SCVP를 이용한 전자 인증서 검증 시스템의 구현에 관한 연구

안연정*, 백선욱**
*(주) 비트컴퓨터
** 상명대학교 컴퓨터소프트웨어전공
e-mail : paeksu@smu.ac.kr

A study on the implementation of SCVP

Youn-Jung Ahn*, Seonuck Paek**
*BIT computer
** Dept. of Computer Software, Sangmyung University

요 약

본 논문에서는 PKI 에서 사용자 인증을 위해 발급되는 전자 인증서 검증을 위해 IETF 에서 표준화 작업 중인 SCVP(Simple Certificate Validation Protocol) 구현 및 테스트 결과를 기술한다. 기존의 전자 인증서 검증 시스템으로 사용되고 있는 OCSPv1 은 전자 인증서의 폐지 목록(CRL)을 통한 상태 검증만을 할 뿐으로 전자 인증서의 발급 경로에 대한 검증이나 CA 에서 발급 당시의 정책이 변경되었을 경우에 대한 검증 기능은 제공하지 못하고 있다. 본 논문에서는 SCVP 를 OpenSSL-0.9.7 상에서 구현하여 기존의 OCSPv1 과 연동함으로써 전자 인증서 발급경로 검증 및 전자 인증서 발급 정책의 변경은 물론 기존의 인증서 상태 검증도 할 수 있도록 하였다.

1. 서론

인터넷 사용자가 증가하면서 악의적인 목적을 가진 사용자에 의해 데이터가 변조되거나 위조될 위험성도 점점 더 높아지고 있다. 이러한 위험성에 대비하기 위해 PKI 에 기초한 전자 인증서 발급 시스템이 인터넷 금융 시스템을 비롯한 여러 응용에서 사용되고 있는데, 이러한 시스템에서 전자 인증서의 위/변조를 검증하는 프로토콜로는 CRL(Certificate Revocation List)나 OCSPv1(Online Certificate Status Protocol)이 현재 사용되고 있다[1][2]. OCSPv1 은 전자 인증서를 발급한 CA 에서 해당 전자 인증서를 폐지시켰는지의 여부를 확인하는 방식으로 전자 인증서의 유효성을 검증한다[2]. 그러나, CA 에서 사용자에게 전자 인증서가 발급되는 경로 상에서 이 인증서가 제 3 자의 손에 들어갈 개연성이 있으며 이로 인해 전자 인증서가 위조나 변조될 우려도 있다 [3]. 이 경우 기존의 OCSPv1 시스템에서는 경로 검증이나 정책 변경 여부에 대한 검증을 실시하지 않으므로 이를 판별하기가 어렵다. 이러한 OCSPv1 의 문제점을 보완하고자 IETF 에서는 SCVP(Simple Certificate Validation Protocol)를 제안하여 표준화 작업을 진행하고 있으며, 구체적인 구현 방안에 관한 연구도 활발하게 진행되고 있다[4][5][6][7]. SCVP 에서는 경로 형성과 경로 검증 기능이 있으므로 OCSPv1 에서 지원하지 않았던 DPD/DPV (Delegated Path Discovery / Delegated Path Validation) 요구사항을 지원할 수 있어서[7][8][9] 최근에 DPD/DVD 표준 프로토콜로 추진되고 있는 실정이다. 한편 OCSPv1 을 보완하여 DPD/DPV 기능을 제공하고자 하는 OCSPv2 에 관한 논의가 진행 중에 있지만 이러한 방향에 대한 구체적 결과는 좀 더 지켜봐야 하는 상태이다. 본 논문에서는 기존의 OpenSSL-0.9.7 에 있는 OCSPv.1 을 기반으로 SCVP 기능을 추가 구현하여 연동함으로써 DPD/DVD 를 제공하는 전자 인증서 검증 시스템을 용이하게 구현하고자 하였다. 개발된 연동 시스템을 이용함으로써 발급 경로에 대한 검증과 해당 CA 가 전자 인증서를 발급할 때 사용하였던 정책에 대한 검증과 전자 인증서의 상태 검증이 가능하도록 하였다. RootCA 에서부터 여러 하위 IntermediateCA 를 거치는 계층적 인증 기관 구조하에서의 경로 형성 및 검증이 가능하도록 하였다.

