서들을 나타낸다.



[그림 3] 인증기관의 계층구조

[Fig.3] Structure of CA

A가 B의 공개키를 획득하기 위하여 인증서의 체인 X≪Y≫Y≪Z≫Z≪B≫를 사용하고 동일한 방법으로 B는 역방향 체인 Z≪Y≫Y≪X≫X≪A≫를 이용하여 A의 공개키를 획득한다. 이러한 체인은 두 개의 인증서에 제한되는 것은 아니다. CA Y는 3쌍의 인증서를 보유한다. 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. CA X에 대한 디렉토리 엔트리는 2가지 타입의 인증서를 포함하고 있는데 다른 CA에 의하여 생성된 클라이언트 인증서는 CA이외

의 누구도 검출되지 않고 인증서를 수정할 수 없다는 특성을 가지고 있으며 누구도 위조할 수 없기 때문에 인증서를 보호하기 위한 특별한 장치가 없어도 디렉토리에 배치될 수 있다.

3. 상호인증 기반구조

공개키 기반구조에서 공개키 인증서 획득방식은 계층구조와 비계층구조로 구분한다. 계층구조는 단일 인증경로 보장으로 경로검색이 용이한 반면 전자상거래에는 부적합하며 반드시 최상위 인증기관이 있어야 하는 불합리성과 비밀키 안전성의 문제를 가지고 있다. 네트웍 구조에서의 인증방식으로 비 계층구조인 상호인증(Cross-Certification)방식은 인증기관들 간에 서로 인증서를 발급하는 형태로 인증기관간의 신뢰를 바탕으로 인증이 이루어지며 비밀키 복구가 간단한 반면 단일경로를 보장받지 못함으로 탐색이 복잡하다. 또한 둘 이상의 인증기관들이 인증서를 서로 교환함으로써 신뢰성의 관계를 보다 확장한 방식이다. 따라서 계층구조에서 다양한 조합의 상호인증이 가능하며 상호 인증하는 해당기관 사이에는 상대방의 정책준수가 반드시 보장되어야 한다.

상호인증은 "인증서 체인"이라고 하는 신뢰도를 확인할 수 있는 여러 인증기관을 거치는 동안 검증되어야 할 인증서의 개수로 정의한다. 문제는 대부분의 "인증서 체인"내에 최상위 인증기관이 최소한 반 이상 포함되어 있다는데 있으며 "인증서 체인"이 점차적으로 늘어감에 따라 신뢰도는 점점 떨어져 간다. 이로 인해 "상호인증"에 대한 필요성이 대두되었다. 상호인증은 인터넷 상거래에서 서버 및 클라이언트들간에 디지털인증으로 매우 중요한 기술이며 인증모델은 같은 도메인 내에 있는 CA간 상호인증 모델과 제3의 신뢰기관을 이용한 상호인증모델의 유형이 있다. 인증서 도메인이 같은 경우는 CA가 같은 영역내에서 인증정책 수준을 조정하고 인증절차를 감독한다. 제3의 신뢰기관을 이용한 모델은 상호인증 서비스를 제공하는 CA는 서로간의 호환성 있는 인증정책을 세워야 하며 인증서 저장소가 존재하지 않기 때문에 사용자에게 인증서 분배 시에 상호인증서가 함께 분배되는 것으로 가정한다.

4. 상호인증 메커니즘 설계

네트워크 상에는 자원을 가진 많은 컴퓨터(Server)들과 이들 자원을 이용하는 다수의 사용자(Client)가 있기 때문에 허락된 사용자만이 자원에 접근하도록 하는 절차가 반드시 필요하다.

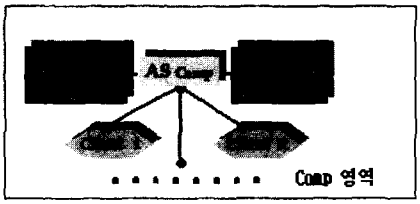
이러한 절차가 안정적으로 동작하기 위해서는 사용자는 자신의 신원확인을 위한 데이터를 인증서버(AS : Authentication Server)에 전송해 주어야 하고 인증서버는 이 데이터를 받고 자신이 인정해준 사용자라는 확인절차를 거치고 확인의 증표로 사용자의 신원정보를 제공해야 한다. 자원을 가진 서버는 인증받은 사용자의 신원증명을 기준으로 자원들에게 할당된 ACL(Access Control List)와 비교하여 사용자에게 자원에 대한 접근을 제어할 수 있다. Client 입장에서는 서버에게 사용자 정보를 제시해야 하고 서버 또한 인증 받은 사용자를 위해서 인증 데이타를 전송해 주어야 한다. 이러한 정보를 전달함에 있어서 보안이 필요하게 되고 이에 AS가 네트워크 상에서 Client, Server, AS 세 통신 주체간에 인증 받은 사용자만이 통신할 수 있도록 기밀성(Confidentiality), 인증(Authentication), 무결성(Integrity)을 제공하여야 한다.

