CRL 분배점과 자동 업데이트 엔진을 이용한 인증서 폐지 목록 관리

윤석주[0] 서재현* 노봉남**
o전남대학교 대학원 전산통계학과, *목포대학교 컴퓨터공학과, **전남대학교 컴퓨터정보학부
addin96@nownuri.net, jhseo@chungkye.mokpo.ac.kr, bongnam@chonnam.ac.kr

Management of Certificate Revocation List Using CRL Distribution Point And Auto-Updating Engine

Seok-Joo Yoon[0] Jae-Hyun Seo* Bong-Nam Noh**
o Dept. of Computer Science and Statistics Graduate School, Chonnam National University
* Dept. of Computer Engineering, Mokpo National University
** Dept. of Computer Science & information, Chonnam National University

요 약

인증서의 유효성을 검사하기 위해 인증기관의 디렉토리내에 있는 최신의 인증서 폐지 목록을 많은 사용자가 동시에 조회시 시스템의 부하 및 속도 저하를 가중시킬 수 있다. 본 논문에서는 디렉토리에 대한 부하를 분산시키고 효율적으로 인증서 유효성 검사를 수행하기 위해 사용자 PC내에 자동 업데이트 엔진을 두어 인증서내의 CRL 분배점을 통한 인증서 폐지 목록을 다운로드 하는 방법을 제안하였다. 다운로드된 인증서 폐지 목록은 사용자의 인증서와 함께 유효성 검사에 이용되며 디렉토리에 대한 조회 횟수를 분산시켜 부하를 감소시킬 수 있다.

Ⅰ. 서 론

공개키 암호기술은 사용자가 각각 키쌍을 생성하여 하나는 자신의 시스템 또는 시스템 외부에 보관하는 개인키(private key)로 사용하고, 다른 하나는 공개하는 공개키(public key)로 하여 제3자가 이 공개키를 이용하여 수신자에게 평문을 암호문으로 만들어 보내면 수신자 즉, 공개키 소유자는 자신의 공개키에 해당하는 개인키를 암호문에 수학적으로 대입함으로써 암호문을 평문으로 만들어 그 내용을 수신자가 볼 수 있도록 하는 것이 공개키 암호 기술의 핵심이다.[1]

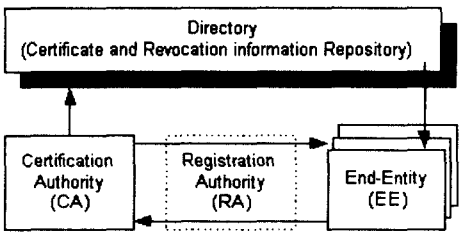
공개키 암호기술을 사용하기 위해서는 즉, 공개키를 안전하게 공개하기 위하여 사용자는 신뢰할 만한 기관 즉, 인증기관(certificate authority)에 자신의 공개키를 등록하는 것이 필요하다. 이는 자신의 공개키에 대한 전자서명을 인증기관에 요구하여 인증기관의 전자서명이 첨부된 공개키 인증서를 발급받아, 이를 다른 인증기관 가입자들이 용이하게 획득할 수 있도록 하여 공개키 암호 기술을 사용할 수 있는 기반을 제공하는 것이다.

본 논문에서는 인증서의 유효성 검사를 위해 인증기관의 디렉토리내에 있는 인증서 폐지 목록을 확인하는 부하를 줄이고자, 사용자의 PC에 항상 최신의 인증서 폐지 목록을 다운로드 하여 인증서의 유효성을 검증하는 방법을 제안하였다.

Ⅱ. 공개키 기반구조

공개키 기반구조는 인증서를 발급 받는 최종 개체, 최종 개체에게 인증서를 발급하는 인증기관, 인증기관의 업무중 신원확인 등의 기능을 수행하는 등록기관, 인증서나 인증서 폐지 목록 등을 보관하기 위한 디렉토리 등으로 구성된다.

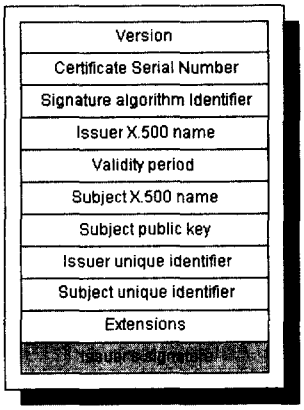
최종개체(End Entity)는 공개키 기반구조의 인증서 주체(subject)이다. 인증기관(CA:Certificate Authority)은 공개키 인증서를 발행하거나 취소하는 기관이다. 등록기관(RA: Registration Authority)은 공개키와 사용자의 신분정보를 보증하는 기관이다. 디렉토리는 인증기관이 발행한 인증서를 보관하거나 여러 사람들이 이를 사용할 수 있도록 하는 시스템이다.[2]



〈그림 1〉 공개키 기반 구조 (PKI)

X.509는 ITU에 의해 제안된 인증서에 대한 기본형식을 정의한 규격이다. 이 구조에서는 인증서의 데이터 형식들과 인증기관에 의해 발행된 인증서를 이용한 공개키의 효율적인 분배 방법을 정의하고 있다. X.509 버전 3의 인증서 형식은 그림 2와 같다.

