2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

실시간 인증서 검증 시스템 모델에 관한 연구

이승우*, 곽 진*, 조석향*, 주미리**, 원동호*
*성균관대학교 전기전자 및 컴퓨터 공학부
**국가보안기술연구소
e-mail : swlee@dosan.skku.ac.kr

A Study on Model for Real-time Certificate Validation System

Seung-Woo Lee*, Jin Kwak*, Seok-Hyang Cho*, Mi-Ri Joo**, Dong-Ho Won*
*School of Electrical & Computer Engineering, Sungkyunkwan University
**National Security Research Institute

요 약

최근 전자상거래 보안을 위해 공인 인증서를 사용하는 공개키 기반구조(PKI) 환경이 널리 확대되고 있다. 이에 따라 인증서의 정당성을 확인하기 위한 공개키 인증서의 실시간 검증에 대한 연구가 활발히 진행되고 있지만 이러한 연구에서는 서비스를 제공하는 서버와 클라이언트 간의 메시지 형식만을 기술하고 실제적으로 서비스를 제공하기 위한 정보 획득에 관한 모델 제시가 나타나 있지 않으며, 현재성있는 인증서 상태를 제공하기 위한 방법이 제시되고 있지 않다. 본 논문에서는 공개키 기반구조에서 사용하고자 하는 인증서의 현재 상태 정보를 제공하며 인증서의 유효성을 실시간으로 제공할 수 있는 실시간 인증서 검증 시스템을 구축하는데 유용한 모델을 제시한다.

1. 서론

인터넷의 확산과 전자상거래의 활성화로 신뢰할 수 있는 네트워크 환경을 제공하기 위해 공개키 기반구조의 사용이 널리 확산되고 있다. 특히 거래 당사자 간의 신뢰가 더욱 요구되는 인터넷상의 전자 상거래와 금융서비스, 증권 거래 등에서는 공개키 기반구조가 필수 요소로 인식되고 있다.

이러한 공개키 기반구조의 기술은 ITU-T 의 X.509 인증서 표준을 근간으로 하며 IETF 에서는 이를 바탕으로 인터넷에 적합한 인증서 표준[1]을 제정하고 있다.

공개키 기반구조에서 상대방의 공개키를 사용하기 위해 인증서를 사용하고자 하는 사용자는 인증서를 사용하기 전에 반드시 인증서의 정당성을 확인하는 인증서 검증 과정을 수행하여야 한다. 이러한 인증서 검증 과정에서 사용하고자 하는 인증서의 폐지 여부의 확인은 매우 중요하다. 기존의 인증서 검증은 인증서를 사용하는 클라이언트가 수행하였으며 인증서 폐지 여부의 확인은 인증서 폐지 목록(CRL : Certificate Revocation List)을 이용해 왔다.

최근 IETF 에서는 인증서 검증만을 수행하는 독립적인 서버에 관한 연구가 활발히 진행되고 있으며, 이러한 연구에는 온라인상에서 실시간으로 인증서의 폐지 여부를 확인해 주는 온라인 인증서 상태 확인 프로토콜(OCSP : Online Certificate Status Protocol)[2][3]과 폐지 여부만이 아닌 전체 인증서 검증을 대행해 주는 간단한 인증서 검증 프로토콜(SCVP : Simple Certificate Validation Protocol)[4]이 제안 되었으며, 공개키 인증서의 검증과 데이터의 소유 증명 등을 서비스 하여 부인 방지 서비스를 제공하는 데이터 검증 및 인증 서버(DVCS : Data Validation and Certification Server)[5]가 제안 되고 있다.

이상의 연구에서 제안된 프로토콜들은 모두 서비스를 제공하는 서버와 서비스를 요청하는 클라이언트 간의 메시지 형식만을 기술하고 있어 실제로 이러한

서비스를 구현하기에 어려움이 많다. 또한 거래 시점에서의 현재성 있는 인증서 상태를 제공하기 위한 메커니즘이 제시되지 않고 있다.