본 논문의 2 절에서는 전자 인증서 검증 시스템과 관련된 기술을 유사 연구와의 비교를 통해 살펴보고 3 절에서는 개발된 검증 시스템의 구조와 특징을 살핀다. 4 절에서 구현된 검증 기법에 대해 기술하고 5 절에서는 개발된 시스템에 대한 테스트 결과를 기술한다.

2. 관련 연구 동향

대표적인 전자 인증서 검증 프로토콜은 다음과 같다.

2.1 전자 인증서 폐지 목록 방식(CRL) [1]
본 방식은 검증이 필요할 때마다 CA 로부터 인증서 폐지 목록(CRL) 전체를 다운 받아서 그 목록에서 해당 전자 인증서를 검색한 후 존재하면 폐지가 되었다고 판단하고 존재하지 않으면 폐지되지 않고 아직 유효하다라고 판단하는 방식이다. 이 방식에서는 실시간으로 전자 인증서의 상태를 검증할 수가 없고 CRL 을 다운로드 하는 사이에 제 3 자가 전자 인증서를 사용하면 전자 인증서 사용자는 제시된 전자 인증서가 실제로는 폐지되어 있음에도 불구하고 그것을 알지 못한다는 문제점이 있어 이를 보안하기 위해 OCSPv.1 시스템이 나오게 되었다.

2.2 OCSPv1 방식 [2]
이 방식은 CRL 방식을 보완하여 전자 인증서의 실시간 상태 검증을 제공하도록 한 방식으로 서버와 클라이언트로 구성된다. 서버는 실시간 검증을 위해 CA 의 정보 저장 서버와 전자 인증서 상태 목록을 공유하여야 하는데 주로 LDAP 을 이용하여 인증서 상태 목록에서 해당 전자 인증서에 대한 정보를 검색한다. 클라이언트가 전자 인증서 검증을 요청해 오면 서버에서는 전자 인증서 상태 목록에서 해당 전자 인증서에 대한 정보를 검색한 후 폐지되었으면 REVOKED 라는 결과 값을 생성하고 여전히 유효한 상태이면 Good 결과 값을 생성하며, 해당 전자 인증서에 대한 정보가 존재하지 않는 경우에는 Unknown 결과 값을 생성하여 클라이언트에게 전달한다.

2.3 SCVP 방식[4]
이 방식은 전자 인증서에 대해 발급 경로 검증과 정책 검증 및 상태 검증을 하여 전자 인증서의 유효성을 확인하는 방식으로 서버와 클라이언트로 구성된다. 전자 인증서가 발급되기 위해 거쳐온 CA 들에 대한 정보를 수집하여 전자 인증서 발급 경로를 형성한 후 형성된 경로에 대해 경로 검증을 하게 된다. 경로 검증은 계층화된 CA 를 거쳐 사용자에게 발급되는 모든 경로에 대해 제 3 자의 개입이 없었는지, CA 들이 모두 유효한지를 확인하는 방법이다. SCVP 는 IETF 에서 현재 DPD/DPV 를 지원하는 프로토콜로 추진 중이며, 국내에서도 이 표준의 국내 적용에 관한 연구가 활발하게 진행되고 있다[5][6]. 한편, 한편 OCSPv1 을 보완하여 DPD/DPV 기능을 제공하고자 하는 OCSPv2 에 관한 논의가 진행 중에 있지만 이러한 방향에 대한 구체적 결과는 좀 더 지켜봐야 하는 상태이다. 본 논문에서는 OpenSSL-0.9.7 상에 구현된 OCSPv1 에 SCVP 를 구현하여 상호 연동함으로써, DPD/DPV 요구사항을 만족하는 시스템을 용이하게 구축할 수 있도록 하였다..

