실시간 인증서 검증 프로토콜

박 재 관, 김 광 조

국제정보보호기술연구소, 한국정보통신대학원대학교

On-line Certificate Validation Protocol(OCVP)

Jaegwan Park, Kwangjo Kim

International Research center for Information Security(IRIS)

Information and Communications Univ.(ICU), Korea

{jgpark, kkj}@icu.ac.kr

요 약

인증서의 정당성을 검증하기 위하여 검증자(verifier)는 소유자(owner)의 인증서와 그 인증서를 인증한 공인인증기관의 인증서들을 검증해야 하고, 그에 앞서 그 인증서들의 폐지 여부를 확인하여야 한다[1]. 이 인증서 폐지 목록의 확인을 대행하는 것이 실시간 인증서 상태 프로토콜(OCSP)이다[2]. 그리고, 이 OCSP가 인증서의 폐지 여부만을 응답하는 단점을 극복하기 위하여 간단한 인증서 검증 프로토콜(SCVP)이 제안되었다[7]. 이 SCVP는 사용자의 질문의 형태에 따라 인증서의 정당성까지 검증하여 주는 프로토콜이다. 그러나, 이 SCVP 역시 새로운 신뢰기관을 필요로 한다. 본 논문에서는 전체 인증서 검증 경로를 알 수 있는 인증서 일련번호 부과 방법[4]을 기반으로 부과적인 신뢰기관 없이 실시간으로 인증서의 정당성 여부를 확인할 수 있는 새로운 프로토콜을 제시하고자 한다. 계산량의 결과로는 SCVP와 동일한 2n 번의 서명 생성 및 검증이 필요하지만, 인증서 폐지 목록과 부과적인 신뢰기관을 필요로 하지 않는다.

I. 서론

현재 공개키 기반구조에서는 X.509v3 인증서가 사용된다. 이 인증서는 공개키와 그 소유자를 대응 시켜주는 문서이며, 또한 공인된 인증기관(CA)이 서명을 함으로써 정당성이 확인된다.

그러나, 인증서는 전자적으로 생성되고 보관되는 것이므로 이를 신뢰하는 것, 즉 검증자가 소유자의 실체를 신뢰하는 것이 무엇보다도 중요하다. 이를 위하여, 검증자는 소유자의 인증서로부터 자신이 신뢰할 수 있는 공인인증기관까지의 경로를 확인하고, 그 경로에 있는 모든 인증서들을 검증함으로써 그 신뢰관계를 새롭게 생성한다. 또한, 소유자의 인증서가 폐지되었는 지를 확인하는 것이 그 무엇보다 선행되어야 한다.

현재는 X.509v2 인증서 폐지 목록이 사용되고 있다[1]. 또한, 인증서 폐지 목록의 확장 필드를 이용한 여러 방법들이 소개되고 있다[6]. 실시간 인증서 상태 프로토콜(OCSP)[4]은 검증자가 행하여야 하는 인증서 폐지 목록의 확인을 대행하는 시스템이다. 그러나, 이 OCSP는 단순히 인증서 폐지 목록의 확인을 대행하는 것으로, 인증서의 폐지 여부만을 확인한다. 간단한 인증서 검증 프로토콜(SCVP)[5]은 OCSP의 이러한 행태를 수정하기 위하여 좀더 다채로운 질문 형태를 취하고 있으며, 이는 그 형태에 따라 인증서의 정당성 여부까지 확인을 할 수 있다. 그러나, OCSP와 같이 SCVP 역시 새로운 신뢰기관을 필요로 한다.

본 논문에서는 새로운 신뢰기관의 가정없이 온라인 상태에서 인증서의 정당성 여부를 검증하는 프로토콜을 제시하고자 한다. 일반적인 방법에서는 인증서 폐지 목록이 같이 사용되지만, 제안하는 방법에서는 각 공인인증기관이 그 서명을 생성하기에 인증서 폐지 목록을 참조하지 않는다.

본문의 구성은 다음과 같다

제 2장에서는 인증서 폐지 목록 및 실시간 인증서 상태 프로토콜, 간단한 인증서 검증 프로토콜, 그리고, 본 프로토콜의 기반이 되는 전체 인증서 검증 경로를 알 수 있는 인증서 일련번호 부과 방법에 대하여 기술한다. 제 3장에서는 제안하는 새로운 실시간 인증서 검증 프로토콜에 대하여 설명하고, 마지막으로 제 4장에서는 결론 및 향후 과제를 기술한다.