본 논문에서는 인증서 검증 서비스를 제공하는 각 프로토콜을 알아보고, 인터넷상에서 이루어지는 전자상거래와 금융 서비스 등에서 특히 요구되는 인증서 상태 검증의 실시간성과 현재성을 제공하는 실시간 인증서 상태 검증 시스템의 모델을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 인증서 폐지 목록과 IETF 의 인증서 검증 프로토콜들에 대하여 알아보고 3 장에서는 인증서 상태의 현재성을 제공하는 실시간 인증서 검증 시스템의 모델을 제안하고, 4 장에서 결론과 향후 연구 과제를 기술한다.

2. 관련 연구 동향

인증기관에 의해 발급된 공개키 인증서는 인증서의 공개키에 대응되는 비밀키의 손상 또는 인증서 주체의 신원 정보의 변경에 의해서 인증서 유효기간 내에 폐지될 수 있다. 이렇게 폐지된 인증서는 공개키 기반구조 내의 모든 사용자들에게 전달되어 사용자들이 사용하지 않게 해야 한다.

다음은 인증서 상태 정보 또는 인증서 검증 서비스를 제공해주는 메커니즘들이다.

2.1 인증서 폐지 목록(CRL)

X.509 CRL 방법은 인증기관이 폐지된 인증서에 대해 폐지 사유 등의 정보를 포함하는 인증서 폐지 목록을 주기적으로 생성하여, 인증기관의 공개 저장소에 저장하여 인증서 사용자들이 이를 사용할 수 있도록 하는 방식으로 1993 년 X.509 version 2 에서 CRL version 1 이 제정되었고, 1997 년 X.509 version 3 에서 CRL vertion 2 가 제정되었다. 이에 IETF 또한 1999 년 RFC 2459[1]에서 CRL 프로파일을 규정하고 있으며 계속 드레프트 되고 있다.[6]

CRL 방식은 주기적인 발행으로 인한 현재의 인증서의 상태를 반영하지 못하는 비현재성과 전체 CRL 에서 인증서를 검색하기 위해 매번 CRL 을 다운 받아야 하고 이를 검색해야 하기 때문에 비실시간적인 문제점을 갖는다.

이러한 문제를 해결하기 위해 인증서 폐지 목록 발급 분배점(CDP)과 Delta CRL, Indirect CRL 등이 개발되었으나 근본적인 해결책이 되지 않고 있다.

2.2 온라인 인증서 상태 검증 프로토콜(OCSP)

OCSP 는 기존 CRL 방식의 인증서 상태 검증의 문제점을 해결하기 위해 제안되었다.

OCSP 는 온라인 상에서 인증서의 상태 정보를 제공해 주는 OCSP 서버와 OCSP 클라이언트 간에 수행되는 프로토콜로, OCSP 클라이언트는 특정 인증서의 상태를 OCSP 서버에 요청하게 되고, 이 요청을 수신한 OCSP 서버는 요청된 인증서의 상태 정보를 포함한 응답 메시지를 생성한 후 이를 서명하여 클라이언트에게 전송하게 되고, 응답 메시지를 수신한 클라이언트는 이 응답 메시지의 서명을 검증하게 된다. 서버의 응답 메시지가 정당한 경우 메시지에 포함된 인증서 상태 정보로 인증서의 효력 정지 및 폐지 상태를 확인 할수 있다. 이러한 OCSP 를 사용함으로써 CRL 방식의 비효율적인 문제를 해결할 수 있으며 실시간으로 인증서의 상태를 반영할 수 있게 된다.

OCSP 는 1999 년 6 월 인증서의 상태 정보를 제공하는 OCSP version 1 이 IETF RFC 2560 으로 발표되었으며, 클라이언트와 서버간의 요청(Request)/응답(Response) 메시지를 정의하고 있다. OCSP 는 현재 여러 드래프트를 거쳐 개정될 RFC 2560 이 드래프트중에 있다.[3]

2.3 간단한 인증서 검증 프로토콜(SCVP)

CRL 을 사용하지 않고 인증서의 상태 정보를 제공하는 OCSP 가 제안되었으나, 인증서 검증을 위한 다양한 정보가 요구됨으로써 인증서 상태 정보 외에 인증경로에 관한 검증 정보들을 제공하는 SCVP 가 제안되었다.

