실시간 인증서 검증을 위한 OCSP와 SCVP의 연동방안에 대한 연구

배두현*, 송오영*, 박세현*

*중앙대학교, 전자전기공학부

A study of real-time certificate validation using OCSP and SCVP

Du Hyun Bae*, Oh Young Song*, Se Hyun Park*

*Chung-Ang University, School of Electrical & Electronic Engineering

요 약

현재 인증서의 상태 검증을 실시간으로 제공하기 위해 각 CA(Certificate Authority)들은 고전적 방법인 CRL(Certificate Revocation List) 배포보다는 OCSP(Online Certificate Status Protocol)을 통하여 인증서의 상태에 대한 정보를 실시간으로 제공한다. 그러나, 경로검증 및 인증서 정책 맵핑 및 정책검증과 인증서 상태검증을 제공하는 SCVP(Simple Certificate Validation Protocol)는 CRL을 사용하는 한계로 인하여 실시간 검증을 제공하지 못하고 있다. 또한 OCSP는 인증서의 실시간 상태검증만을 제공할 뿐, 인증서의 경로검증과 인증서 정책 맵핑 및 정책검증에 대한 서비스는 제공하지 못하고 있다. 따라서, 이러한 두 프로토콜의 단점을 보안하고, 인증서 검증서버가 제공해야 하는 모든 서비스를 제공하기 위해 OCSP와 SCVP의 연동방안에 대한 연구를 통하여 SCVP에서의 실시간 검증을 제공할 수 있도록 한다.

I. 서론

온라인 금융거래 및 전자상거래가 활성화됨에 따라 사용자 인증과 요구되는 정보들에 대한 보안문제가 대두되었고, 이에 대한 해결책으로 인증서에 기반한 보안 서비스들이 각광받고 있다. 그러나, PKC(Public Key Certificate)를 이용한 인증 및 보안을 사용하는 대부분의 시스템이 인증서의 실시간 상태검증을 제공하지 못하고 있으며, 간혹 OCSP를 통해 제공한다 하더라도 인증서의 경로검증 및 정책검증을 통한 완벽한 인증서 검증은 제공하지 못하고 있다. 전자상거래는 실시간으로 이루어지는 반면 사용자 인증 및 정보보안에 대한 검증이 실시간으로 이루어지지 않는다면 PKC기반의 정보보안 서비스는 전자상거래에서 사용될 수 없게 된다[10].

현재 SCVP를 통한 인증서 경로 형성 및 인증서 검증과 정책검증은 인증서의 CRL을 이용하는 방법으로 이루어 질 수 있다. 그러나 CRL을 이용하는 방법은 CRL의 Update 주기로 인한 Update 기간 사이에 폐기되는 정보는 알 수 없으므로, 진정한 실시간 검증을 할 수 없게 된다.

한편, 현재 OCSP server에서 사용되고 있는 검증 방법은 CA가 발행한 인증서 폐기 정보를 OCSP server가 가져와서 CRL에 대한 서명검증을 하여야 하며, 그 다음 인증서의 폐기 유무를 CRL을 살펴봄으로서 가능하다. OCSP server는 CRL cache를 통하여 CRL 검증 및 획득에 대한 overhead를 줄일 수 있으나, CRL cache를 사용한 경우 인증서의 nextUpdate 필드에 표시되어 있는 시간까지 새로 Update된 인증서 폐기 정보를 알 수 없어서 실시간 검증을 지원하지 못하고 있다. 이러한 방법에 대안으로 CA와 OCSP가 인증서 폐기 정보에 대한 같은 DB를 사용함으로서 해결할 수 있으므로, 인증서의 실시간 검증이 이루어 질 수 있으나, OCSP는 경로검증 및 정책검증을 할 수 없다는 단점이 있다[9]. 이러한 두 프로토콜의 단점을 보안하기 위해 두 가지 프로토콜을 동시에 사용하여 인증서 경로검증을 실시간으로 이루는 모델을 제시하고, 구현하는 것이 논문의 주제이다.

II. OCSP를 통한 인증서 상태검증

인증서의 실시간 검증을 위해서 현재 많이 사용되고 있는 OCSP를 사용하고, 인증서의 경로검증 및 인증서 policy mapping과 policy 검증을 위해서 SCVP를 사용한다.

