인증서 검증서버의 인증경로 생성

노종혁, 김태성, 원형석, 진승헌

한국전자통신연구원 인증기반연구팀

jhroh, jinsh@etri.re.kr

Building Certification Paths in Certificate Validation Server

Jong Hyuk Roh, Taesung Kim, Hyungsuk Won and Seunghun Jin

ETRI Certification Infrastructure Research Team

요 약

PKI에 필수적인 요소인 인증서 검증에 있어 인증서 검증서버인 ETRI/VA는 인증서의 상태 검증의 적시성을 제공하고 인증경로 생성 및 검증에 대한 클라이언트의 부담을 줄이며, PKI 상호연동을 지원하고 도메인간의 인증서 정책을 중앙집중 관리한다. 본 논문은 ETRI/VA에서의 신속하고 효율적인 인증경로 생성 방법을 제안하였다. 인증기관 인증서로 이루어진 인증경로를 미리 생성하고 저장하여 사용함으로써 검증 요청시 빠르게 인증경로를 생성할 수 있고, 요청에 의해 생성된 인증경로를 저장하여 이후 동일한 검증대상 인증서의 검증시 기 저장된 인증경로를 재사용하게 함으로써 효율적으로 인증경로를 생성한다.

1. 서론

정보보호를 위해 공개키 암호 시스템(Public Key Cryptography System)과 공개키(Public Key)에 대한 인증서를 기반으로 보안 메커니즘을 제공하는 기반 구조인 PKI (Public Key Infrastructure)에 대하여 많은 연구가 진행되고 있다. PKI가 정보보호 핵심 기반구조로 활용되면서 PKI 시장의 규모가 팽창되고 있지만, PKI에는 앞으로 해결해야 할 문제를 여러 가지 안고 있으며, 그 중 인증서에 대한 상태 검증과 인증경로 검증을 들 수가 있다. PKI간 상호연동이 요구되는 현 시점에서, 인증서 상태 검증의 적시성 제공 및 타 도메인의 인증서 검증은 필수불가결한 상황이다.

인증서 검증은 인증경로 생성과 인증경로 검증, 두가지 작업으로 나뉠 수 있다. 인증경로 생성은 클라이언트가 신뢰하는 인증기관의 인증서로부터 검증하고자 하는 인증서까지의 인증서 체인을 생성하는 것이고, 인증경로 검증은 인증서 체인에서 대상 인증서 안에 있는 소유자의 identity, 소유자의 공개키, 소유자의 특성들 간의 binding 등을 검증하는 것이다. 인증경로 생성을 위해서는 인증서 체인에 필요한 인증기관의 인증서를 수집하여야 하고, 인증경로 검증을 위해서는 인증서의 상태 검증이 요구된다. 현 PKI에서는 이러한 작업들이 PKI 클라이언트에서 이루어지고 있는데 무선 PKI에 대한 연구가 활발해 지고 있는 지금 인증경로의 생성과 인증경로 검증은 무선 단말기에 많은 부담을 안겨주고 있다. 이러한 문제들을 해결하기 위해 많은 연구가 이루어지고 있으며, IETF PKIX 워킹그룹에서는 OCSP(Online Certificate Status Protocol)[2], SCVP (Simple Certificate Validation Protocol) [3] 등을 제안하고 있다. 이러한 기술은 검증과 관련된 기반 기술임에는 틀림없지만 실제 적용을 위한 관리 메커니즘과 운영 메커니즘은 제시하지 않고 있다.

인증서 검증서버 ETRI/VA는 인증서의 상태 검증의 적시성을 제공하고 인증경로 생성 및 검증에 대한 클라이언트의 부담을 줄이며, PKI 상호연동을 지원하고 도메인간의 인증서 정책을 중앙집중 관리할 수 있다. 본 논문에서는 ETRI/VA에서 사용되는 인증경로 생성 방법에 대하여 기술하고 있다. ETRI/VA의 인증경로 생성은 클라이언트의 요청에 빠른 응답을 지원하기 위하여 인증기관 인증경로를 미리 생성하고, 요청에 의해 생성된 인증경로를 재사용함으로써 ETRI/VA의 효율을 높인다.