SCVP 의 목적은 클라이언트의 인증서 유효성 검증 관련 기능의 부담을 서버에게 위임함으로써 이의 구현을 간단화하는 것으로, 이를 통해 PKI 구현이 용이하게 되며 정책의 관리를 집중화 할 수 있는 장점을 가지게 된다.

SCVP 는 IETF 에서 1999 년 처음 드레프트되었으며 대리 인증 경로 검증 서비스(Delegated Path Validation : DPV)와 대리 인증 경로 발견 서비스(Delegated Path Discovery : DPD)를 제공하는 프로토콜로 선정되었다.[7]

SCVP 는 SCVP 서버와 SCVP 클라이언트간에 수행되는 프로토콜로 클라이언트와 서버간의 요청(Request)/응답(Response) 메시지를 정의하고 있다.

클라이언트는 서버를 통해 온라인으로 특정 인증서의 유효성과 효력 정지 및 폐지 상태를 확인할 수 있으며 또한 인증서 유효성 검사 경로 등 다양한 정보를 이용할 수 있다. 이러한 서비스는 인증서 검증 과정에 대한 클라이언트의 부담을 덜어줄 수 있다.

2.4 데이터 검증 및 인증 서버 프로토콜

DVCS 는 신뢰할 수 있는 부인 방지(non-repudiation) 서비스를 구축하는 데 필요한 하나의 구성 요소로 사용될 수 있는 제삼의 신뢰 기관(TTP : Trusted Third Party)을 제공할 수 있는 프로토콜로서 2001 년 2 월 IETF RFC 3029 로 등록되었다.

DVCS 의 역할은 서명된 문서 또는 공개키 인증서의 유효성과, 데이터의 소유 또는 존재를 증명하는 것으로 DVCS 로 제공될 수 있는 서비스로 다음의 4 가지 서비스가 정의되고 있다.

- 데이터 소유 인증(Certification of Possession of Data)
- 데이터 소유 주장 인증(Certification of Claim of Possession of Data)

- 전자서명 된 문서의 정당성 검증(Validation of Digitally Signed Documents)
- 공개키 인증서의 유효성 검증(Validation of Public Key Certificates)

이상의 서비스들 중에서 공개키 인증서의 유효성 검증 서비스는 특정 시간에서의 공개키 인증서의 유효성을 검증하거나 인증서의 정당함을 주장할 때 사용하는 서비스로 신뢰 지점까지의 전체 인증 경로에 대한 유효성 검증이 이루어진다.

3. 제안 모델

3.1 제안 배경

인증서 검증 메커니즘으로 CRL 방식이 제안되었으나 주기적인 발행 특성으로 인증서 폐지 시점과 CRL 발행 시점의 시간차이(Time-gap) 문제가 발생하며 매번 큰 크기의 CRL 을 다운받아야 한다. CRL 다운의 문제점을 해결하기 위해 OCSP, SCVP 와 이를 활용하는 DVCP 가 인증서 검증 관련 프로토콜로 제안되었으나 구체적인 구현 모델과 현재의 인증서 상태를 반영하기 위한 메커니즘이 제시 되지 않았다.

3.2 제안 모델의 요구사항

제안하는 실시간 인증서 검증 시스템은 다음의 요구사항을 만족해야 한다.

- 인증서 상태 정보의 현재성(timeliness)
  : 서버가 제공한 정보는 클라이언트가 요청한 시점에서의 인증서의 현재 상태를 제공해야 한다.

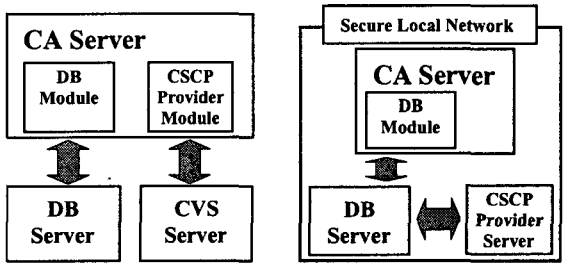
- 실시간 서비스(real-time service)
  : 클라이언트는 인증서를 수신하는 즉시 서버에게 인증서의 ' 폐지 또는 효력 정지 여부' 또는 인증서의 유효성을 요청하여 이를 확인하며 서버는 서비스를 요청 받은 즉시 수용할 수 있는 시간 안에 적절한 서비스를 제공한다.