II. 관련연구

1. 인증서 폐지 목록

폐지된 인증서들에 대한 목록을 인증서 폐지목록(Certificate Revocation List : CRL)이라고 하며, 인증기관의 저장소 또는 디렉토리 시스템 등에 등재하여 신뢰당사자가 언제든지 이 목록를 검색할 수 있도록 하여야 한다. 사용자에 의해 인증서 폐지 신청이 접수될 경우 인증기관은 CRL을 생성, 배포함으로써 다른 사용자의 인증서 사용을 중지시킬 수 있다.

CRL은 1988년 ITU-T에서 X.509v1이 제정되었으며, 1993년 ITU-T에서 X.509v2가 제정되어 사용되고 있다. 또한 RFC 2459 (X.509 Internet Public Key Infrastructure Certificate & CRL Profile)에 명시되어 사용되고 있다[1]. 국내 표준화 작업은 인터넷 보안기술 포럼의 PKI 분과 위원회에서 행해지고 있으며 국내 표준으로 ISTF-002(전자서명 인증서 효력정지 및 폐지목록 프로파일 표준)가 2000년 10월에 만들어졌다[2].

CRL의 확장 필드를 이용하여 폐지 목록 발급 분배점(Distribution Point), Delta CRL, Over-issued CRL, Indirect CRL 등의 서비스들이 제안되고 있다[6].

2. 실시간 인증서 상태 프로토콜

실시간 인증서 상태 프로토콜(Online Certificate Status Protocol : OCSP)은 OCSP 서버와 OCSP 클라이언트간에 수행된다. OCSP 클라이언트는 특정 인증서의 유효성과 취소 상태를 서버로 문의하고 서버는 인증서 유효성과 취소 상태를 전달한다. 클라이언트는 서버로부터 인증서가 유효하고 취소되지 않았다는 정보를 수신한 후에 문의한 인증서를 사용해야 한다. OCSP 규격에서는 서버와 클라이언트의 기능과 인증서의 상태를 확인하기 위하여 교환해야 하는 데이터 형태를 정의하고 있다. 이는 실시간으로 인증서의 유효 상태를 확인할 수 있는 장점이 있다.

OCSP는 1999년 IETF PKIX Working Group에서 제안하여 현재 version 1이 RFC 2560 (X.509 Internet Public Key Infrastructure Online Certificate, Status Protocol Version 1.0 : 1999. June)로 제정되었으며, Internet draft로 version 2.0 (Draft-ietf-pkix-ocspv2-02.txt , 2001. March) 이 제안되어 있다.[4]

3. 간단한 인증서 검증 프로토콜

간단한 인증서 검증 프로토콜 (Simple Certificate Verification Protocol : SCVP)는 OCSP보다 좀 더 일반적인 인증서 상태 문의/응답 프로토콜이다. OCSP가 인증서의 폐지 여부만을 응답해주는데 비해 SCVP는 인증서의 유효성 뿐만 아니라, 전체 검증 과정까지 대행해 주는 등 다양한 서비스를 제공해 줄 수 있다.

SCVP는 Internet Draft (draft-ietf-pkix-scvp-06)로 1999년 처음 제안되었으며 가장 최근 버전은 6번째 버전으로 2001년 7월에 IETF Working group에 의해서 제출되었다[5].

4. 전체 인증경로를 포함한 일련번호

전체 인증경로를 포함한 일련번호는 인증서의 일련번호에 그 인증서의 발행에 관련된 모든 공인인증기관들의 식별자를 같이 포함함으로써 전체 인증서 검증 경로를 알 수 있다[3]. 그 일련번호의 형태는 다음과 같다.

Flag | Year | Month | Date | Hour | Minute | Second | Caid | ... | RootCA

III. 제안방법

1. 가정

일반적으로 본 연구를 적용하기 위하여 다음을 가정한다.

1) 공인인증기관은 일반 사용자보다 높은 계산 능력을 가지고 있다.

2) 인증서를 관리할 수 없는 상태가 되는 즉시, 인증서의 소유자는 인증서를 발급한 공인인증기관에 폐지 신고를 한다.

3) 공인인증기관의 인증서를 폐지할 경우, 상위 공인인증기관 뿐만이 아니라, 자신이 발급한 모든 인증서의 소유자에게 그 사실을 알린다.

4) 자신의 인증서를 발급한 공인인증기관의 인

증서가 폐지되었다는 사실을 확인하였을 경우, 자신의 인증서 역시 폐지된다.

