경로기반 상호인증을 위한 효율적 프로토콜

김 홍 석(金 泓 奭), 박 세 현(朴 世 炫)
중앙대학교 전자전기공학부
전화 : (02) 820-5338 / 팩스 : (02) 825-1584

An Efficient Protocol for the Cross Certification Path Validation

Hongsuk Kim, Sehyun Park
School of Electronics and Electrical Engineering, Chungang University
E-mail : k-airbus@orgio.net

Abstract

With the expansion of E-commerce, Public Key Infrastructure (PKI) solutions are required to resolve Internet security problems. But the certification mechanism for each organization has been independently developed under its own circumstances, so the cooperation of heterogeneous certification mechanisms must be carefully taken into account. In this paper, we propose an efficient protocol for the cross certification based on the path validation. The proposed "cross certification gateway" provides flexibility and convenience with the initial establishment protocol for the cross certification among different certification domains.

I. 서론

전 세계적으로 공개키기반구조(PKI: Public Key Infrastructure)[1]를 이용한 인증체계가 전자상거래와 특정공동체를 위해서, 각국의 정부와 각종 표준화 기구, 기업 및 대학을 중심으로 진행되고 있다. 이러한 표준화 작업은 계층적 구조를 기반으로 PKI를 이용하여, 인터넷상의 데이터 송수신에 무결성(integrity), 기밀성(confidentiality) 및 확실성(authenticity)을 제공하는데 기본 목적이 있다[4]. 이러한 상호인증 과정은 크게 두 가지 단계로 구분된다. 첫 번째는 당사자간의 암호키 교환 및 설정이고, 두 번째는 인증서 전달 방식의 설정이다. 이를 위해 현재 미국, 독일, 대만 등지에서는 ITU-T X.509v3 및 기타 표준을 적용하여 국제적 상호연계를 시도하고 있으며[3], 우리 나라도 국내 PKI규격을 확정함과 동시에 국가간 상호인증을 추진하고 있다[6]. 그러나 각 나라 환경에 맞추어 진행되고 있는 전자서명체계를 차세대 인터넷을 위한 범용표준방식으로 확장하기 위해선, 다음과 같은 사항들이 고려되어야 한다. 즉 단순히 국가간 상호인증 뿐만 아니라, 인터넷 자원과 보안을 위한 새로운 방식의 QoS의 실현이 필요하다. 본 논문은 상호인증 측면에서 유연성과 편의성이 고려된 보안 QoS를 제공하고자 한다. 이를 위해 국가간 상호인증 게이트웨이 및 초기 상호인증 확립 프로토콜을 제안한다.

서론에 이어 2장에서는 IETF의 인증경로를 통한 인증경로 검증절차와 상호인증요구 프로토콜을 소개하였다. 3장은 본 논문의 핵심으로, 기존의 기술이 보다 효과적으로 구현되기 위한 초기 상호인증 확립 프로토콜을 제안한다. 마지막으로 4장에서 이 논문의 결론을 맺는다.

II. 기술 동향

1. IETF PKIX Workgroup의 인증경로 검증절차

IETF에서는 RFC2459(Internet Public Key Infrastructure Certificate & Certificate Revocation List Profile)[1]에서 인증경로 검증절차를 정의하고 있

다. 이것의 목적은 인증된 대상의 DN(Distinguish Name)혹은 대체이름(alternative name)이 그것의 공개키와 제대로 부합되어 있는지를 확인하는 것이다. 다음과 같은 가정으로, 인증서 연쇄(Certificate Chain)를 구성하는 각각의 인증서 정보를 검증한다.

가정1: PKI 계층구조에서 최상위 인증기관인 root CA가 most-trusted CA이다.

가정2: 믿을 수 있는 공개키는 root CA의 자가서명(self-signed) 인증서를 통해 얻을 수 있다. (이것은 보안 서비스를 제공하지 않으나, 검증절차를 간단히 묘사시키고 있다.)

따라서, 유효한 인증서로 판명난 최종 인증대상의 공개키를 믿을 수 있게 된다.