3. 전자 인증서 검증 시스템 구조

본 논문에서 개발한 전자 인증서 검증 시스템은 그림 1 과 같다. 기존의 OCSPv1 전자 인증서 검증 서버와 본 논문에서 개발한 SCVP 전자 인증서 검증 서버를 연동하였으며 인증서 발급 기관은 최상위 인증 기관과 하위 인증 기관으로 계층적으로 구성하여 DPD/DPV 기능을 테스트할 수 있도록 하였다. 인증서를 발급받은 사용자는 본 논문에서 개발한 SCVP 클라이언트를 이용하여 SCVP 서버에게 전자 인증서 검증 요청을 하게 된다. SCVP 서버는 검증 요청을 받은 후 해당 정보를 인증서 발급 기관의 디렉토리 서버로부터 가져오게 된다. SCVP 서버가 정보를 가져온 후 검증을 시작하는데 우선 경로를 형성하고 난 후 형성된 경로를 검증하고 그 과정에서 정책 검증도 같이 실행하게 된다. 경로 검증과 정책 검증을 마친 SCVP 서버는 상태 검증을 위해 OCSPv.1 서버에게 상태 검증을 요청하게 된다. OCSPv1 서버로부터 상태 검증 응답을 받은 후 SCVP 서버는 모든 검증 결과를 종합하여 그 중 한 가지라도 유효하지 않은 결과가 있을 때는 유효하지 않다라는 결과를 생성해서 SCVP 클라이언트에게 보내게 된다.

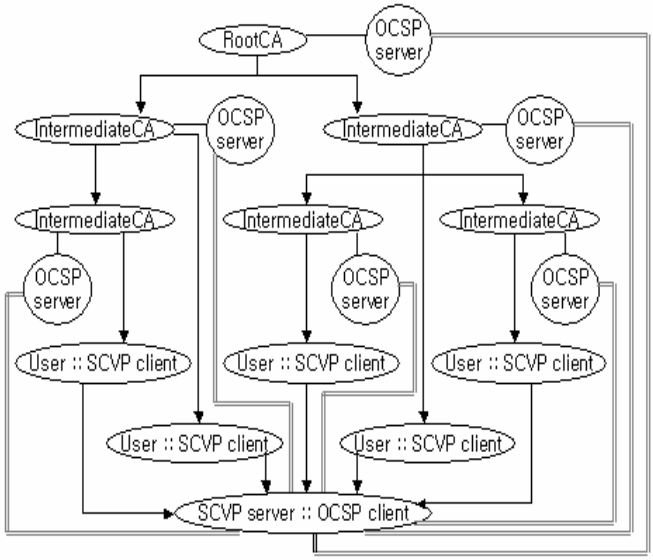

그림 1. 전자 인증서 검증 시스템 구성

4. 전자 인증서 검증 기법

본 논문에서 구현한 전자 인증서 검증 서버는 경로 검증과 정책 검증과 상태 검증을 하며 경로 검증을 위해 먼저 경로 형성을 한다. 경로 형성을 위해 본 논문에서는 forward direction 방식을 사용하며 이는 최종적으로 전자 인증서를 발급 받은 사용자에서 최상위 CA 로 추적해 나가는 방법이다[3]. 그림 2 는 인증서 발급 경로 형성을 나타내며, 인증서를 보관하고 있는 저장 서버로부터 인증서를 가지고 온 후 이를 매칭시

켜서 경로를 추적해 나가는 과정을 보여주고 있다. 전자 인증서는 발급된 순서에 의해서 상위 인증서와 하위 인증서로 그 계층이 존재한다.