- 로드의 분산 처리
  : 서비스를 제공하는 서버는 다수의 클라이언트에 의한 요청을 처리할 수 있어야 한다. 때문에 서버의 과다한 로드는 해당 서비스의 정당한 권한을 갖고 있는 다른 서버로 위임하여 서버가 서비스 불능에 빠지는 일이 없어야 한다.

3.3 제안 모델

현재성 있는 인증서 상태와 실시간 인증 경로 검증 및 인증 경로 발견 서비스를 제공하는 실시간 인증서 검증 시스템은 다음과 같은 구성요소를 갖는다.

가) 인증서 상태 및 인증 정책 제공자(Certificate Status and Certificate Policy Provider: CSCPProvider)
: CSCPProvider 는 인증기관에서 제공하는 인증서의 상태와 인증기관의 인증 정책을 인증서 검증 서버에 제공하는 모듈로 인증기관이 보유하고 있는 인증서 상태 정보와 인증 정책을 안전한 통신 채널을 통해 실시간으로 인증서 검증 서버에 제공한다. 이를 위해 인증기관의 서버에 모듈로서 탑재되거나 방화벽 등의 보안 서비스가 제공되는 인증기관의 동일 지역 네트워크에 위치하게 된다. [그림 1]은 CSCPProvider 와 인증기관과의 관계를 나타낸다.



(a)CA 서버 내부 모듈 b)지역 네트워크 상의 서버

[그림 1] CSCPProvider 와 인증기관과의 관계

나) 인증서 검증 요청 클라이언트
: 인증서 검증 요청 클라이언트는 인증서의 유효성을 검증하기 위해 인증서 검증 서버에 위에서 기술한 인증서 상태 제공 서비스 등을 요청한다. 클라이언트는 해당 서비스의 요청 메시지를 구성할 수 있어야 하며 응답 메시지를 수신하여 이의 전자서명과 내용의 정당성을 확인하는 등의 처리 능력을 갖추어야 한다.

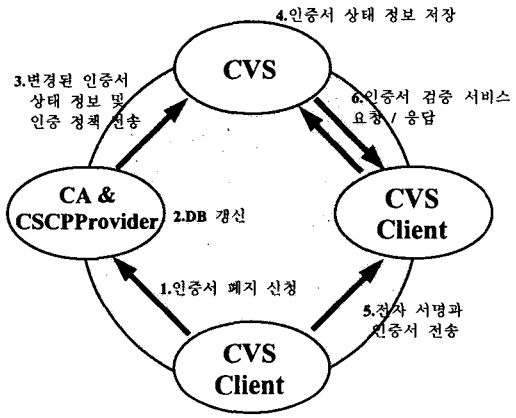
다) 인증서 검증 서버(Certificate Validation Server : CVS)
: 인증서 검증 서버는 CSCPProvider 가 안전한 통신 채널을 통해 제공한 인증서 상태와 인증 정책을 자체 데이터베이스에 저장하며, 이를 바탕으로 클라이언트의 서비스 요청 시 인증기관으로부터 발급 받은 서명용 키로 전자서명된 서비스 응답 메시지를 구성하여 클라이언트에 제공한다.

라) 인증기관(Certificate Authority : CA)
: 인증기관은 기본적으로 인증서 사용자들의 정보와 인증서 상태 정보를 자체 데이터베이스에 저장하고 있다. 인증기관은 사용자의 인증서 폐지 요청 또는 변경 요청으로 인해 인증서의 상태가 변경되는 즉시 이를 CSCPProvider 에게 변경된 인증서 상태 정보를 제공한다.