그림 1은 X.509의 인증경로 검증절차를 요약한 순서도이다.

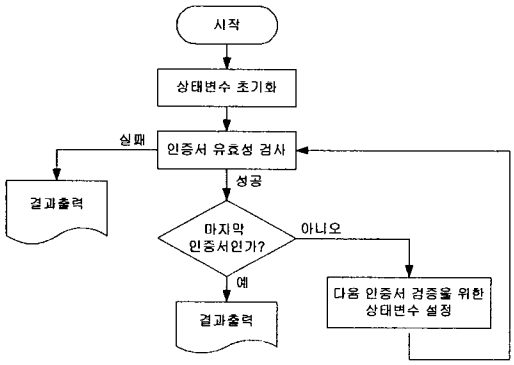

그림 1 X.509 인증경로 검증절차 순서도

2. IETF PKIX Workgroup의 상호인증 요구 프로토콜

RFC2510(Internet Public Key Infrastructure Certificate Management Protocol)[2]은 인증서의 생성 및 관리 운용 전반적 측면에서의 프로토콜 메시지를 규정하고 있다. 주요 PKI 운용 동작(Management Operations)은 다음과 같다.

- CA 제정(초기 CRL 생성 및 공개키 보급)
- 종단 사용자(end entity) 초기화: root CA의 공개키 획득하는 과정 포함
- 인증: 초기 등록 및 인증, 키페어 갱신, 인증서 갱신, CA 키페어 갱신, 상호인증 요구, 상호인증서 갱신
- 인증서 및 CRL의 구현 동작: 인증서 발급, CRL 발행
- 복구 동작: 키페어 복구
- 폐지(revocation) 동작: 폐지 요구
- 개인보안환경(PSE : Personal Security Environment) 관련 동작

위 동작들의 구현은 온라인 프로토콜에 의해서만 이루어지는 것은 아니다. 오프라인 상으로 하드웨어 토큰을 사용한다든지, 또는 그 토큰을 물리적으로 이동시킬 수 있다. 특히, 상호인증을 체결하기 위한 두 CA에서, 인증서를 요구하는 CA가 상호인증서의 인증대상자(subject), 인증서요구에 응답하는 CA가 상호인증서의 발행자(issuer)이다. 양방향 상호 인증을 원한다면 각각 다음과 같은 절차가 서로간에 이루진다.

① 응답할 CA 관리자가 상호인증하기를 원하는 CA를 확인한 다음, 응답 CA 장비에서 인증코드를 생성한다. 응답 CA 관리자는 이 인증코드를 요구 CA 관리자에게 전달한다. 요구 CA 관리자는 온라인 교환을 시작하기 위해 요구 CA 에 인증코드를 등록시킨다.(인증코드는 인증 및 정보의 보존을 위해 사용된다. 이것은 대칭키[symmetric key]기반 인증코드로 생성되며, 모든 메시지 교환에 사용되는 메시지-인증-코드[Message Authentication Codes : MACs]를 생성하기 위해 대칭키가 쓰여진다.)

② 요구 CA는 (요구자의) 임의의 수를 생성하는 것으로 교환을 시작한다. 그후, 요구 CA는 응답 CA에게 상호인증요구(cross certification request : ccr) 메시지를 보낸다. 이 메시지 필드는 인증코드를 기반한 MAC에 의해 임의의 수정이 불가하도록 보호된다.

③ ccr 메시지를 받은 응답 CA는 프로토콜 version을 확인, 요구자의 임의의 수를 저장, 자신의(응답자의) 임의의 수를 생성, MAC을 검증한다. 그리고, 응답 CA 비밀키로 요구 CA 공개키가 담긴 정보를 서명한 후, 새로운 요구자 인증서를 생성한다. 응답 CA는 상호인증응답(cross certification response : ccp) 메시지로 응답한다. 이 메시지 필드는 인증코드를 기반한 MAC에 의해 임의의 수정이 불가하도록 보호된다.