2. 실시간 인증서 검증 프로토콜

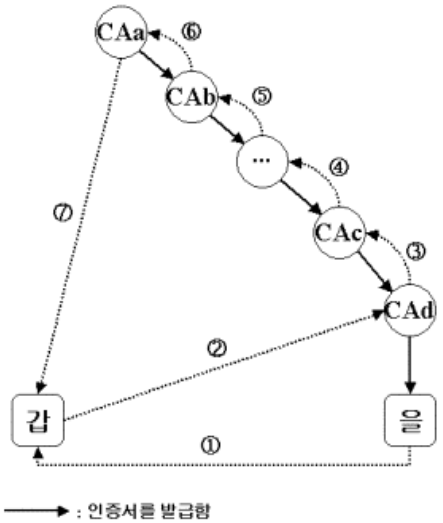

그림 1: 온라인 인증서 검증 프로토콜

① "을"은 자신의 인증서를 "갑"에게 전달한다.

message : "을"의 인증서

② "갑"은 "을"의 인증서 일련번호로부터 "을"의 인증서를 발급한 공인인증기관의 식별자를 확인한다. 만약, "을"의 인증서를 발급한 공인인증기관을 신뢰할 수 없다면, "갑"은 "을"의 인증서를 발급한 공인인증기관에 자신의 인증서와 "을"의 인증서, 그리고, 시간정보와 시간정보를 서명한 값을 전달한다.

message : "갑"과 "을"의 인증서, 시간정보 및 모든 메시지에 대한 서명

③ 공인인증기관 CAd는 전달받은 "을"의 인증서를 자신이 발급을 했는지를 확인한다. 만약 발급을 하였다면 "YES"를 그렇지 않다면 "NO"를 자신의 인증서를 발급한 상위 공인인증기관에 전달한다. 이때, 자신이 받은 "갑"과 "을"의 인증서, 그리고, "갑"이 보낸 시간정보 및 그에 상응하는 서명값을 같이 전달을 하며, 또한, 자신이 응답-YES 또는 No-와 "갑"이 보낸 시간정보에 대하여 서명을 하여 전달한다.

message : "갑"과 "을"의 인증서, 시간정보 및 "갑"의 서명, YES(NO), 그리고 모든 메시지에 대한 서명

④⑤⑥ 공인인증기관이 그의 하위 공인인증기관으로부터 전달받은 메시지를 기본으로 그 메시지를 보낸 공인인증기관의 서명을 검증함으로써 공인인증기관의 정당성을 확인한다. 이때, 하위 공인인증기관의 공개키가 폐지되었는지도 확인하여야 한다. 만약, 정당성이 확인되었다면 "YES"를 그러지 않다면 "NO"를 상위 공인인증기관에 전달한다.

message : "갑"과 "을"의 인증서, 시간정보 및 "갑"의 서명, YES(NO), 그리고 모든 메시지에 대한 서명

⑦ 공인인증기관 CAa는 자신이 받은 서명을 확인함으로써 하위 공인인증기관에 대한 정당성을 확인한다. 이때, 하위 공인인증기관의 공개키의 폐지 여부를 확인하여야 한다. 만약, 정당성이 확인되었다면 "YES"를 그러지 않다면 "NO"를 상위 "갑"에게 전달한다.

message : "갑"과 "을"의 인증서, 시간정보 및 "갑"의 서명, YES(NO), 그리고 모든 메시지에 대한 서명

"갑"은 신뢰하는 공인인증기관 CAa로부터 받은 자신의 인증서 및 "을"의 인증서, 그리고 자신이 생성한 시간정보 및 이 메시지들에 대한 서명를 확인한다. 이후, CAa가 서명한 서명값을 확인하여 "을"을 인증할 것인지에 대한 판단을 한다.

※ ②~⑦의 단계에서 먼저, 공인인증기관은 자신이 받은 두 개의 인증서의 일련번호를 비교함으로써 자신이 ⑦에 해당하는 지를 검사한다.

3. 공격 시나리오

공격자는 자신에게 유리한 방향으로 프로토콜를 이끌어 나가며, 또한 그러기 위하여 자신의 모든 역량를 이용한다. 다음과 같은 공격이 가능하다.

크게 다음과 같은 공격 방법를 적용할 수 있다.

1 사용자의 인증서만를 공격하는 경우

2 공인인증기관의 인증서만를 공격하는 경우

3 사용자와 그의 인증서를 발급한 인증기관의 인증서를 공격하는 경우

4 사용자와 그의 인증서를 발급에 관여된 인증기관중의 일부분에 대한 공격

1의 공격의 경우, "을"의 인증서를 발급한 공인인증기관 CAd가 "을"의 인증서의 폐지 여부를 알고 있으므로, CAd는 "NO"를 메시지에 담게 된다. 만약, 공격자가 "서비스 거부 공격(Denial Of

Service)"을 행함으로써 CAd를 작동하지 못하게 하는 경우, 자신이 CAd로 위장하는 경우와, 그렇지 않은 경우가 있다. 그러나, 이 두 경우 모두 CAc가 CAa의 서명을 확인할 수 없으므로 CAc에서 "NO"라는 메시지가 생성된다.