4.1 영역내 사용자 인증

동일 영역에서의 사용자에 대한 인증은 [그림 4]와 같이 Comp영역의 인증서버인 AS_{Comp}와 사용자 신원정보를 저장하는 DB, 공개키 인증서 획득을 위한 디렉토리서버(DS)로 구성된다. Client i는 AS_{Comp}에게 자신의 ID와 서비스 받을 영역을 요청하면 AS_{Comp}는 Client i에 관한 정보를 사용자 데이터베이스에서 검색하여 인증하고 요청한 서비스 영역을 디렉토리서버를 통하여 검색하며 서비스 영역이 동일영역 내에 있으면 영역간 인증은 불필요하다. AS_{Comp}는 인증기관의 역할로 인증서를 발행하며 인증서에는 사용자와 사용자의 공개키가 AS_{Comp}의 비밀키($SKAS_{Comp}$)로 전자서명($SIGSKAS_{Comp}$)되어 공개키 디렉토리에 공개되고 인증서는 각 사용자들에게 발급된다. Client i의 인증서는 $Cert_i$ =($SigSKAS_{Comp}$ (IDi, PK_i))로 AS_{Comp}의 비밀키를 모르면 인증서 위조가 불가능하다. 단지 여기서 AS_{Comp}의 비밀키로 서명된 것

은 인증서 내의 공개키가 위조되지 않았다는 사실만을 강조한다.

① 각 사용자들은 자신의 ID와 공개키(PK)를 생성하여 인증기관인 AS_{Comp}에 등록하고 인증서(CERT)를 발급 받는다. 이 인증서는 X.509에서 정의된 형식을 가지며 AS_{Comp}의 비밀키로 서명되어 있다.



[그림 4] 사용자 인증 서비스

[Fig.4] user authentication process

② Client i는 Client k와의 서비스를 요청한다.
Client i → ASC_{omp} : IDi , IDk

③ AS_{Comp}는 Client k의 공개키 인증서(PK_k)를 반송한다. AS_{Comp} → Client i : $E_{SKASComp}$[Certk]

④ Client i는 Client k의 공개키를 이용하여 nonce와 함께 통신을 요청한다. 여기서 nonce는 임시비표로 timestamp, 카운터, 난수가 사용될 수 있다.
Client i → Client k : E_{PKk}[nonce, ID_i]

⑤ Client k는 AS_{Comp}에게 Client i의 공개키 인증서와 통신을 위한 세션키를 요구한다. Client k는 AS_{Comp}가 그 nonce와 함께 세션키를 보호할 수 있도록 Client i의 nonce를 포함하며 AS_{Comp}의 공개키를 이용하여 보호한다.
Client k → AS_{Comp} : ID_k, ID_i, $E_{PKASComp}$ [nonce]

⑥ AS_{Comp}는 Client k에게 Client i의 공개키 인증서와 세션키(K_S), 정보를 반환한다. 세션키 K_S는 AS_{Comp}에 의해 생성되고 nonce에 결부된 비밀키라는 것과 K_S와 nonce의 결합은 Client i에게 K_S가 투명하다는 것을 보여준다. AS_{Comp}의 비밀키를 사용한 것은 이 메시지가 AS_{Comp}에서 발행된 것이라는 것을 보장하며 Client k의 공개키를 사용한 것은 다른 Entity가 Client i와의 부정한 연결설립을 방지하기 위함이다.
AS_{Comp} → Client k : $E_{SKASComp}$[ID_i, PK_i], E_{PKj}[$E_{SKASComp}$[nonce, K_S, ID_i, ID_k]

⑦ nonce값이 IDi와 함께 항상 포함된 것은 다른 사용자들의 nonce값과 구별하여 Client i에 의해 만들어진 유일하다는 사실을 밝히는 것이다. 즉 [IDi, nonce]는 Client I의 연결을 유일하게 확인하는 짝이다. Client k → Client i : E_{PKi}[$E_{SKASComp}$[nonce, K_S, ID_i, ID_k, nonce2]