④ ccp메시지를 받은 요구 CA는 자신의 시스템시간과 응답 CA 시스템시간의 차이 정도 확인, 받은 임의의 수의 확인, MAC을 검증한다. 요구 CA는 PKIConfirm 메시지로 응답한다. 이 메시지 필드는 인증코드를 기반한 MAC에 의해 임의의 수정이 불가하도록 보호된다.

⑤ PKIConfirm 메시지를 받은 응답 CA는 임의의 수를 확인, MAC을 검증한다.

III. 초기 상호인증 확립 프로토콜

위에서 소개된 RFC 및 각 나라의 인증운용 표준으로 상호인증을 맺기 위해서는 많은 문제들이 고려되어야 한다. 두 개의 이질적인 인증체계 영역을 통해 생성된 인증경로가 유효하게 검증되려면, 이를 구성하는 인증서 X.509v3의 기본영역 및 확장영역의 항목들(예 : 보

안정책 및 여러 제한)이 연쇄 확인 절차로 이루어져야 한다. 본 논문에서는 이와 같은 구체적 경로기반 검증에 관련된 사항을 제외하였고, 보다 효과적인 국가간 상호인증 체결을 위한 초기 상호인증 확립 프로토콜에 그 초점을 두었다. RFC2510에서 제안된 방법은 상호인증 과정의 응답 CA가 요구 CA를 확인한 뒤, 요구 CA에게 인증코드를 전달하여 등록시키게 함으로써 그 프로토콜이 시작된다. 이 방법은 대칭키 암호기법을 사용하여 키교환 및 인증정책이 교환되므로 컴퓨팅 파워에 장점이 있는 반면, 응답 CA와 요구 CA가 같은 인증체계 영역 안에서 서로 믿을 수 있다는 가정을 두었다. 이질적인 인증체계 영역에 있는 CA간에 서로 확인할 수 있는 가장 좋은 방법은 요구 CA의 바로 상위 CA가 발급하는 인증서를 경로기반 하에 검증하는 것이다. 이러한 검증은 응답 CA의 인증영역 체계 내에 역방향 인증서가 존재하는 것을 가정하고, 또 최상위 인증기관끼리 상호인증이 이루어질 때만 가능하다.

본 논문에서는 이에 대한 개선책을 제시하기 위해서 그림 2와 같은 시나리오를 고려하고자 한다.

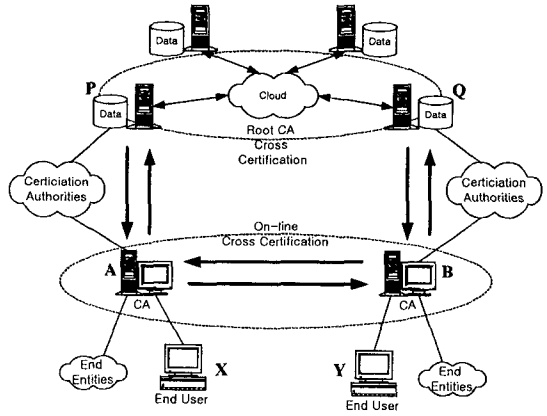

그림 2 효율적인 상호인증을 위한 시나리오

그림 2에서 Y가 X에게 어떠한 일련의 통신을 시작하려면, Y는 X에게 자신의 인증체계를 통한 내부 인증서(B<<Y>>)를 첨부하여 보내야 한다. X가 B<<Y>>를 받게 되면 B의 전자서명을 검증하기 위해 자신의 인증체계를 통한 인증경로기반 인증서 검증을 하여야 한다. 이미 root CA끼리(P와 Q)는 상호인증을 하였다고 가정하더라도, A가 상위 CA와 역방향 인증을 하지 않았다면 경로기반에 의한 인증서 검증이 이루어지지 않는다. 그러므로 종단 사용자를 인증하는 CA간(A와 B)에 on-line 상호인증을 맺으면 인증서 연쇄(Certificate chain)를 최소화하면서 이질적인 인증체계 영역이라도 경로기반 인증서 검증을 할 수 있게 된다.

본 논문에서는 A가 B에 대한 상호인증서를 생성하여 자신의 인증체계 영역 디렉토리에 저장하기 위한 과정을 위해, 다음과 같은 가정을 세웠다.

