이종의 시스템에서 OCRS를 이용한 효율적인 인증서 상태 검증에 관한 연구

황민구[0] · 오해석
숭실대학교 컴퓨터학과 멀티미디어 연구실
hminkoo@hanmail.net[0], oh@computing.ssu.ac.kr

A Study on the Efficient Certificate Status Validation using OCRS in Heterogeneity System

Min-Koo Hwang[0] · Hae-Seok Oh
Dept. of Computer Science, Soong-sil University

요 약

공개키 기반 구조에서 가장 비용이 많이 드는 부분이 인증서가 유효한지 여부를 검증하는 것이다. 특히 고액의 주식 거래나 전자상거래에서 실시간 인증서 상태 검증은 반드시 필요하다. 그동안 연구되어 왔던 인증서 폐지 여부를 확인하는 방법으로 CRL, delta-CRL, OCSP, CRTs, CRSL 등의 방법들이 제안되었다. 하지만, 이들 방법들은 즉시성과 네트워크 비용간의 trade-off가 발생하는 문제점이 있다. 본 논문에서는 Simple skip lists를 사용하여 인증서 사용 용도에 따라 알맞게 서비스를 제공하는 방안인 OCRS를 제안한다.

1. 서 론

인터넷이 대중화가 되지 않은 몇 년 전만 해도, 어떠한 거래를 하기 위해서는 서로가 직접 만나서 종이 문서에 서명 또는 도장을 찍어 문서를 교환하였다. 하지만, 인터넷이 대중화가 된 요즘은 서로 대면하지 않고서도 온라인상으로 신속하게 문서를 주고받을 수 있게 되었다. 하지만, 인터넷을 통해 흘러가는 정보가 전 세계의 네트워크 망에 노출되어있다는 사실 때문에 불법적인 도청이나 위조와 변조, 신분 위장 등 문제점이 발생한다. 특히, 많은 돈이 오가는 전자상거래나 온라인 주식거래에서 거래 당사자간에 더욱 보안성을 제공해야 한다.

이러한 보안성을 제공하기 위해서 개인키와 공개키를 사용하는 공개키 기반 구조(PKI : Public key Infrastructure)를 구축하고 있다[1]. 공개키 기반 구조는 문서를 암호화해서 본인 외에 다른 사람이 그 문서를 볼 수 없도록 하는 기능인 기밀성(confidentiality), 사용자의 신원이 확인된 사람만 메시지에 접근할 수 있는 인증성(authentication), 메시지의 내용이 전송중에 수정, 변조되지 않고 전달되는 무결성(integrity), 거래 상대가 거래 사실을 번복하거나 부인하지 못하도록 방지하는 부인방지(non-repudiation)를 모두 제공해준다.

그런데, 사용자의 공개키는 공개되어 있기 때문에 다른 사람으로부터 위조될 수 있다는 문제점을 가지고 있다. 이를 해결하기 위해서 신뢰할 수 있는 제 3자인 인증기관(CA : Certificate Authentication)이 공개키를 포함한 기타 정보를 가진 인증서를 발급하고 CA의 개인키로 서명하여 공개된 디렉토리 서버에 게시한다. 사용자 A가 원문과 원문에 해쉬한 값에 다 자신의 개인키로 전자 서명하여 사용자 B에게 줄 때, 사용자 B는 사용자 A의 인증서를 디렉토리로부터 얻고, CA의 공개키로 그 인증서의 신뢰성을 검증한다. 여기서 인증서의 신뢰성을 검증한다고 하는 것은 인증서가 유효기간 내에 있는지 체크하고, CA의 전자 서명에 대한 무결성을 체크하는 것이다.

만일 사용자의 실수로 개인키가 손상되었거나 노출되었거나 자격이 박탈되었을 경우 유효기간 내에 인증서를 폐지할 수 있다. 이러한 경우 사용자는 인증서를 사용하기 전에 반드시 인증서의 폐지 여부를 확인하는 인증서 검증 과정을 수행해야 한다.

인증서 폐지 여부를 확인하는 방법으로 인증서 폐지 목록(CRL), 온라인 인증서 상태 확인 프로토콜(OCSP), 인증서 폐지 트리(CRTs)등이 제안되었다. 하지만, 이들 방식은 실시간성과 네트워크 부하(비용)간의 trade-off가 발생하는 문제점이 있다.

본 논문에서는 이종의 시스템에서 효율적인 인증서 검증 서비스를 제공하기 위해 Simple skip lists를 사용해서 인증서 사용 용도에 따라 알맞게 서비스를 제공하는 OCRS(Online Certificate Revocation Simple skip lists)를 제안한다.