⑧ 세션키에 대한 Client i의 지식을 Client k에게 보증한다. Client i → Client k : E_{KS}[nonce2]

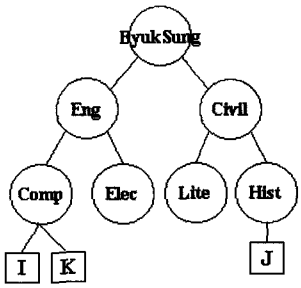
4.2 영역간 상호인증 메커니즘

Client에서 서비스를 요청하면 AS는 서비스 영역을 확인한 후 X.509를 이용하여 서비스를 제공하는 원격영역에 대한 인증 절차는 다음과 같다. Client로부터 세션연결을 위한 요청이 발생할 경우 해당영역의 AS는 자신의 영역에 대한 인증을 하고 원격영역일 경우 경로연결 세션을 설립한다. 원격영역의 서버, 클라이언트에 대한 공개키 인증서를 취득하고 상대방의 공개키로 Client간의 인증이 이루어지며 인증이 확인되면 AS가 세션키를 생성하여 발행하고 서로간의 공개키로 세션키를 교환하여 통신하는 단계이다.

① Client i ---> AS_{Comp} : IDi , R(Remote)
Client i는 R과의 서비스를 요청한다.

Client i가 요청한 영역이 외부영역에 있는 경우 원하는 목적지까지 연결 해주는 경로가 필요하다. 연결경로는 디렉토리 서비스에 의해 경로를 설정하고 DNS에 의해 상대방의 공개키 인증서를 받는다.

[그림 5]는 DS를 이용하여 외부영역에 있는 목적지까지 경로 연결 세션 과정을 도식한 것이다. 즉, Comp영역에 있는 클라이언트가 Hist영역에 있는 서비스를 사용하기 위한 내용으로 Comp영역의 클라이언트는 선인증하여 eng영역과 연결을 한 후 다시 byuksung영역과 연결을 하게 된다. byuksung영역은 civil영역과 연결을 설정한 후 civil의 서브 영역인 Hist와 연결을 하게된다. 각 영역의 Directory server는 단지 연결 설정의 역할만 있을 뿐 인증의 기능은 갖지 않는다.



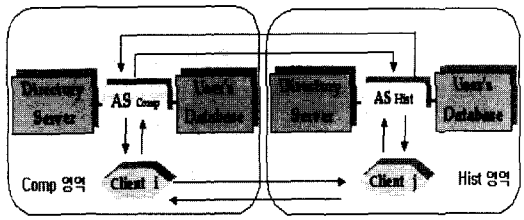
[그림 5] 디렉토리간 연결
[Fig.5] directory Authentication

이제 클라이언트가 있는 영역 즉, Comp영역과 Hist 영역간 연결이 직접적으로 이루어지므로 상호영역간에 있어서 클라이언트를 인증하는 절차를 필요로 하게 된다. 그 이유는 침해자가 서비스를 요청한 클라이언트처럼 가장하여 서비스를 가로채거나 변경시킬 수 있기 때문이다. Comp의 Client는 Hist에 있는 서비스를 이용하기 위한 전방인증서(forward certificate)와 후방인증서(reverse certificate)는 다음과 같다.

② 전방인증서(Comp≪Eng≫Eng≪Byuksung≫Byuksung≪Civil≫Civil≪Hist≫)
후방인증서(Hist≪Civil≫Civil≪Byuksung≫Byuksung≪Eng≫Eng≪Comp≫)

[그림 5]와 [그림 6]에서 Client i는 Hist영역의 AS_{Hist}에게 X.509를 이용하여 획득한 공개키 PK_{AShist}로 인증정보를 암호화하여 전송함으로써 송, 수신측의 통신을 방해하는 침해자로부터 보호할 수 있게 된다. AS_{Hist}는 자신의 비밀키로 수신된 메시지를 복호화한 후에 다시 Client i에게 공개키 PK_i로 메시지를 암호화하여 전송한다. Client i는 자신의 비밀키로 메시지를 복호화하고 Client j와 통신에 필요한 세션키를 요구하여 공통키로 사용하게 된다.

