Collaborative VA 모델

노종혁* 김태성* 최대선* 진승헌* 정교일**
한국전자통신연구원 *인증기반연구팀 **정보보호기반연구부

Collaborative VA Model

Jong Hyuk Roh*, Taesung Kim*, Daeseon Choi*, Seunghun Jin* and Kyo Il Chung**
ETRI, *Certification Infrastructure Research Team **Information Security Basic Department

요 약

정보보호 분야의 핵심 기술인 PKI는 전자정부 및 전자상거래 전반의 응용 환경에서 정보보호의 기반구조로서 그 활용의 폭을 더욱 넓혀가고 있으며, 현재 유선 인터넷 환경을 기반으로 구성되어진 PKI는 무선 인터넷 환경의 정보보호 기반구조로 그 영역을 더욱 확장해 나가고 있다. 본 논문은 이러한 PKI에 필수적인 요소인 인증 경로 검증에 효율적으로 대응하고 확장성을 지원하기 위하여 Collaborative ETRI VA를 제안하였다. ETRI VA는 클라이언트의 인증 경로 검증에 대한 부담을 줄이고, 신뢰 모델에 영향을 받지 않고 검증을 수행하며, 중앙집중적으로 신속하게 정책을 반영할 수 있게 한다.

1. 서론

인터넷을 통한 전자상거래가 급격히 확산됨에 따라 정보보호에 대한 필요성이 증대되고 있다. 최근, 이러한 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 관한 많은 연구가 진행되고 있으며, 정보보호 핵심 기반구조로 활용되면서 PKI 시장의 규모가 급격히 팽창되고 있다. 그러나 PKI에는 앞으로 해결해야 할 문제를 여러 가지 안고 있으며, 그 중 인증서에 대한 상태 검증과 인증 경로 검증을 들 수가 있다. 현재 인증서의 상태 검증은 주로 CRL(Certificate Revocation Lists)에 의존하고 있다. 그러나, CRL은 사용자 수의 증가에 따라 크기가 계속적으로 증가하는 것에 대한 관리 문제와 검증 시점의 인증서 상태 정보를 지원할 수가 없다는 문제가 있다. 또한, 현 PKI에서는 인증 경로의 구축과 인증 경로의 검증은 PKI 클라이언트에서 이루어지고 있는데, 무선 PKI에 대한 연구가 활발해 지고 있는 지금 인증 경로의 생성과 인증 경로 검증은 무선 단말기에게 부담을 안겨주고 있다. 이러한 문제들을 해결하기 위해 많은 연구가 이루어지고 있으며, IETF PKIX 워킹그룹에서는 OCSP(Online Certificate Status Protocol), SCVP (Simple Certificate Validation Protocol) 등을 제안하고 있다. 이러한 기술은 검증과 관련된 기반 기술임에는 틀림없지만 실제 적용을 위한 관리 메커니즘과 운영 메커니즘은 제시하지 않고 있다.

본 논문에서는 인증서의 상태 검증의 적시성을 제공하고 인증 경로 생성 및 검증에 대한 클라이언트의 부담을 줄이기 위해 Collaborative ETRI VA(Validation Authority)를 제안한다. ETRI VA는 OCSP Responder, SCVP Server의 기능을 지원하여 표준을 준용하고, 다양한 신뢰 모델에 대해서 독립적으로 인증 경로 검증을 제공하므로 인증서 검증에 대한 중앙집중관리를 가능하게 하며 클라이언트의 부담을 최소화 할 수 있다.

본 논문의 구성은 다음과 같다. 2 장에서는 인증 경로 구축과 인증 경로 검증에 대한 개요 및 방법에 대하여 설명하고 3 장에서는 ETRI VA 기본 모델 및 시스템 구조에 대하여 기술한 후, 4 장에서 결론을 맺는다.

2. 인증서 검증 기술

인증서 검증 기술은 인증 경로 구축과 인증 경로 검증으로 이루어져 있다. 인증 경로란 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. 인증 경로 검증이란 인증 경로상의 모든 인증서의 유효성을 검증하는 절차를 말하며, 이를 통하여 상대방의 인증서를 신뢰할 수 있게 된다. 인터넷 기술의 표준화를 담당하는 IETF에서는 PKI 인증 경로 검증 절차는 X.509 의 12.4.3 절에 근거를 두고 있다[1].