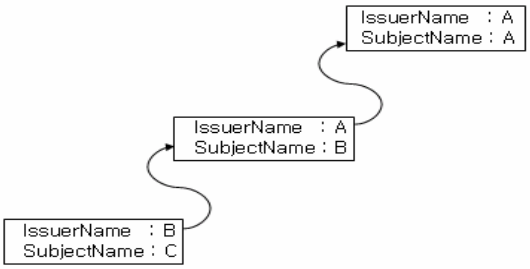

그림 2. 전자 인증서 발급 경로 형성

사용자에게 발급 된 전자 인증서에서 Issuer name 항목에서 그와 동일한 subject name 항목 값을 가진 인증서를 찾는다. 찾은 인증서를 상위 인증서로 여기고 경로 형성을 한다. 마찬가지로 상위 인증서의 그 다음 상위 인증서를 찾는 방법도 issuer name 과 subject name 을 매칭시켜서 찾는다. 본 논문에서 구현한 매칭 기법은 먼저 전자 인증서를 발행한 인증서 발행 기관을 찾는 것인데, 이를 위해 SCVP 클라이언트에서 작성하여 보낸 검증 요청 메시지의 한 항목인 TrustedAnchors 항목을 검색한다. 검색 결과에 따라 그 이후의 처리가 달라지는데, 첫 번째 경우는 TrustedAnchors 항목에서 인증서 발행 기관을 찾은 것이고 두 번째 경우는 그 항목에서 발행 기관을 찾지 못한 경우이다. 찾지 못한 경우에는 SCVP 클라이언트가 전송한 검증 요청 메시지에서 IntermediateCerts 항목을 찾는다. 각 항목에서 인증서 발행 기관을 찾았으면 인증서 폐지 목록 검색 작업으로 넘어가게 된다. 모든 작업 수행 중에는 실패 시 곧바로 응답 메시지 작성 작업으로 넘어간다. 인증서 검증을 하기 위해서는 우선적으로 인증서 경로 형성이 이루어져야 되기 때문에 인증서 경로 형성부터 실패한 경우 곧바로 모든 검증 과정을 수행하지 않고 오류 메시지와 원인을 담은 응답 메시지를 작성하게 된다..

정책 검증의 경우 전자 인증서를 발급한 해당 CA 에서 전자 인증서를 발급할 당시의 정책 OID 값을 확인하는 작업이다. 정책 OID 값에는 CA 고유의 정책이 들어 있을 수도 있고 Any Policy 가 들어 있을 수도 있다. 요청 메시지에 포함된 정책 OID 값과 해당 전자 인증서를 발급한 CA 가 현재 사용하고 있는 정책 OID 값이 동일한지 확인한다.

상태 검증의 경우 SCVP 는 CRL 방식, OCSP 방식, delta-CTL 방식 등 여러 방식이 있으며 본 논문에서는 기존의 시스템인 OCSPv1 와 연동한다.

그림 3 과 그림 4 는 본 논문에서 구현한 SCVP 의 프로토콜 형식을 보여주고 있다.

그림 3 의 SCVP Request 메시지에서 TypeOfCheck 항목은 클라이언트가 서버에게 해주기를 원하는 서비스 종류를 나타내며 서비스 종류로는 최상위 신뢰 루트까지의 인증 경로 발견과 신뢰 루트까지의 인증 경로 검증과 인증서 취소 검사가 있다. WantBack 항목은 클라이언트가 서버에게 요청하는 종류로서 인증서를 위한 인증 경로와 취소 증거 정보 등을 포함한다. 그 외에 Validity Time 항목은 클라이언트가 관련 정보를 알기 원하는 시간을 나타내는 항목이다.