본 논문의 구성은 다음과 같다. 2 장에서는 인증경로 생성과 인증경로 검증에 대한 개요 및 기술에 대하여 설명하고, 3 장에서는 ETRI/VA와 인증경로 생성에 대하여 기술한 후, 4 장에서 결론을 맺는다.

2. 인증서 검증 기술

인증서 검증 기술은 인증경로 생성과 인증경로 검증으로 이루어져 있다. 인증경로란 검증자가 신뢰하는 지점(Trust Point)의 인증서로부터 검증 대상이 되는 인증서까지의 인증서 체인을 의미한다. 즉, 상위 인증서의 소유자(subject)가 하위 인증서의 발행자(issuer)가 되며, 인증서 체인의 마지막 인증서가 인증서 검증의 대상이 된다. 인증경로 검증이란 인증경로상의 모든 인증서의 유효성을 검증하는 절차를 말하며, 이를 통하여 상대방의 인증서를 신뢰할 수 있게 된다. 인터넷 기술의 표준화를 담당하는 IETF에서는 PKI 인증경로 검증 절차는 X.509 의 12.4.3 절에 근거를 두고 있다[1].

일반적으로 인증경로 생성은 복수개의 인증기관이 운영되는 배타적 환경에서 서로의 영역을 유지하며 확장성을 지원하여야

한다. 복수개의 인증 기관들은 서로간의 확장성을 지원하기 위해 계층 구조, 상호 인증 구조 등의 다양한 신뢰 모델(Trust model)을 따르고 있다[5]. 신뢰 모델은 PKI의 전체 구조를 결정하는 사안으로, 향후 국제 연동에 대한 준비가 필요하며, 각 모델에 관련된 인증경로 검증 기술이 요구되고 있다. 신뢰 모델은 계층 구조, 상호 인증 구조, Bridge CA 구조, 신뢰 리스트 등으로 구분된다.

인증경로 생성은 인증서 검증자가 신뢰하는 지점의 인증서에서 시작하여 검증 대상 인증서까지의 인증경로를 생성하는 reverse 방법과 검증 대상 인증서로부터 시작하여 신뢰하는 지점의 인증서까지 인증경로를 생성하는 forward 방법이 있으며, 두 방법을 혼용하여 사용하는 방법이 있다. 효율적인 방법의 선택은 PKI의 신뢰 모델에 의존적이다. 또한 인증경로를 생성하며 인증경로 검증을 동시에 수행하는 방법도 있는데, 이 경우는 forward 방법보다 reverse 방법이 보다 효율적이다[6].

인증경로 검증은 대상 인증서 안에 있는 소유자의 identity, 소유자의 공개키, 소유자의 특성들 간의 binding을 검증하는 것이다. 인증경로는 검증자가 신뢰하는 지점의 인증서로부터 시작되어야만 하며, 인증경로가 검증되기 위해서는 아래 사항들을 만족하여야 한다[1,5].

- 인증경로의 첫번째 인증서는 신뢰 기관에서 발행해야 한다.
- 인증경로의 마지막 인증서는 검증 대상의 인증서야 한다.
- 발행자와 소유자의 이름이 체인을 이루어야 한다. 즉, 첫번째 인증서와 마지막 인증서를 제외한 모든 인증서에서는 상위 인증서의 소유자가 다음 순서인 인증서의 발행자이어야 한다.
- 인증경로의 모든 인증서는 요구되는 시간에 유효하여야 한다.

그러나 위의 조건은 필요 조건일 뿐 인증경로가 완전히 검증되기 위해서는 기본 제한(basic constraints), 명칭 제한(name constraints), 정책 제한(policy constraints) 등이 고려되어야 한다.