2. 관련 연구 동향

2.1 인증서 폐지 목록(CRL)

CRL 방식은 주기적인 발행으로 인해 실시간 인증서 상태를 제공해 주지 못하며, 사용자는 CRL을 매번 다운로드 받아야 하기 때문에 네트워크 비용이 많이 든다는 비판을 받아왔다[2].

2.2 delta-CRL

delta-CRL은 CRL의 단점을 개선하고자 가장 최근에 폐지된 인증서만을 포함하는 인증서 폐지 목록이다[3]. 하지만, 이 역시도 완벽한 실시간성을 제공해 줄 수 없다는 단점이 있다.

2.3 온라인 인증서 상태 검증 프로토콜(OCSP)

OCSP는 기존의 CRL 방식이 실시간 인증서 상태 정보를 제공해 주지 못한다는 문제점을 해결하기 위해 제안되었다[4].

하지만, 각각의 인증서에 대해 실시간적으로 인증서 폐지 여부를 확인하고 전자 서명해야 하므로 OCSP 서버는 과부하가 걸리게 된다는 문제점을 가지고 있다.

2.4 인증서 폐지 트리(CRTs)

CRTs는 인증서 폐지 목록을 이진 트리의 리프 노드로 지정하는 방식으로, 한 방향 해쉬 함수와 경량 전자 서명을 제공함으로써 CRL과 OCSP의 문제점을 해결하기 위해 제안되었다[5, 6]. 하지만 인증서가 폐지되어 트리에 추가되거나 인증서가 만료되어 트리에 삭제될 때마다 트리를 변경해야 하는데, 이때 비용이 많이 든다는 단점이 있다.

2.5 인증서 폐지 스킵 리스트(CRSL)

CRSL은 CRTs의 이진 트리 대신에 skip lists를 사용하여 CRT의 단점인 트리를 변경하는데 부하가 많이 걸린다는 문제점을 해결하고자 제안한 것이다[7]. skip lists는 폐지된 인증서를 linked list의 순서로 표현하고, 맨 앞에 최소값을, 맨 뒤에 최대값을 삽입하여 맨 아래 레벨에 놓는다. 그리고 그 레벨에 있는 폐지된 인증서들을 임의로 1/2의 확률로 선택하고 해쉬하여 다음 레벨의 리스트로 만든다. 이것을 반복 적용하고 루트 레벨의 최소값을 CA가 전자 서명한다.

하지만, 이 방식도 CRTs와 마찬가지로 인증서를 검증하기 위해서 사용자가 직접 해쉬값을 계산해야 된다는 문제점이 있다.

3. 제안한 방법

본 논문에서는 기존의 CRSL에서 사용하였던 skip lists 보다 간략화된 Simple skip lists를 사용하여 빠르게 인증서 폐지 여부를 알 수 있게 하였고, 고액의 증권 거래와 같은 실시간성을 요구하는데 사용되는 인증서인 경우 해쉬없이 바로 인증서 상태를 CA의 개인키로 서명하여 전송하는 방안인 OCRS (Online Certificate Revocation Simple skip lists)를 제안한다.

3.1 제안한 시스템의 전체적인 구조

제안한 시스템의 전체적인 구조는 그림 1에서 보여준다.

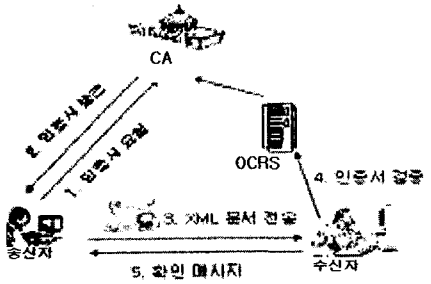

그림 1 제안한 시스템의 전체적인 구조

먼저 송신자는 CA로부터 인증서 발급을 요청한다. 그러면 CA는 송신자에게 인증서를 발급한다. 송신자는 수신자에게 인터넷상으로 문서를 보내기 위해 그 문서를 해쉬한 값에다 자신의 개인키로 서명을 해서 문서와 함께 암호화를 해서 보낸다. 수신자는 암호를 풀고, 송신자의 인증서 상태를 검증하기 위해서 OCRS에게 요청한다. 이때 고액의 현금거래와 관련된 거래일 경우 수신자는 '긴급'이라는 메시지를 인증서 시리얼 번호와 함께 OCRS에게 보낸다. 이 경우 OCRS는 인증서의 상태를 CA의 개인키로 서명하여 수신자에게 보낸다. 수신자는 CA의 공개키로 서명을 풀고 인증서 상태를 검증한다. 이와는 반대로 실시간성이 요구되지 않는 경우엔 수신자는 인증서 시리얼 번호만 OCRS에게 보낸다. OCRS는 여러 개의 해쉬값들을 보낸다. 수신자는 OCRS로부터 받은 해쉬값들을 계산하여 비교를 통해 인증서 상태를 검증한다. 인증서 상태를 검증한 수신자는 송신자로부터 받은 문서를 해쉬하고, 서명된 문서를 송신자의 공개키로 서명을 푼다. 그리고, 해쉬한 문서와 서명을 푼 문서를 비교해서 같으면 인증과 무결성이 보증된다. 그런 후, 수신자는 확인 메시지를 송신자에게 보낸다.