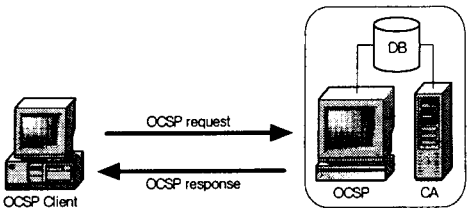

그림 1: OCSP의 실시간 인증서 검증을 위한 구성도

OCSP server는 CA가 가지고 있는 폐기 정보들을 공유함으로써, 인증서의 실시간 상태검증을 제공하게 된다. 즉, CA와 OCSP가 같은 도메인 내에 위치하거나, 폐기정보를 담은 database를 공유함으로써, CA가 가지고 있는 폐기정보를 OCSP도 가지고 있게 되어, 실시간 검증을 제공하는 것이다. OCSP server는 요청메시지가 오면 요청메시지를 검사하고, issuer name hash 와 issuer key hash부분을 비교하여 server가 제공하는 도메인에서 발행된 인증서인지를 확인하게 된다. 일치하면 요청메시지에 있는 인증서 serial number를 확인하여 database에 해당 serial number의 상태를 확인하여 인증서의 상태를 결정하고 해당 응답 메시지를 생성하여 요청자에게 보내게 된다[2].

Ⅲ. SCVP를 이용한 인증서 검증 방법

SCVP server는 인증서에 있는 CRL DP (Distribution Point)를 통하여 발행자의 인증서와 해당 인증서의 CRL을 획득하여 검증하게 된다 [1]. CRL과 발행자의 인증서는 caching을 통하여 획득과정에서의 network overhead 및 검증시간지연을 줄일 수 있으나, CRL의 다음 발행주기 동안에 있는 폐기 정보들을 획득할 수 없게 되어 실시간 검증을 할 수 없게 된다[7]. 이것은 CRL을 매번 획득한다 하여도, CA에서 발행된 인증서의 폐기가 이루어 질 때 마다 CRL을 발행하는 것은 CA에 부담이 되므로 다음 발행주기까지 발행하지 않게 되어, 실시간 인증서 검증을 제공하지 못하게 된다는 점은 그대로 남게 된다.

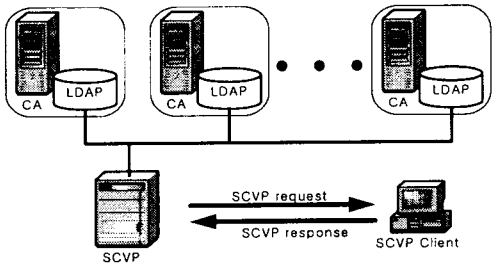

그림 2: SCVP의 기반 모델

Ⅳ. SCVP와 OCSP 연동을 통한 실시간 검증

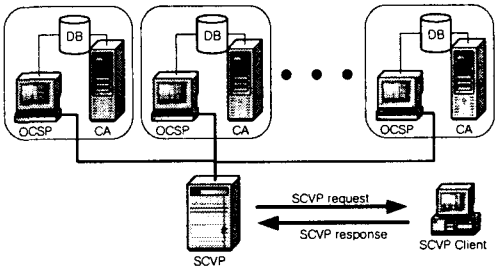

그림 3: SCVP와 OCSP 연동 모델

SCVP server는 OCSP를 이용하여 인증서의 상태를 검증하고, OCSP response로부터 발행자의 인증서를 획득하여 인증서 경로 검증을 하게 된다. 제안된 모델에서 OCSP server는 OCSP response를 CA의 인증서와 개인키를 가지고 서명하거나, 응답메시지에 CA의 인증서를 첨부해야 SCVP에서 발행자의 인증서를 획득할 수 있다.