가정1: 서로 다른 인증체계 영역의 최상위 root CA간, 구체적인 보안 정책의 합의가 이루어져 있는 상태 하에 root CA가 직접 관리하는 국가간 상호인증 게이트웨이(제한된 CA만이 접근 가능)가 설치되어 있다.

가정2: 이질적인 인증체계 영역에 보내질 종단사용자의 인증서 확장영역은 두 인증체계가 허용하는 보안정책을 벗어나지 않는다.

가정3: 국가간 상호인증 게이트웨이에 쓰이는 키페어의 공개키는 root CA들 만이 공유하고 있다.

본 논문에서 제시하는 초기 상호인증 확립을 위한 프로토콜을 위해 다음과 같은 표현이 사용되었다.

- ID_X : X의 ID
- $K_{U<A>}$: 내부 인증체계에 사용되는 A의 공개키
- $K_{R<A>}$: 내부 인증체계에 사용되는 A의 비밀키
- $K_{U<A>'}$: 상호인증에 쓰이는 A의 공개키
- $K_{R<A>'}$: 상호인증에 쓰이는 A의 비밀키
- E[{C},D] : key D를 이용한 C의 암호화
- Sig[{C},D] : key D를 이용한 C의 디지털 서명
- A<<X>> : X의 $K_{U<X>}$가 포함된 인증정보를 A의 $K_{R<A>}$로 전자서명한 인증서
- A'<<X>> : X의 $K_{U<X>}$가 포함된 인증정보를 A의 $K_{R<A>'}$로 전자서명한 인증서
- A<<X'>> : X의 $K_{U<X>'}$가 포함된 인증정보를 A의 $K_{R<A>}$로 전자서명한 인증서
- Ni : 상호인증확립을 시작하는 CA가 생성한 nonce (replay attack 방지)
- Nr : 상호인증확립에 응답하는 CA가 생성한 nonce (replay attack 방지)
- ccr_A_B : A와 B의 상호인증을 요구하는 메시지

과정은 다음과 같다.

(1) X→A : ID_X||ccr_A_B
A→X : ID_A||ack (agree or deny)

(2) A→B : ID_A||ccr_A_B
B→A : ID_B||ack (agree or deny)

(3) A→P : ID_A || E[{ $K_{U<A>'}$||Ni||ID_B|| Sig[{$K_{U<A>'}$||Ni||ID_B},$K_{R<A>}$] }, $K_{U<P>}$]

(3)'B→Q : ID_B || E[{ $K_{U<B>'}$||Nr||ID_A|| Sig[{$K_{U<B>'}$||Nr||ID_A},$K_{R<B>}$] }, $K_{U<Q>}$]

(4) P→Q : E[{ ID_A||$K_{U<A>'}$||Ni||ID_B|| Sig[{ID_A||$K_{U<A>'}$||Ni||ID_B},$K_{R<P>'}$], $K_{U<Q>'}$]

(4)'Q→P : E[{ ID_B||$K_{U<B>'}$||Nr||ID_A|| Sig[{ID_B||$K_{U<B>'}$||Nr||ID_A},$K_{R<Q>'}$], $K_{U<P>'}$]

(5) P→A : E[{ ID_B||$K_{U<B>'}$||Nr||ID_A||Ni|| P<<A'>> }, $K_{U<A>'}$]

(5)'Q→B : E[{ ID_A||$K_{U<A>'}$||Ni||ID_B||Nr|| Q<<B'>> }, $K_{U<B>'}$]

(6) B→A : E[{ ID_A||Ni }, $K_{U<A>'}$]

(6)'A→B : E[{ ID_B||Nr }, $K_{U<B>'}$]

과정 (1)처럼 종단사용자가 프로토콜을 개시하며 할 수도 있지만, (2)에서와 같이 필요에 따라 CA부터 시작될 수 있다. 그리고 초반에 메시지가 암호화 되지 않고 간단한 내용이 교환되므로, DOS(Denial Of Service)공격에 대해 좀 더 자유로워질 수 있다.