위의 예제에서 W3C에서 표준으로 확정된 XML 전자 서명을 사용하는 이유는 어떠한 디지털 컨텐츠에도 적용이 가능하기 때문이다[8]. 그림 2는 XML 암호와 전자 서명을 한 예를 보여준다.

```
<?xml version="1.0">
<consumer>
  <order>
    <book serial_num="SKE7859" date="2002-06-23"> XML and Java </book>
    <quantity>3</quantity>
    <manufacture_name>Addison-Wesley </manufacture_name>
  </order>
  <payment>
    <consumer_name> kil-dong, hong </consumer_name>
    <card_number secure="true">Uxo5hznutAZxTK... </card_number>
    <expiration_date secure="true">Kdqwln3+ veE=</expiration_date>
    <signature>mc0CFQCou78llAMpmM1eknZAq2j3kfcCNJQndkx9Lu3...</signature>
  </payment>
</consumer>
```

그림 2. XML 암호와 전자서명의 예

3.2 OCRS의 알고리즘

아래의 그림 3은 CRSL에서 사용하고 있는 skip lists 구조에서 중복된 것을 제거함으로써 간략화된 Simple skip lists를 만들고 폐지된 인증서 시리얼 번호를 찾는 과정을 보여준다.

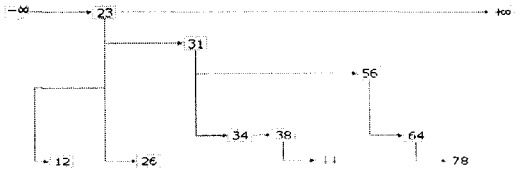

그림 3. Simple skip lists를 통한 search 과정

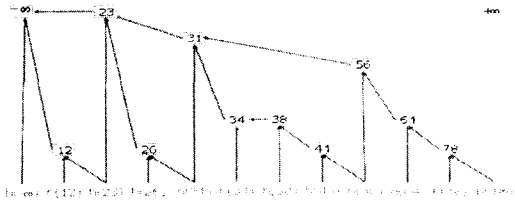

그림 4. OCRS의 해쉬 과정

위의 그림 4는 Simple skip lists를 적용하여 해쉬값을 계산하는 과정을 보여준다.

아래의 그림 5는 Simple skip lists를 적용하여 인증서를 검증하는 과정이다. 여기서는 인증서 시리얼 번호가 45인 인증서를 검증하는 과정을 예로 보여준다.

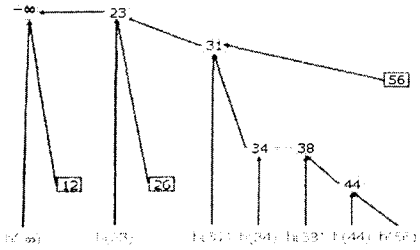

그림 5. OCRS에서 검증하는 과정

이상에서 살펴본 그림은 실시간성을 요구되지 않은 경우에 인증서를 검증하는 과정이다. 만일 실시간성이 요구되는 인증서를 검증할 경우 그림 3에서 보여진 과정을 통해 요청한 인증서 시리얼 번호를 찾고 OCSP처럼 폐지되었는지 여부를 CA의 개인키로 서명하여 수신자에게 실시간으로 전송한다.

본 논문에서 제시하는 알고리즘을 요약하면 다음과 같다.