3.4 제안 모델의 동작 과정

비밀키의 손상 또는 인증서 주체의 신원정보의 변경으로 인증서의 폐지 또는 변경 신청이 필요한 경우

인증기관 또는 등록기관(RA)에 이를 신청하게 된다. 인증서 폐지 또는 변경 신청을 받은 인증기관은 이를 처리하고 즉시 폐지된 인증서의 일련번호와 폐지 사유 등의 인증서 상태 정보를 CSCPProvider 에게 제공한다. 변경된 인증서 상태 정보를 제공받은 CSCPProvider 는 이 정보를 안전한 통신 메커니즘을 사용하여 인증서 검증 서버에게 전달한다. 인증서 검증 서버는 이를 자신의 데이터 베이스에 저장하고 클라이언트의 요청시 이를 바탕으로 요청된 서비스를 제공한다. CSCPProvider 는 인증기관의 인증 정책 역시 제공하며 인증서 검증 서버는 이를 바탕으로 인증서 검증 서비스를 제공할 수 있게 된다. [그림 2]는 구성 요소들이 동작하는 과정을 나타낸다.



[그림 2] 인증서 검증 서버의 동작

3.5 제안 모델이 제공하는 서비스

제안하는 실시간 인증서 검증 시스템 모델에서 제공하는 서비스의 종류는 다음과 같다.

- 인증서 상태 제공 서비스
  : 요청된 인증서의 폐지 또는 효력 정지 여부'를 제공
- 인증 경로 검증 서비스
  : 사용하고자 하는 인증서의 인증 경로 검증을 대행
- 인증 경로 발견 서비스
  : 인증서 상태 정보를 포함하는 인증 경로의 발견을 대행

3.6 제안 모델 분석

제안된 인증서 검증 시스템 모델은 각 인증기관에 CSCPProvider 를 위치하게 하여 인증기관이 보유한 가장 최신의 인증서 상태를 인증서 검증 서버에 제공함으로서 현재성 있는 인증서 상태를 반영할 수 있게 된다. 또 인증서 검증 서버가 CSCPProvider 로부터 인증 정책 또한 제공받아 인증 경로상의 인증서 유효성 검사를 대행할 수 있다. [표 1]은 CRL 방식과 OCSP, SCVP 와 제안 모델을 비교분석한 결과다.

[표 1] 제안 모델 분석

	CRL	OCSP	SCVP	제안모델
인증서 상태 제공	0	0	0	0
실시간 서비스	×	0	0	0
인증서 유효성 검증	×	×	0	0
인증서 상태 정보의 현재성	×	×	×	0
정보획득 모델 제공	•	×	×	0

4. 결론 및 향후 연구 과제

본 논문에서는 실시간으로 인증서 상태 제공, 인증 경로 검증, 인증 경로 발견 서비스를 제공하는 실시간 인증서 검증 시스템 모델을 제안하여 기존의 CRL을 이용한 인증서 상태 검증 방식의 문제점을 개선하였으며, 인증서 상태 정보의 변경 시 즉시 이를 인증서 검증 서버에 전송해 주는 인증서 상태 및 인증 정책 제공자를 제안하여 거래 당시의 인증서의 상태가 매우 중요한 금융 서비스, 증권 거래, 전자상거래 등에 필수적인 현재성 있는 인증서 상태를 제공한다.

향후, 인증서 상태 및 인증 정책 제공자와 인증서 검증 서버와의 안전하고 인증가능한 전송 프로토콜에 대한 연구가 필요하다.

참고문헌

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

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

[3] M. Myers, R. Ankney, A. Malpani, S. Galperin and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP", IETF draft-ietf-pkix-rfc2560bis-01.txt, February, 2002

[4] Ambarish Malpani, Russ Housley and Trevor Freeman, "Simple Certificate Validation Protocol (SCVP)", IETF draft-ietf-pkix-scvp-07.txt, February, 2002

[5] C. Adams, P. Sylvester, M. Zolotarev and R. Zuccherato, "Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols", IETF RFC 3029, February, 2001

[6] R. Housley, W. Polk, W. Ford and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", IETF draft-ietf-pkix-new-part1-12.txt, January, 2002

[7] Alfred W. Arsenault and Sean Turner, "Internet X.509 Public Key Infrastructure: Roadmap", IETF draft-ietf-pkix-roadmap-07.txt, January, 2002