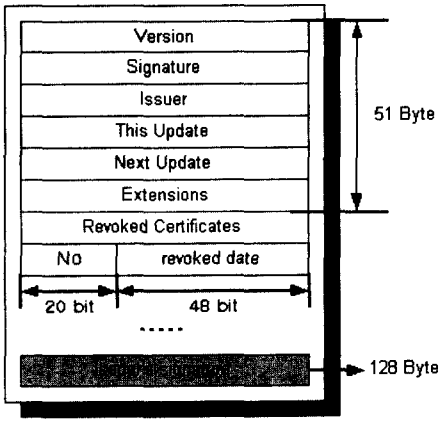
버전(version)은 인증서의 X.509 버전을 나타내는 정수이다. 일련번호(serial number)는 인증서를 유일하게 확인하기 위한 인증서의 일련번호이다. CA 서명문(signature algorithm)은 CA가 서명문 생성을 위해서 사용하는 서명 알고리즘 식별자이다. 발급자 이름(issuer name)은 인증서를 발행하는 발행기관, 즉 CA의 X.500 이름이다. 유효 기간(validity period)은 인증서의 유효기간을 나타낸다. 주체이름(subject name)은 인증서의 소유자, 즉 인증된 공개키에 대응되는 개인키를 소유하고 있는 개체의 x.500 이름을 말한다. 주체 공개키 정보(subject public key information)는 키가 사용되는 알고리즘의 식별자 및 공개키 값을 포함한다. 발급자 서명은 CA의 서명용 개인키로 서명한 서명문이다.[1][2]



〈그림 2〉 X.509 V3 인증서

인증서 소유자가 인증서를 발행 받은 조직을 탈퇴하거나 인증서의 공개키에 부합되는 비밀키가 손상되었거나, 유출이 의심스러운 경우등 에는 유효기간이 만료되지 않은 인증서라 할지라도 취소될 필요가 있다. 인증서를 취소하기 위해 X.509에 정의된 매커니즘이 인증서 폐지 목록(Certificate Revocation List : CRL)이며 X.509 V2 인증서 폐지 목록의 형식은 그림 3과 같다.

서명 알고리즘(Signature)은 인증서 폐지 목록에 서명한 서명 알고리즘 및 관련 파라미터이다. 발급자(Issuer)는 발급자 CA의 X.500 이름을 나타낸다. 최근 수정일자(Last Update)는 인증서 폐지 목록의 최근 수정일자이며, 차후 수정일자(Next Update)는 다음 수정일자를 말한다. 폐지된 인증서 목록(Revoked Certificates)은 폐지된 인증서 목록들을 기술한다. 확장자(Extension)는 인증서 폐지 목록의 확장자 유무 및 내용을 나타낸다. 발급자 서명문(Issuer's Signature)은 발급자의 서명문을 표시한다.[1][2]



〈그림 3〉 X.509 V2 인증서 폐지 목록

III. CRL 분배점을 이용한 인증서 폐지 목록 관리

인증서에 대한 폐지 목록을 관리하는 전통적인 방법은 인증서 폐지 목록(Certificate Revocation List : CRL)을 주기적으로 발행하는 것이다. CRL은 CA 도메인 내의 취소된 모든 인증서의 일련번호를 포함하고 있는 타임 스탬프 되고 전자 서명된 목록이다. 이러한 구조를 보다 효율적으로 사용하기 위해 CRL을 기반으로 한 많은 구조들이 수정되고 확장되었다.[3]

CRL 분배점은 CRL의 최대 크기를 주소화하는 방법을 사용하여 CRL 구조를 확장한 것이다. 하나의 CA에 대한 전체 사용자 수를 세그먼트 수로 나눈 값으로 CRL 크기를 정한다. 각 세그먼트는 CRL 분배점과 연계되어 있으며 다른 호스트나 디렉토리에 위치한다. 각 인증서내에는 CRL 분배점의 위치에 대한 포인터를 가지고 있어, 폐지 정보위치에 대한 분배점을 찾거나 사전지식이 없어도 된다. 인증서 내부에 인증서 폐지 목록을 분배하는 위치를 적어놓으면 디렉토리든 웹사이트든 해당 주소에 접근하여 인증서와 관련된 인증서 폐지 목록을 얻을 수 있다.[4][5]

예를 들어 송신자 A가 수신자 B에게 자신의 신분을 증명하기 위해서는 송신자 A의 인증서를 발행한 CA의 인증서, 인증서 폐지 목록, 송신자 A의 인증서를 제공한다. 송신자 A의 인증서 유효성을 검증하기 위해서 수신자 B는 CA의 인증서 폐지 목록을 검사하거나 OCSP(Online Certificate Status Protocol)

를 이용한다.[5] 거대한 공개키 기반구조의 공동체에서는 인증서 폐지 목록이 자주 발행되며 인증서 폐지 목록의 크기 또한 커진다. 그러므로 응용 프로그램은 과중한 부하를 갖는 디렉토리로부터 최신의 인증서 폐지 목록을 검색하는 데 많은 시간이 소요된다. 더욱이 수신자가 인증기관의 인증서 관리 시스템에 인증서 조회 요청 메시지를 송신함으로서 인증서 폐지 목록을 조회할 때마다 부하가 가중될 뿐만 아니라 시스템 자원과 성능 측면에서 비효율적이다.