다음은 인증경로 검증의 절차를 나타낸다.

1. 초기화(Initialization)
2. 인증서 검증(Basic certificate checking)
3. 인증경로에서의 다음 인증서 준비(Preparation for the next certificate in the sequence)
4. Wrap-up

위 네 단계 중 1, 4 단계는 각 한번씩 만 수행되고 단계 2는 인증경로의 모든 인증서 마다 수행된다. 단계 3은 대상 인증서인 마지막 인증서를 제외한 모든 인증서에 대해 수행된다[5].

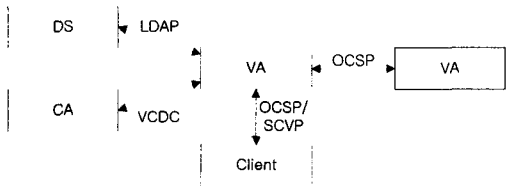
인증서 검증에 관련된 프로토콜로 OCSP와 SCVP가 있다. OCSP는 인증서 검증에 필요한 인증서의 상태정보를 제공하기 위한 프로토콜로써 기존에 사용되고 있는 CRL(Certificate Revocation Lists)의 크기 문제뿐만 아니라 검증 정보에 적시성을 제공할 수 있다[2,3]. 현재 IETF PKIX 워킹그룹에서 버전 2가 draft 상태이며, 실시간 인증서 검증 서비스인 ORS (Online Revocation Status) 뿐만 아니라 인증경로 생성을 위한 DPD(Delegated Path Discovery), 인증경로 검증을 위한 DPV(Delegated Path Validation)에 관한 연구가 진행중이다[3]. OCSP는 CRL이 가지고 있는 한계적인 문제점들을 해결할 수 있지만 각 응답마다 서명을 해야 하는 부담과 요청이 많아 졌을 경우에 발생하는 OCSP Server의 부담, DOS(Denial of Service) 공격에 대한 취약성은 문제로 지적되고 있다.

인증경로 검증 서비스를 제공하기 위한 프로토콜로 IETF PKIX 워킹그룹에 현재 draft 상태인 SCVP가 있다. 검증 서비스를 제공하는 SCVP 서버는 클라이언트가 인증경로 검증을 수행하는데 필요한 정보를 제공하는 untrusted SCVP 서버와 인증경로 생성에서 검증까지 모든 서비스를 제공하는 trusted SCVP 서버로 구분하고 있다. Trusted SCVP 서버는 클라이언트의 검증에 대한 부담을 줄이고 PKI 검증 정책을 중앙관리 할 수 있도록 되어 있다[4]. OCSP 서버와 마찬가지로 서명에 대한 부담, 요청이 급증할 때 서버의 오버헤드 등의 단점을 가지고 있다.

3. ETRI/VA의 인증경로 생성

본 장에서는 클라이언트의 인증경로 검증에 대한 부담을 줄이고 통합적인 정책 관리를 위한 ETRI/VA에서의 인증경로 생성 방법에 대하여 기술한다.

ETRI/VA는 클라이언트의 인증경로 검증을 대행해 주는 시스템으로, 클라이언트는 인증경로 검증에 대하여 VA를 신뢰한다. VA는 인증경로를 생성하고 인증서 상태를 실시간으로 검증하고 다른 VA와 CA들과의 연동을 통하여 인증경로 전체를 검증하는 서비스를 제공한다. 이는 다양한 신뢰 모델에 대해서 독립적으로 인증경로 검증을 제공하므로 향후 국제 PKI 연동에도 활용될 수 있다.