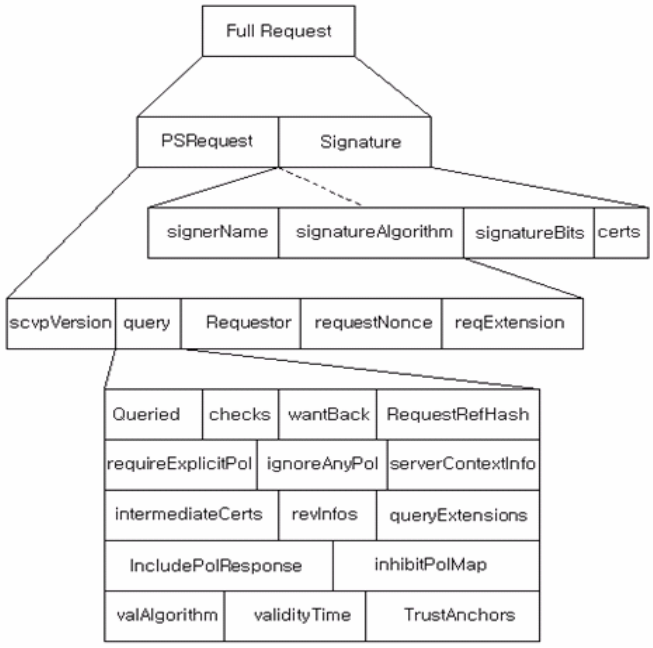

그림 3. SCVP 검증 요청 메시지 형식

그림 4 의 SCVP Response 메시지에서 responseStatus 항목은 전체 요구에 대한 서버의 상태 응답을 나타내며 그 값은 성공(0), 인식불가능 항목발견(1), 너무 바쁨(2), 잘못된 구조(3) 등과 같이 숫자로 나타내어진다. ReplyWantBack 항목은 클라이언트에게 주어지는 해당 인증서에 대한 정보로서 인증체인과 취소상태인 경우 인증서 취소 상태의 증거(CRL 또는 OCSP 응답) 등을 포함한다. 그 외에 ProductAt 항목은 서버가 이 응답을 생성한 시점을 나타낸다.

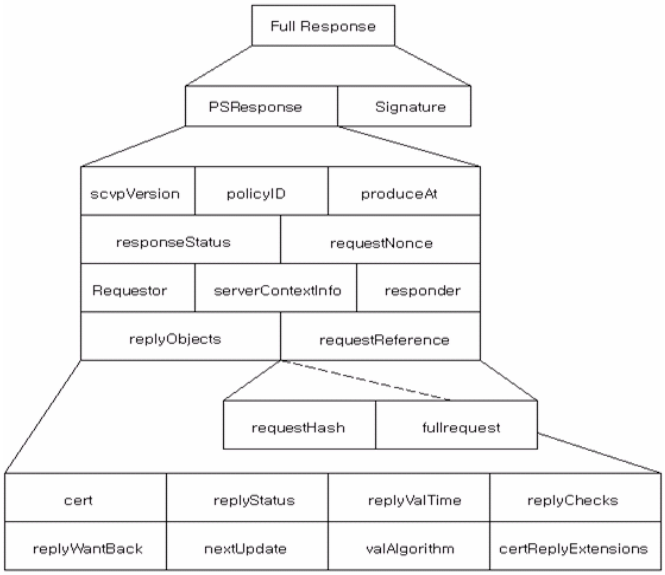

그림 4 SCVP 검증 응답 메시지 형식

5. 테스트

본 논문에서는 전자 인증서 발급 경로가 유효하지 않은 전자 인증서를 발급하여 기존의 검증 시스템이었던 OCSP 서버만으로 검증을 시도해 보고 또한, 동시에 본 논문에서 구현한 검증 시스템으로도 검증을 하도록 테스트하였다. <표 1>은 테스트 결과를 보여주고 있다. 특히 유효하지 않은 전자 인증서에 대해 OCSP 서버에서는 1)good 이라는 잘못된 결과를 보여주고 있으나, 본 논문에서 구현한 SCVP 를 이용한 시스템에서는 OCSP 서버로부터 Good 이라는 결과를 응답받아도 최종 결과에서 Valid 라는 잘못된 결과 값이 아닌 Invalid 라는 의도한 결과 값을 생성함으로써 올바르게 검증을 수행한다는 것을 확인하였다.

<표 1> 검증 테스트 결과

	전자 인증서 발급 경로가 invalid한 경우	전자 인증서 상태가 revoked 인 경우	전자 인증서가 Vaild 인 경우
OCSP 서버	1) good	2) revoked	3) good
SCVP 서버	4) invalid	5) invalid	6) valid

즉, 전자 인증서가 발급된 경로를 역추적하여 경로를 형성시킨 후, 형성된 경로에 대해 경로 검증을 한 결과 올바르지 않다는 결과가 생성되었다. 그림 5 는 표 1 의 6)의 경우에 해당하는 테스트를 본 시스템에서 수행한 결과 화면을 보여주고 있다. wantback 이 valid 인 결과가 있는데, 이 경우는 전자 인증서가 제 3 자에 의해 변조되지 않고 유효한 전자 인증서임을 입증한 것이다.