[그림 4]는 SCVP server의 인증서 검증과정에 대한 순서도이다[1, 8]. SCVP 요청메시지가 도착하면 요청메시지를 검사하고, target 인증서를 획득하고, 인증서의 'Authority Info Access' 확장영역을 통하여 OCSP server의 URI를 획득하고, OCSP 요청메시지를 생성하여 OCSP server에게 보내고 응답을 받아 OCSP response의 서명을 검증하여 인증서 상태를 확인하게 된다. 발행자의 인증서를 OCSP 응답 메시지로부터 얻어내어 target 인증서의 경로를 검증, 즉 target 인증서의 발행자 서명을 확인하고 제한영역 및 정책맵핑을 실시하여 인증서 경로를 형성하게 된다. 획득한 발행자 인증서가 SCVP request message에 포함된 trust anchor 인지 확인하거나 self-signed 인증서이면 경로형성 및 검증은 끝나게 되고, 발행자의 인증서가 요청메시지의 trust anchor에 설정된 인증서가 아니고 또한 self-signed 인증서가 아니면, 발행자의 인증서를 가지고 다시 OCSP 검증 및 경로 검증을 하게 된다. 인증서의 경로검증은 SCVP 요청메시지에 포함된 trust anchor로부터 target 인증서까지의 인증서 서명검증과, OCSP response 응답의 서명검증과 서명자가 권한을 가지고 있는지 확인하는 것이 되겠다. 정책검증은 인증서 안의 'certificate policy'와 'basic constraint'확장영역으로부터 인증서 정책맵핑을 실시하고 검증하게 된다.

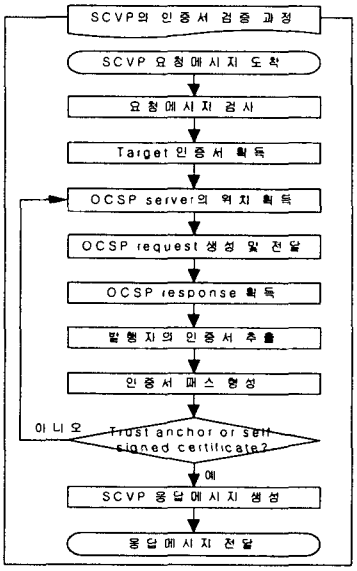

그림 4: SCVP 인증서 검증 과정

V. 성능 비교

성능비교는 인증서의 depth가 i일때, SCVP만을 이용했을 때와 OCSP와 SCVP를 연동했을 때에 처리시간과 각 server와 client 간의 메시지 수를 비교한다.

1. 메시지 수 및 RTT

SCVP만을 이용했을 때 시스템간 메시지 전송 수는 SCVP 메시지 1쌍과 경로구성을 위한 LDAP 접근이 i-1쌍([그림 5] 참조)이 된다. OCSP service를 이용할 경우 시스템간 메시지 전송 수는 SCVP 메시지 1쌍과 OCSP 메시지 i-1쌍([그림 6] 참조)이 된다. 따라서 두가지 경우의 각 시스템간 메시지 트랜잭션 수는 같다.

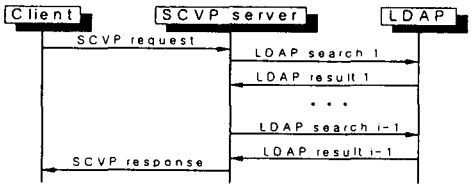

그림 5: SCVP만 사용시 시스템간 메시지 transaction

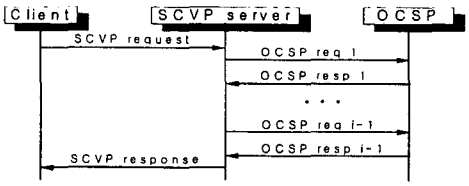

그림 6: OCSP와 연동시 시스템간 메시지 트랜잭션

각 시스템간 메시지 트랜잭션의 수가 같으면 OCSP를 사용하는 모델이나, CRL을 이용한 SCVP만을 사용하는 모델에서의 RTT가 비슷하다고 가정할 수 있다.

2. 처리시간 비교

SCVP 서버에서 가장 시간이 오래 걸리는 hash, 서명, 서명검증의 횟수를 비교해 봄으로서 처리시간을 비교한다. 인증서의 depth가 i라 하고 계산해보면 SCVP만 이용했을 때 [표 1]과 같다. 요청메시지에 대한 hash 및 서명검증(1회), 인증서에 대한 hash 및 서명검증($i-1$회), CRL에 대한 hash 및 서명검증($i-1$회), 응답메시지 hash 및 서명(1회)이다.

	필수	선택	합계
HASH	$2i$		$2i$
서명	1		1
서명검증	$2i-1$		$2i-1$

표 1: SCVP만 이용시 주요 처리시간

SCVP와 OCSP 연동시 서버에서의 주요 처리시간을 보면 [표 2]와 같다. 요청메시지에 대한 hash 및 서명검증(1회), 발행자 이름 hash 및 key hash($2i-2$회), OCSP 요청메시지 생성시 hash 및 서명($i-1$회), OCSP 응답메시지 hash 및 서명검증($i-1$회), 경로검증시 인증서의 hash 및 서명검증($i-1$회), 응답메시지 hash 및 서명(1회)이다.