[그림 1] ETRI/VA model

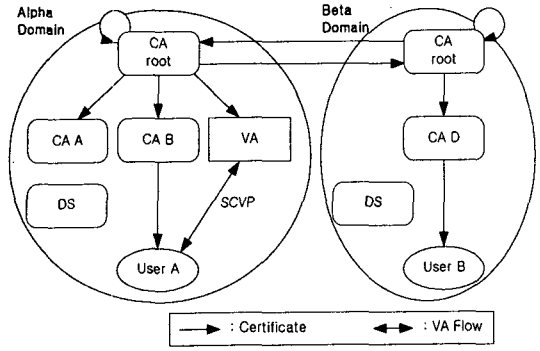
3.1 ETRI/VA

클라이언트는 하나의 VA를 Trusted Anchor로 하여 인증경로 검증에 관련된 모든 작업에 관하여 VA만을 신뢰하고 서비스를 요구한다. VA는 클라이언트가 요구한 검증 대상 인증서를 검증하기 위하여 클라이언트가 신뢰하는 신뢰 지점으로부터 검증 대상 인증서까지의 인증경로를 생성하고 인증경로 상의 각 인증서의 상태 정보를 검증하여 인증경로 검증 작업을 수행한다. 신뢰하고 있는 VA가 인증경로상의 인증서에 대한 상태 정보를 검증하지 못하는 경우는 VA가 신뢰하는 다른 VA나 디렉토리 서버로 정보를 요청하고 서비스를 제공 받을 수 있다. VA는 CA 간의 인증 관계와는 무관하므로 신뢰 모델에 독립적으로 신속한 정책 반영이 가능하고 복잡성을 최소화 한다.

3.2 인증경로 생성

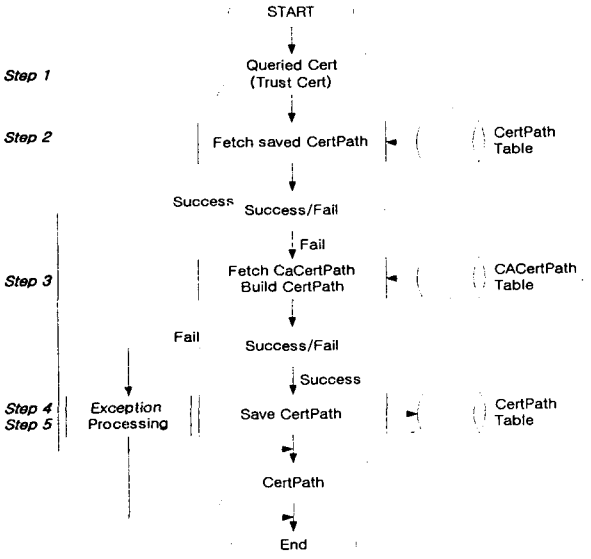
ETRI/VA는 클라이언트의 요청에 대한 신속한 응답을 지원하고 효율을 높이기 위해 인증기관 인증서로 이루어진 인증경로를 미리 생성하여 저장한다. 검증서버가 지원하는 도메인이 확장됨에 따라 도메인에 속하는 인증기관의 인증서를 수집하고, 수집한 모든 인증기관 인증서의 소유자의 이름과 발행자의 이름으로 지원하는 도메인 내에서 생성될 수 있는 모든 인증기관 인증서 인증경로를 생성하고 저장한다. 인증경로를 생성한 후 인증경로 검증 작업을 수행하여 유효하지 않은 인증경로는 제거한다. 이는 클라이언트의 요청으로 인증경로를 생성과 인증경로 검증시 보다 신속하게 처리할 수 있게 한다.

PKI 도메인이 그림 2와 같이 구성되어 있을 때, 검증서버는 각 도메인에 속하는 모든 CA로부터 인증서를 수집한다. CA의 인증서는 셀프사인, 크로스 인증서 등이 있을 수 있으며 검증서버가 신뢰하는 인증기관의 인증서에서 시작되는 모든 인증경로를 생성한다. 인증경로 생성시 인증경로에 같은 인증서가 중복되지 않도록한다.



[그림 2] PKI 도메인

또한, 클라이언트의 요청으로 생성된 인증경로는 저장을 하여 다른 인증서 검증 요청에 재사용할 수 있다. 인증경로를 생성하기 위한 알고리즘은 아래 그림 3 과 같다.