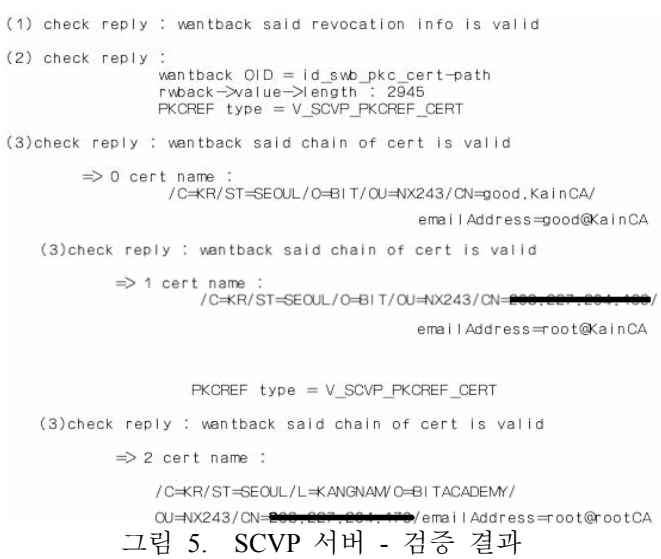

그림 5. SCVP 서버 - 검증 결과

OCSP 시스템과는 다르게 본 논문에서 구현한 검증 시스템에서는 전자 인증서 검증을 수행하는 시간을 예약할 수 있는데, 실시간 서비스가 아니어도 상관없는 경우 집중적인 서비스 발생 시간 대를 피하여 수행을 분산시킬 수 있다.

한편, SCVP 서버는 OCSP 서버와 마찬가지로 SCVP 클라이언트로부터 검증 요청 메시지를 받아들여야 하므로 이를 이용당하여 DoS 공격받을 수 있다는 취약점이 있다[8]. 하지만 본 논문에서 제시한 시스템에서는 이를 대비하여 SCVP 서버 측에서 전달받은 검증 요청 메시지에 대해 index 를 관리하여 어느 SCVP 클라이언트가 보냈는지 관리하도록 함으로써 악의적으로 서비스 검증 요청 메시지를 발생시킬 경우 SCVP 서버가 해당 SCVP 클라이언트를 차단하여 검증 요청 메시지 수신을 거부할 수 있도록 하였다.

6. 결론

본 논문에서는 PKI 의 전자 인증서를 효과적으로 검증하기 위한 전자 인증서 검증 시스템을 개발하였다. 상태 검증만 제공하는 OCSPv1 의 기능을 보완하여 본 논문에서는 경로 검증과 정책 검증이 가능하도록 IETF 에서 표준화 작업 중인 SCVP 를 구현하여 기존의 OCSPv1 와 연동함으로써 경로검증, 정책 검증 및 상태 검증을 제공하는 시스템을 용이하게 구축하고자 하였다. 본 시스템을 이용하면 전자 인증서 발급 경로 상의 제 3 자의 개입에 대한 경로 검증과 전자 인증서를 발급한 기관에서 발급 정책을 바꾸었을 경우에 대한 확인 작업을 할 수 있으며, 테스트 결과 기존의 OCSPv1 만으로는 검증 시스템에서 검증할 수 없었던 유효하지 않은 전자 인증서에 대해서도 올바른 검증이 가능함을 확인할 수 있었다. 본 시스템은 인터넷 금융 서비스를 비롯한 전자 인증서 활용 분야에 널리 활용될 수 있으리라 기대된다.

참고문헌

[1] R. Housley, W. Ford, W. Polk, D. Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL,” RFC2459, 1999.
[2] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, “X.509 Internet Public Key infrastructure Online Certificate Status Protocol - OCSP,” RFC2560, 1999.
[3] D. Pinkas, R. Housley, “Delegated Path Validation and Delegated Path Discovery Protocol Requirements,” RFC3379, 2002.
[4] SCVP Draft 13 SCVP -Draft-ietf-pkix-scvp-13.txt, 2003.
[5]http://www.rootca.or.kr/news/announce/2003012701.html
[6]http://www.etri.re.kr/inform/newtech/etri21c_81_2003.html
[7] 배두현, “실시간 인증서 검증을 위한 SCVP 와 OCSP 연동 방안에 대한 연구 및 구현,” 중앙대 대학원, 2003.
[8] 곽 진, “인증서 상태 정보의 현재 성을 제공하는 실시간 검증 모델에 관한 연구,” 성균관대 대학원, 2003.
[9] 최영철, “효율적인 인증서 상태 및 경로 검증 시스템에 관한 연구,” 성균관대 대학원, 2003.