일반적으로 인증 경로 구축은 복수개의 인증기관이 운영되는 배타적 환경에서 서로의 영역을 유지하며 확장성을 지원하여야 한다. 복수개의 인증 기관들은 서로간의 확장성을 지원

하기 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 인증 경로 검증 기술이 요구되고 있다. 신뢰 모델은 계층 구조, 상호 인증 구조, Bridge CA 구조, 신뢰 리스트 등으로 구분된다.

인증 경로 검증은 대상 인증서 안에 있는 소유자의 identity, 소유자의 공개키, 소유자의 특성 들간의 binding을 검증하는 것이다. 인증 경로는 검증자가 신뢰하는 지점의 인증서로부터 시작되어야만 하며, 인증 경로가 검증되기 위해서는 아래 사항들을 만족하여야 한다.

- 인증 경로의 첫번째 인증서는 신뢰 기관에서 발행해야 한다.
- 인증 경로의 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.
- 인증 경로의 모든 인증서는 요구되는 시간에 유효하여야 한다.

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

다음은 인증 경로 검증의 절차를 나타낸다.

1. 초기화(Initialization)
2. 인증서 검증(Basic certificate checking)
3. 인증 경로에서의 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 인증 경로의 모든 인증서 마다 수행된다. 단계 3 은 대상 인증서인 마지막 인증서를 제외한 모든 인증서에 대해 수행된다.

인증 경로 검증 과정에는 인증 경로의 각 인증서들이 유효한지, 폐기되었는지 등을 판단하는 단계가 필요하다. 대부분의 PKI에서 인증서 상태 검증을 위하여 CRL을 사용하고 있다. CRL은 신용카드의 hot list처럼 폐기된 인증서의 리스트로 구성된다. CRL은 일정 주기마다 갱신을 하며, 각 CA 마다 root 인증서에 대한 하나의 CRL을 유지하며 root 인증서가 폐기될 때까지 CRL은 축적된다. 이로 인해 CRL은 데이터 크기에 대한 overhead가 문제가 되고 있고 실시간으로 인증서의 상태 검증은 불가능 하다. 이러한 문제를 해결하기 위하여 CRL DP, Delta CRL, CRT, OCSP 등이 제안되었다.

CRL DP(Distribution Points)는 CRL 정보를 mini CRL이라 불 수 있는 여러 개의 bucket으로 나누어 저장한다. 인증서가 폐기 되는 경우, 폐기 정보를 얻어 올 수 있는 위치, 즉 buclket의 위치 정보를 인증서의 확장필드에 저장하고 있다. CRL DP는 CRL의 크기 관리 문제를 해결 하는 방법으로 사용된다.

인증서를 검증하기 위해 CRL 전체를 가져오는 부담을 줄이기 위해 Delta CRL을 사용한다. Delta CRL은 CRL 발행 시 base CRL이라 불리는 기존의 CRL에 대한 갱신 내용만을 담고 있어, CRL을 수신할 때 발생하는 통신 부하를 줄일 수 있다. 클라이언트에서는 기존에 수신한 CRL에 Delta CRL을 추가함으로써 폐기된 정보를 얻을 수 있다.

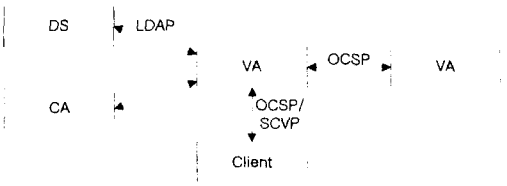
CRT(Certificate Revocation Tree)는 Mere Hash tree를 기반으로 한 방법으로 Valicert가 특허를 가지고 있으며 Online과 offline 모두 지원된다[7]. CRL 보다 response 크기가 작고, 매 response마다 서명이 필요 없다는 장점을 가지고 있다.

위 세가지 방법은 CRT의 문제점 중 하나인 CRL 크기 문제만을 해결할 뿐 인증서에 대한 실시간 검증 정보는 제공하지 못한다. 크기 문제뿐만 아니라 검증 정보에 적시성을 제공하는 방법으로 OCSP가 있다[2,3]. OCSP는 인증서 검증 요청을 처리하는 OCSP Server를 두어 클라이언트에게 OCSP 응답을 제공한다. 현재 IETF PKIX 워킹그룹에서 버전 2 가 draft 상태이며, 실시간 인증서 검증 서비스인 ORS(Online Revocation Status) 뿐만 아니라 인증 경로 구축을 위한 DPD(Delegated Path Discovery), 인증 경로 검증을 위한 DPV(Delegated Path Validation)를 제공하고 있다[3]. OCSP는 CRL을 배포하지 않아도 되므로 CRL이 가지고 있는 한계적인 문제점들을 해결할 수 있다. 하지만 각 응답마다 서명을 해야 하는 부담과 요청이 많아 졌을 경우에 발생하는 OCSP Server의 부담, DOS(Denial of Service) 공격에 대한 취약성은 문제로 지적되고 있다.