[그림 3] 인증경로 생성

검증서버가 클라이언트로부터 인증서 검증 요청을 받게 되거나 또는 인증경로 생성을 요청 받을 시, 검증서버는 클라이언트로부터 수신한 검증대상 인증서(Queried Cert)와 선택적으로 클라이언트가 신뢰하는 인증서를 수신하게 된다(Step 1). 검증서버는 기 저장된 인증경로 테이블(CertPath Table)에서 클라이언트의 요청으로 생성될 수 있는 인증경로를 수집한다(Step 2). 기 저장된 인증경로에 요청에 합당한 인증경로가 없을 경우, 기 저장된 인증기관 인증경로 테이블(CACertPath Table)에서 해당 검증대상 인증서에 합당한 인증경로를 선택하고, 검증대상 인증서와 인증경로를 연결하여 요구되는 인증경로를 생성한다(Step 3). 인증경로 생성이 성공하는 경우, 다음 요청을 위하여 생성된 인증경로를 인증경로 테이블에 저장한다(Step 4). 인증경로 생성을 실패한 경우, 검증서버는 실패 처리를 수행하고 그 결과에 대한 로그 및 그 응답을 생성한다(Step 5).

클라이언트의 요청시 검증대상 인증서 외에 클라이언트가 신뢰하는 인증서와 검증에 사용할 인증서 정책을 제공할 수 있다. 신뢰하는 인증서가 제공되면 검증서버는 인증경로 생성시 반드시 제공된 인증서부터 시작하는 인증경로를 생성하여야 하고, 신뢰하는 인증서가 제공되지 않는 경우에는 검증서버가 관리하는 신뢰 인증기관 리스트에 등록된 인증기관의 인증서부터 시작하는 모든 인증경로를 생성한다.

4. 결론

ETRI/VA는 인증서의 상태 검증의 적시성을 제공하고 인증경로 생성 및 검증에 대한 클라이언트의 부담을 줄이며, PKI 상호연동을 지원하고 도메인간의 인증서 정책을 중앙집중 관리함으로써, 다양한 신뢰 모델에 대해서 독립적으로 인증경로 검증을 제공하므로 향후 국제 PKI 연동에도 활용될 수 있다.

본 논문은 인증서 검증서버인 ETRI/VA에서 클라이언트로부터의 인증서 검증 요청에 효율적으로 대응하기 위한 인증경로 생성 방법을 제안하였다. 클라이언트의 요청을 신속하게 처리하기 위하여 인증기관 인증서로 이루어진 인증경로를 미리 생성하여 저장해 두며, 기존에 생성한 검증대상 인증서의 인증경로를 저장하여 이후 동일한 검증대상 인증서의 검증시 기 저장된 인증경로를 재사용함으로써 인증경로 생성을 효과적으로 수행할 수 있게 하였다.

참고문헌

[1] R. Housley, W. Ford, W. Polk and D. Solo, "Internet X.509 Public Key Infrastructure, Certificate and CRL Profile," RFC 2459, January 1999.

[2] M. Myers, R. Ankney and A. Malpani, S. Galperin, C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP," RFC 2560, June 1999.

[3] M. Myers, R. Ankney, C. Adams, S. Farrell and C. Covey, "Online Certificate Status Protocol, version 2," draft-ietf-pkix-ocspv2-02, March 2001.

[4] A. Malpani, P. Hoffman and R. Housley, "Simple Certificate Validation Protocol (SCVP)," draft-ietf,-pkix-scvp-09, June 2000.

[5] R. Housley, T. Polk, *Planning for PKI*, John Wiley & Sons, 2001.

[6] Y. Elley, A. Anderson, S. Hanna, S. Mullan, R. Perlman, S. Proctor, "Building Certification Paths: Forward vs. Reverse," *Network and Distributed System Security Symposium Conference Proceedings*, 2001.