① 송신자는 문서에 신용카드 번호, 비밀번호, 유효기간 등의 중요한 부분이 있으면 그 부분을 선택하여 <secure>로 태깅을 한다. 만일 중요한 부분이 없으면 생략한다.
② 그 문서를 XML 문서로 변환한다.
③ <secure>안에 있는 부분을 수신자의 공개키로 암호화를 한다. <secure>가 없으면 생략한다.
④ 암호화된 문서를 해쉬한 후, 자신의 개인키로 서명을 한다.
⑤ ③번 문서와 ④번 문서를 XML 전자 서명 형식으로 수신자에게 보낸다.
⑥ 수신자는 ③번 문서를 추출해서 <secure>가 있는지 확인하고 있으면 "긴급"이라는 메시지와 함께 OCRS에게 인증서 상태 검증을 요청한다. 그러면 OCRS는 인증서 폐지 여부만 알려준다.
만일 <secure>가 없으면 OCRS는 여러 개의 해쉬값을 수신자에게 전송하여 수신자가 직접 인증서 폐지 여부를 확인한다.
⑦ 유효한 인증서가 확인되면, 수신자는 ④번 문서를 추출해서 송신자의 공개키로 서명을 풀고, ③번 문서를 해쉬한 값과 비교하여 같은지 여부를 확인한다.

3.3 기대 효과

본 논문에서 제안하는 방식인 실시간성을 요구하는 인증서와 그렇지 않은 인증서를 분류함으로써 얻어지는 기대 효과는 다음과 같다.

1. OCSP보다 서버의 부하가 줄어든다.
실시간성을 보장하기 위해 모든 인증서가 OCSP를 통해서 검증하게 되면 OCSP 서버에 부하가 많이 발생한다. 본 논문에서는 고액의 현금 거래와 같은 안전성과 실시간성이 중요하게 요구되는 경우에만 OCSP 서버처럼 인증서 폐지 여부를 검증하므로 서버의 부하를 줄일 수 있다.
2. CRSL보다 실시간성을 보장한다.
모든 인증서가 CRSL을 통해서 검증하게 되면, 검증자가 직접 해쉬값을 여러 번 계산해야 하므로 인증서 폐지 여부를 확인해야 하는데 시간이 걸린다. 본 논문에서는 skip lists의 구조를 단순화하여 보다 빠르게 검색할 수 있고, 검증자에게 보내는 해쉬값의 개수도 줄일 수 있다. 또한 실시간성을 요구하는 인증서인 경우 폐지 여부를 결과를 보내줄 때, 그 결과만 보내줌으로써 실시간성을 보장할 수 있다.
3. 부분 암호화를 사용하여 암호화 속도가 개선된다.
송신자가 문서를 XML로 변환하고, 보안이 요구되는 정보만을 따로 <secure>로 태깅하여 그 부분만을 암호화한다. 따라서 빠르게 암호화를 할 수 있다는 장점이 있다.

4. 결론 및 향후 연구 방안

인터넷 뱅킹이나 고액의 증권 거래, 현금 거래를 할 때 실시간적으로 인증서 폐지 여부를 확인해야 한다. 하지만, 기존의 인증서 폐지 여부를 확인하는 방법인 CRL, delta-CRL, OCSP, CRT, CRSL을 통해서는 실시간성과 네트워크 부하 간에 trade-off가 발생한다는 문제점이 있다. 본 논문에서는 보안성과 실시간성을 요구하는 경우와 그렇지 않은 경우를 분류하여, 보안성이 요구되는 경우에는 인증서 상태 결과만 CA의 개인키로 서명해서 보내주고, 그렇지 않은 경우는 Simple skip lists를 통해 기존의 CRSL보다 더 적은 개수의 해쉬값을 보내주는 것을 제안하였다. 이 방식은 사용자의 요구(인증서의 용도)에 맞게 효율적으로 서비스를 할 수 있다는 큰 장점이 있다. 향후 연구 방안으로는 요즘 이슈가 되고 있는 무선 PKI에서 효율적으로 인증서 폐지 여부를 검증할 수 있는 방안에 대해 연구하는 것이다.

참고 문헌

[1] Pay Hunt. "PKI and Digital Certification Infrastructure.", IEEE, 2001.
[2] Ronald L. Rivest. "Can We Eliminate Certificate Revocation Lists?" In Proceedings of Financial Cryptography 1998. Springer, February 1998.
[3] Warwick Ford and Michael S. Baum. "Secure Electronic Commerce." Prentice Hall PTR, 1997.
[4] Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams. "X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol." IETF RFC2560, June 1999.
[5] Paul Kocher. "A Quick Introduction to Certificate Revocation Trees(CRTs)." Technical report, ValiCert, 1999.
[6] Moni Naor and Kobbi Nissim. "Certificate Revocation and Certificate Update." In Proceedings of the 7th USENIX Security Symposium, 1998.
[7] M. T. Goodrich and R. Tamassia. "Efficient authenticated dictionaries with skip lists and commutative hashing." Technical Report, Johns Hopkins Information Security Institute, 2000.
[8] W3C, "http://www.w3.org/TR/xmldsig-core"