CA가 발행한 전체 인증서 수를 n, 만료되기 전에 폐지되는 인증서 폐지 비율을 p, 하나의 CA가 관리하는 평균 인증서 수를 k, 일일 인증서 상태 예상 조회수를 q라 가정하면 CA가 디렉토리내에 인증서 폐지 목록을 갱신하기 위해 소요되는 부하는 수식 (1)과 같고, 인증서의 유효성을 확인하기 위해 사용자가 디렉토리내의 인증서 폐지 목록을 조회시 소요되는 부하는 수식 (2)와 같다.

$$T_{CRLUpdate} = 20 \times p \times n \quad (1)$$

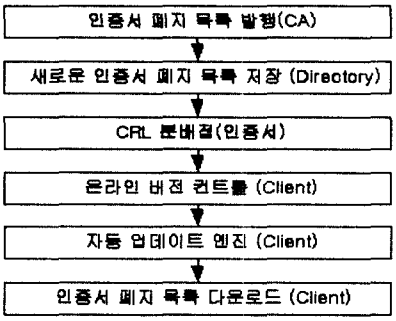
$$T_{CRLQuery} = 68 \times p \times k \times q \quad (2)$$

예를 들어 인증서 폐지 목록의 갱신 주기를 3일이라고 가정한다면, 하루에 소요되는 디렉토리 조회 비용은 수식(2)의 q에 크게 의존하지만 인증서 폐지 목록을 자신의 PC에 다운로드해 두면 인증서 폐지 목록내의 다음 발행 시간(NextUpdate)이내에는 디렉토리를 조회하지 않아도 된다.

인증서 폐지 목록을 다운로드하기 위한 알고리즘은 다음과 같고, 디렉토리의 현재 상태를 버전 컨트롤 프로그램이 감시하고 있다가 디렉토리 내에 새로운 인증서 폐지 목록이 발행되면 PC내의 자동 업데이트 엔진이 자신의 인증서 내에 있는 인증서 폐지 목록 분배점을 이용하여 다운로드 한다.

```
CheckCRLUpdateVersion :
if(CurrentTime>revocationInfo[DpNo].nextUpdate){
then EXPIRED_BASE;
      CRLDownload(revocationInfo[DpNo]); }
CRLSignedVerify((Asn1Primitive*)&((crl)
      ->toBeSigned.self),&((crl)->algorithm),
       &((crl)->signature),(provider),(key)) )
CertVerify(cert, provider, key)
```

디렉토리에 대한 부하를 분산시키는 방법으로 인증기관의 디렉토리 내에 새로운 인증서 폐지 목록이 발행되면 사용자가 자신의 PC로 다운로드 하는 방법을 그림 4와 같이 제안하였다. 인증서의 유효성을 검증할 때마다 해당 디렉토리에 조회하지 않고 사용자의 PC에 저장된 인증서 폐지 목록을 사용하므로 인증서 폐지 목록내의 다음 발행 시간(NextUpdate)때까지 디렉토리 조회에 대한 부하를 줄일 수 있다.



〈그림 4〉 제안한 인증서 폐지 목록 관리

Ⅳ. 결 론

많은 사용자가 동시에 인증서의 유효성을 검사할 때마다 디렉토리로부터 인증서 폐지 목록을 요청하면 디렉토리의 부하를 가중시키고 많은 지연이 발생하므로, 본 논문에서는 사용자의 디렉토리 조회에 대한 부하를 분산시키기고 효율적인 유효성 검사를 위해, 사용자 PC내에 자동 업데이트 엔진을 두어 CRL 분배점을 통한 최신의 인증서 폐지 목록을 다운로드할 수 있도록 제안하였다. 송신자의 인증서와 PC내에 저장된 인증서 폐지 목록을 사용하여 수신자는 송신자의 인증서에 대한 유효성을 확인할 수 있다. 향후 인증서 폐지 목록 분배점과 함께 델타 CRL이나 간접 CRL등의 확장된 방법을 제안한 방법과 접목하여 보다 효율적인 인증서 폐지 관리에 대한 연구가 필요할 것이다.

참 고 문 헌

[1] 이만영,김지홍,류재철,송유진,염흥렬,이임영, "전자상거래 보안 기술", *생능출판사*, 1999

[2] NIST, "Public Key Infrastructure Study:Final Report", Gaithersburg, MD, April 1994.

[3] D. A. Cooper, " A model of certificate revocation", *In Proceedings of the Fifteenth Annual Computer Security Applications Conference*, pp. 256-264, Dec. 1999.

[4] D. A. Cooper, " A more effcient use of Delta-CRLs ", *Drafts for IEEE Symposium on security and privacy*, May 2000.

[5] M. Noar and K. Nassim, "Certificate Revocation and Certificate Update", *In Proceedings of the 7th USENIX Security Symposium*, pp. 217-228, Jan. 1998.