인증 경로 검증 서비스를 제공하기 위한 프로토콜로 IETF PKIX 워킹그룹에 현재 draft 상태인 SCVP가 있다. 검증 서비스를 제공하는 SCVP 서버는 클라이언트가 인증 경로 검증을 수행하는데 필요한 정보를 제공하는 untrusted SCVP 서버와 인증 경로 구축에서 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]. 서명에 대한 부담, 요청이 급증할 때 서버의 오버헤드 등의 단점을 가지고 있다.

3. ETRI VA

본 장에서는 클라이언트의 인증 경로 검증에 대한 부담을 줄이고 통합적인 정책 관리를 위해 ETRI VA를 제안한다. ETRI VA는 클라이언트의 인증 경로 검증을 대행해 주는 시스템으로, 클라이언트는 인증 경로 검증에 대하여 VA를 신뢰한다. VA는 인증 경로를 구축하고 인증서 상태를 실시간으로 검증하고 다른 VA와 CA들과의 연동을 통하여 인증 경로 전체를 검증하는 서비스를 제공한다. 이는 다양한 신뢰 모델에 대해서 독립적으로 인증 경로 검증을 제공하므로 향후 국제 PKI 연동에도 활용될 수 있다.



(그림 1) VA model

3.1 기본 모델

클라이언트는 하나의 VA를 Trusted Anchor로 하여 인증 경로 검증에 관련된 모든 작업에 관하여 VA만을 신뢰하고 서비스를 요구한다. VA는 클라이언트가 요구한 검증 대상 인증서를 검증하기 위하여 클라이언트가 신뢰하는 신뢰 지점으로부터 검증 대상 인증서까지의 인증 경로를 구축하고 인증 경로 상의 각 인증서의 상태 정보를 검증하여 인증 경로 검증 작업을 수행한다. 신뢰하고 있는 VA가 인증 경로상의 인증서에 대한 상태 정보를 검증하지 못하는 경우는 VA가 신뢰하는

다른 VA나 디렉토리 서버로 정보를 요청하고 서비스를 제공받을 수 있다. VA는 CA간의 인증 관계와는 무관하므로 신뢰 모델에 독립적으로 신속한 정책 반영이 가능하고 복잡성을 최소화 한다.

3.2 ETRI VA 시스템 구조

VA와 CA의 관계는 세가지로 나뉠 수 있다. 첫번째는 VA와 CA가 동일한 경우로, 클라이언트의 인증서를 제공한 CA가 VA 역할을 수행하는 경우이다. VA 서비스에 사용되는 인증서와 비밀키는 CA의 인증서와 비밀키를 사용한다. 이는 클라이언트가 신뢰하는 지점이 한곳으로 되어 있어 구조가 간단해지나, 하나의 시스템에서 다수의 검증 요구를 처리하기에는 무리가 따를 수 있고 DOS 공격에 취약점을 드러낼 수 있다. 두번째는 VA가 CA에 의해 위임 되는 경우로 VA의 인증서는 CA에 의해 발급된다. 다수의 검증요구에 대처하기 위해 VA는 자체적인 구조를 형성하여 부담을 줄일 수 있다. 세번째는 CA와는 무관한 독립적인 VA로써, 자신의 인증서를 셀프 사인하여 배포하며 클라이언트는 CA와 무관하게 신뢰를 형성한다.

3.2.1 클라이언트 서비스

클라이언트는 인증 경로 검증에 대하여 신뢰 모델과 상관없이 VA만을 신뢰한다. 클라이언트는 VA의 인증서를 가지고 서비스 요청에 대한 응답의 서명을 검증한다. 클라이언트는 인증 경로 구축 또는 인증 경로 검증을 위해 SCVP를 사용하여 서비스를 요청하고, 인증서 상태 정보 서비스를 지원 받기 위하여 OCSP를 사용한다.

VA가 인증서 상태 정보 서비스에 적시성을 제공하기 위해서는, VA가 관리하는 도메인 내의 CA가 갖고 있는 인증서 상태 정보를 실시간으로 VA의 DB에 반영을 한다. CA의 DB를 반영하지 못하는 경우에는 적시성을 제공하지 못하지만 LDAP을 사용하여 CRL을 획득하여 상태 정보를 얻는다. 또한, 클라이언트에게 서비스를 신속하게 지원하고 VA의 부하를 경감시키기 위해, 이미 검증된 인증 경로에 대해서는 캐쉬로 유지하고 요구된 인증 경로가 캐쉬와 부합할 경우 인증서 상태 확인만으로 서비스를 수행한다.