[2]의 공격의 경우, 공인인증기관의 인증서가 공격을 당하였으므로, 그 공인인증기관의 인증서를 발급한 상위 공인인증기관에 의하여 "NO"가 형성된다. 또한, 이 경우, 가정 4)와 3)에 의하여 자신의 인증서 역시 폐지된다. 따라서, 이 공격의 경우는 [1]의 공격의 경우에 귀속된다.

[3][4] 의 경우, 공격받은 인증서 중 최고 상위에 있는 공인인증기관의 상위 공인인증기관에서는 이 사실을 알고 있으므로, "NO"라는 메시지가 만들어진다. 또한, 이 공격받은 인증기관은 자신의 상위 기관(가정 2)과 자신이 발급한 인증서를 소유한 모든 소유자에게 이 사실을 알리므로(가정 3) 이 공인인증기관을 신뢰하는 모든 하위 공인인증기관 및 사용자는 이 기관을 신뢰할 수 없게 된다. 따라서, 공격받은 공인인증기관의 하부의 모든 인증서는 그 정당성을 잃어버리게 된다.(가정 4)

4. 장점 및 비교분석

일반적으로 인증서 검증 경로의 길이를 n이라 하고, 모든 인증서에 대하여 그 폐지 여부를 확인할 때, 그 인증서 검증 경로의 쌍은 다음과 같다.

{<1, 2>, <2, 3>, ..., <n-1, n>}

여기서, 1은 최상위 공인인증기관으로서 자신의 인증서는 스스로 사인을 한다. 위의 쌍에서 <x-1, x>라 함은 x-1이 x의 인증서를 발급했다는 의미이다. 따라서, 우리는 n의 인증서를 검증하기 위하여 n의 인증서를 전달받아, n-1번의 서명를 검증한다. 그러나, 제안하는 프로토콜에서는 2n번의 서명 생성 및 검증이 필요하다.

그러나, 이때 각 인증서에 대하여 인증서 폐지 여부를 확인하기 위하여 n번의 서명 검증이 이루어져야 한다. 하지만, 제안하는 프로토콜에서는 인증서 폐지 목록의 탐색은 필요하지 않다.

	OCSP	SCVP	OCVP
인증서 폐지 여부	○	○	×
CRL 검증 회수	n	n	×
인증서 정당성 여부	×	○	○
서명 생성 및 검증	×	n	2n
계산 종합	n	2n	2n

또한, OCSP와 SCVP에서는 부과적인 신뢰기관이 필요하지만, 제안한 프로토콜에서는 필요없다.

제안하는 프로토콜이 계산량에서 SCVP와 동등하지만, 부과적인 신뢰기관은 필요하지 않다.

IV. 결론 및 향후 과제

본 논문에서는 전체 인증서 검증 경로를 포함한 일련번호[3]를 이용하여, 실시간으로 인증서의 검증을 수행하는 방법을 제시하였다. 이 방법은 다른 부과적인 신뢰기관(OCSP 서버 또는 SCVP 서버 등) 없이 자신의 인증서를 발급한 공인인증기관들에 대한 기본적인 신뢰를 밑바탕으로 한다. 또한, 기존의 방법은 인증서 폐지 목록(CRL)을 기본으로 그 인증서의 폐지 여부를 확인 후 검증하게 되지만, 제안되는 방법에서는 새로운 신뢰기관을 생성하지 않고, 인증서 폐지 여부에 상관없이 인증서의 정당성를 검증할 수 있다.

향후, 다양한 서비스를 지원하는 프로토콜로 확장시키는 연구가 필요하다.

참고문헌

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

[2] ISTF-002, "전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준", 인터넷 기술 보안 포럼, 2000. 10

[3] 박재관, 김광조, "전체 인증경로를 알 수 있는 일련번호 부과 방법", 제5회 한국정보보호학술발표회[충청지부] 제출

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

[5] Ambarish Malpani, Paul Hoffman, Russ Housley, and Trevor Freeman, "Simple Certificate Validation Protocol (SCVP)", July, 2001, IETF draft-ietf-pkix-scvp-06.txt

[6] A. Arnes, "Public Key Certificate Revocation Schemes", Ph.D Thesis, Queen's University, 2000. 2

[7] Byoungcheon Lee, Kwangjo Kim, Moonseog Seo, and Wonkeun Huh, "Efficient Offline Path Validation", 1st International Workshop for Asian PKI (IWAP 2001), Oct. 19~20, 2001, Daejeon, Korea