과정 (2)가 성공적으로 끝나면 A와 B는 상호인증에 사용될 새로운 키페어를 생성한다[3]. (키페어는 사전에 준비되어질 수 있다.)

과정 (3)을 통해 A의 인증체계 영역 내 국가간 상호인증 게이트웨이에 접근하여 P<<A'>>를 생성할 정보를 P에게 넘겨주고, (4)에서 P는 B가 B'<<A>>를 생성할 수 있도록 Q에게 해당 정보를 전달한다. B쪽에서도 (3)',(4)'와 같은 순서로 상호인증 게이트 웨이에 접근하여 Q<<B'>> 및 A'<<B>> 생성을 위한 정보를 넘겨준다. 이 과정에서 B는 A가 P의 인증체계의 일부임을 인증할 수 있고, A 또한 B가 Q의 인증체계 중 하위임을 알 수 있게 된다. 이는 P와 Q가 서로 믿고 있다고 가정함으로써 가능하다.

과정 (5)에서 A는 P가 발행한 P<<A'>>를 받고, B의 공개키를 인증하는 A'<<B>>를 발행하기 위한 정보를 얻는다. 과정 (6)을 통해, A가 생성했던 nonce를 B로부터 되돌려 받아 A'<<B>>를 생성하는 것으로 상호인증을 성공적으로 완료한다. B는 (5)',(6)'을 통해 최종적으로 B'<<A>>를 생성하게 된다.

기존의 방법으로는 서로 다른 인증체계 영역간에 안전한 상호인증을 확립할 수 없다. 따라서 본 논문에서는 기존의 상호인증 확립을 위해 상대방 CA의 확인절차를 실제로 실현하여, 경로기반 검증작업을 최소화하였다.

P<<A'>>A'<<B>>B<<Y>> 식(1)

식(1)은 본 논문에서 제시한 상호인증서를 이용하여 종단사용자 X가 Y를 인증하는 경로를 표현한 것이다. 이 방법의 장점은 역방향 인증서 없이도 두 종단사용자가 매우 간단하게 경로기반에 입각한 상호인증을 검증할 수 있게 되며, 상호인증의 구체적 보안정책 제한을 CA 및 종단사용자가 합의하에 결정할 수 있다.

표 1은 본 논문에서 제안한 상호인증 프로토콜과 RFC2510을 비교한 것이다.

표 1. 국가간 상호인증확립의 경우에 대한 프로토콜 비교

	제안된 프로토콜	RFC2510
암호화 방식	Public-key	Shared Key
메시지 인증 방식	Digital Signature	MAC
상대 CA 확인절차	초기 상호인증 확립과 동시에 수행되므로 매우 간단함	가정으로 두었음
경로기반 검증시 필요한 인증서 갯수	Constant (=3)	Variable(>=3)

IV. 결론

본 논문에서는 국가간 상호인증 게이트웨이를 통해, 종단사용자를 관리하는 CA끼리 직접 상호인증을 맺는 방법을 제안하였다. 종단사용자 측면에서는 인증경로가 짧아져 사용자의 부담을 줄였고, 보안측면에서는 root CA의 자가서명을 이용하여 상호 인증이 인증되기 때문에 자신의 인증체계 영역이 안전하다면 종단사용자가 믿고 사용할 수 있다. 그리고 국가간 상호인증 게이트웨이의 공개키는 상호인증이 합의된 root CA들만이 공유하므로 불특정 다수로부터 공격당할 확률을 현저히 줄일 수 있다.

참고문헌(또는 Reference)

[1] Housley, R., Ford, W., Polk, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", IETF RFC2459, January 1999.

[2] Adams, C. and S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocol", IETF RFC2510, March 1999.

[3] "Cross Certificate Guideline (alpha version)", ECom, June 1998.

[4] B. Clifford Neuman, "Security, Payment, and Privacy for Network Commerce", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 13 NO. 8, OCTOBER 1995, p1523-1531.

[5] William Stallings, "Cryptography And Network Security", Prentice Hall, 1999.

[6] 전자서명 인증관리센터 homepage, http://www.rootca.or.kr