AS와 X.509을 이용하여 [그림 3]에서 다룬 내용을 기반으로 하여 Client i가 Hist영역의 Client j의 서비스를 제공받기 위한 인증정보가 교환되는 알고리즘은 다음과 같다. Client의 인증서 교환단계로 각 영역의 AS들간에 Client의 인증서와 비밀키, 사용자 타입(알고리즘, 인증서버전, PKCS), 통신주체 등을 선인증으로 획득한 상대방의 공개키로 암호화하여 교환한다.



[그림 6] 영역간 인증
[Fig.6] Cross Certification

③ $AS_{Comp} \rightarrow AS_{Hist}$: $E_{PKASHist}[K_{SKAScomp}$, User_Type, ID_j, AS_{comp}<<Client i>>]
④ $AS_{hist} \rightarrow AS_{comp}$: $E_{PKAScomp}$[KSKAShist, User_Type, ID_i, A_{Shist}<<Client j>>]

원격 Client간 상호인증을 위해서 Comp영역의 Client i는 난수(nonce)를 생성하여 ④단계에서 획득한 공개키를 이용하여 전송, 상호간에 검증한다.

⑤ Client I → Client j : $E_{PKj}[ID_i$, nonce]

Client j는 $D_{SKj}[c]$를 해독하여 나온 값 nonce2를 Client i의 공개키로 전송하면 Client i는 값을 비교(nonce=nonce2)하여 검증한다.

⑥ Client j → Client i : $E_{PKi}[ID_j$, t]

상호인증의 종료사실을 AS에게 알리고 비밀통신을 위한 세션키(KS)를 요청한다(⑦). 무결성을 보증하기 위해 처음에 사용한 nonce 값을 포함한다(⑧⑨).

⑦ Client j → AS_{hist} : IDi, IDj, $E_{PKASHist}$[nonce]
⑧ $AS_{hist} \rightarrow$ Client j : $E_{PKj}[E_{SKASHist}$[nonce, K_S, ID_i, ID_B]
⑨ Client j → Client i : $E_{PKi}[E_{SKAScomp}$[nonce, K_S, ID_i, ID_B]
⑩ Client i → Client j : E_{KS}[message]

5. 결론

인터넷의 전자상거래, 응용서비스는 공개키 암호시스템을 바탕으로 구현되어야 사용자의 편리성과 안전성을 보장할 수 있으며 사용자의 공개키를 안전하고 신뢰를 가질 수 있도록 수단을 제공하는 것이 공개키 기반구조이다. 분산환경에서 서버와 클라이언트의 상호인증을 위한 PKI의 구성요소와 X.509 디렉

토리 인증서비스를 고찰하였다. 본 논문에서는 X.509와 DNS를 이용, 체인에 의해 수행되는 PKI 환경에서의 영역간 상호인증 메커니즘을 설계하였다. 영역간 세션연결은 DS를 적용하여 공개키를 획득함으로써 AS가 각 사용자의 공개키를 보관하는 부담이 없으며 각 개체간 신원확인을 위해 인증프로토콜이 적용되었다. 향후 연구과제로써 한번 인증받은 개체는 해당영역의 타 자원서비스를 받기 위해 일정시간 동안 세션키를 허용하는 메커니즘이 필요하다.

※ 참고문헌

[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] 최용락, 소우영, 이재광, 이임영, 통신망 정보보호, 그린출판사, pp.204-211, 365-371, 1996.

[5] 염흥렬, 홍기융."공개키 기반구조", 통신정보보호학회 학회지 제8권 3호.pp.5-18, 9, 1998

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

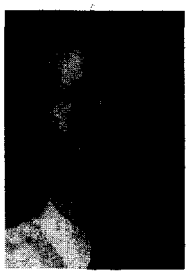
[7] ITU-T Recommendation X.500(1993), ISO/IEC 9594-1:1993, Information Technology-Open Systems Interconnection-The directory : Overview of Concepts, Models and Service, 1993

[8] 김상균, 백종현, 이강석, 이석준, "공개키 인증기반구조로서의 X.509에 대한 연구",통신정보보호학회지, 제8권, 제3호, pp.33-46, 1998

[9] [WOO92a] Woo, T., and LAM, S."Authentication for Distributed Systems." computer, Jan. 1992.

[10] [SIMM92b] Simmons, G. "A Survey of Information Authentication." in [SIMM92b].

신 광 철



1991년~1995년 전쟁연습 프로그램관 및 전산실장 (육군대학)

1995년~1999년 성균관 대학원 정보공학과 수료

1996년~현재 벽성대학 소프트웨어개발전공 교수

관심분야 : 정보보호기술, 객체지향 분석/설계, 전자상거래응용