	필수	선택	합계
HASH	$3i-1$	$2i-2$	$5i-3$
서명	1	$i-1$	i
서명검증	$2i-1$		$2i-1$

표 2: SCVP/OCSP 연동시 주요 처리시간

OCSP 요청메시지 생성시 hash 및 서명은 선택사항이고, 발행자 key hash는 인증서의 Authority Key Identifier 확장영역의 값이 발행자의 공개키의 hash 값이므로 이 값을 사용하면 실제 필수적인 주요 처리시간에서 CRL을 통한 SCVP만을 사용시의 차이점은 hash를 $i-1$회 더 해야한다는 부담이 있다. 그러나, 메시지 hash는

전자서명 및 전자서명 검증보다 처리시간이 빠르므로 처리시간이 치명적으로 늘어나지 않는다. 또한, OCSP와 SCVP를 연동할 시에는 delta-CRL이나 segmented CRL에 대한 획득과 처리과정에 대한 부담을 줄일 수 있어서 hash 처리에서의 SCVP의 부담이 상대적으로 경감된다 할 수 있다.

SCVP와 OCSP를 연동함으로서, SCVP server에 걸리는 *computation overhead*는 있으나, PKI에서 가장 중요하다 할 수 있는 인증서에 대한 실시간 검증이 가능하다. OCSP를 지원하지 않는 CA에서 발행한 인증서에 대해서는 기존의 방식대로 CRL을 통하여 인증서의 검증을 할 수 있으나, CRL 갱신이 빠르게 된다거나, delta-CRL을 사용한다 하더라도 CRL의 주기로 인한 엄격한 의미의 실시간 검증은 이루어지기 어렵다.

Ⅵ 결론

PKI 기반에서 인증서에 대한 검증은 대략적으로 인증서의 상태검증, 경로검증, 정책검증으로 나눌 수 있다. 인증서 검증 3가지 중 어느하나도 소홀히 하여서는 안된다. 또한, 전자상거래의 활성화로 인하여 PKI기반의 인증 및 보안 시스템이 활성화되고 있는 반면, OCSP를 통한 실시간 검증은 제공될 수 있으나, 인증서의 경로검증은 제대로 이루어지지 않고 있다. SCVP는 3가지 검증을 모두 제공할 수 있는 반면, 실시간 인증서 상태검증은 제공할 수 없다. 이러한 두가지 프로토콜의 단점을 보안하기 위해 SCVP와 OCSP의 연동방안을 제시하였고, 연구를 통하여 연동시의 단점으로 SCVP 서버의 처리시간에 대한 overhead는 있으나, 인증서의 실시간 검증을 제공할 수 있고 처리시간에 대한 overhead도 optional hash 및 서명, 서명검증부분을 제거하면 실제적으로 그리 큰 차이는 보이지 않았다. 따라서, 본 논문에서 제시한 모델을 통해 SCVP 서버가 실시간 검증을 하기 위한 하나의 모델을 제시하였고, 이러한 실시간 검증을 통해 PKI 전반에 걸쳐 인증서 사용 및 전자서명에 대한 신뢰성을 부가시킬 수 있겠다.

참고문헌

[1] A. Malpani, R. Housley, T. Freeman, Simple Certificate Validation Protocol, 2002

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

[3] S. Boeyen, T. Howes, P. Richard, Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2, RFC 2559, 1999

[4] Boeyen, S, T. Howes, and P. Richard, Internet X.509 Public Key Infrastructure LDAPv2 Schema, RFC 2587, 1999

[5] R. Housley, W. Ford, W. Polk, and D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280, 2002

[6] D. Pinkas, R. Housley, Delegate Path Validation and Delegate Path Discovery Protocol Requirements, RFC 3379, 2002

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

[8] R. Housley, Cryptographic Message Syntax, RFC 2630, 1999

[9] Russ Housley and Tim Polk, Planning for PKI, Wiley Computing Publishing, 2001

[10] Andrew Hash and William Duane and Celia Joseph and Derek Brink, PKI:Implementating and Managing E-Security, McGraw-Hill, 2001