3.2.2 Collaboration

클라이언트가 요구한 인증 경로 검증 수행 시, 검증대상 인증서가 VA가 관리하는 도메인이 아닌 경우는 다른 VA에게 인증서 상태 검증을 요청할 수 있다. 이를 위해 VA 간에 신뢰가 요구된다.

VA에게 요청을 하는 VA는 기동록 되어있는 라우팅 서버 목록, 신뢰 서버 목록을 이용하여 검증 대상 인증서의 상태 검증이 가능한 VA를 찾아 상태 검증 요청 메시지를 송신하고, 요청을 받는 VA는 기동록 되어있는 접근 허용 서버 목록으로 요청 메시지에 대한 작업 여부를 판단함으로써 인증서 상태 검증에 대하여 collaboration을 수행 한다. 상호 요청/응답에 사용되는 프로토콜은 OCSP를 사용한다.

인증 경로 구축을 위하여 저장하고 있는 Trust CA List에서 CA의 인증서를 사용하고 인증서가 List에 없는 경우에는 LDAP을 이용하여 디레토리 서버로부터 인증서을 얻어온다. 검증을 위한 인증서의 상태 정보를 얻기 위하여 OCSP를 사용하며, 해당 인증서에 대하여 OCSP 서비스를 받지 못하는 경우는 상태 검증에 대한 적시성은 제공 받지 못하지만 디렉토리 서버로부터 CRL을 얻어와 검증을 수행한다.

3.2.3 신뢰 리스트

VA 시스템은 클라이언트가 신뢰하는 CA들의 Trust CA List를 관리한다. 이는 클라이언트가 신뢰 지점을 지정하거나 지정하지 않는 모든 경우에도 인증 경로 구축을 지원할 수 있게 한다. 또한 VA 시스템은 클라이언트에게 서비스를 신속하게 제공하고 VA의 부하를 경감시키기 위해, 이미 검증된 인증 경로에 대해서는 캐쉬로 유지한다. 요구된 인증 경로가 캐쉬와 부합할 경우는 인증 경로의 인증서 상태 확인만으로 인증 경로 검증 서비스를 수행한다. 다른 VA로부터 인증서 상태 정보를 지원 받기 위하여 신뢰하는 VA의 List를 관리한다.

3.3 ETRI VA 모델 특징

VA 시스템에게 인증 경로 검증에 대한 부담을 전이함으로써 클라이언트는 다음과 같은 장점을 얻게 된다.

- Protocol Stack의 단순화
- Trust CA 관리 단순화
- 메모리, 프로세싱 요구 최소화 : 무선 환경에 적합
- 사용자 프로그램 업그레이드 요구 최소화

VA가 인증 경로 검증에 있어 collaboration을 적용하고 검증된 인증 경로를 캐쉬함으로써 얻어지는 이득은 아래와 같다.

- 신뢰 모델에 독립적인 신속한 정책 반영
- 신속한 응답 처리로 인한 효율성 증대

또한 클라이언트가 하나의 VA만을 신뢰함으로써 자사 고객에 편리한 검증 서비스를 제공할 수 있고, 타사 고객 및 타 인증기관 요청에 대한 서비스는 별도로 관리 하여 서비스를 제공할 수 있다.

4. 결론

본 논문은 PKI에 필수적인 요소인 인증 경로 검증에 효율적으로 대응하고 확장성을 지원하기 위하여 ETRI VA를 제안하였다. ETRI VA는 인증 경로를 구축하고 인증서 상태를 실시간으로 검증하며 다른 VA와 CA들과의 연동을 통하여 인증 경로 전체를 검증하는 서비스를 제공함으로써 클라이언트의 인증 경로 검증에 대한 부담을 줄였다. ETRI VA는 중앙집중적으로 신속하게 정책을 반영할 수 있고 다양한 신뢰 모델에 대해서 독립적으로 인증 경로 검증을 제공하므로 향후 국제 PKI 연동에도 활용될 수 있다.

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-05, June 2000.

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

[6] ITU-T Recommendation X.509(1997) ISO/IEC 9594-8:1997, Information Technology Open System Interconnection - The Directory : Authentication Framework, 1997.

[7] Valicert, http://www.valicert.com.