PKI환경에서의 다중 CA를 위한 효율적인 인증서 폐지 검증 방안에 관한 연구

김경희[U], 송주석
연세대학교 컴퓨터과학과
e-mail : {kkh[0], jssong}@emerald.yonsei.ac.kr

A Study on the efficient Certificate Revocation Validation Method to multiple CA for the PKI

Kyung-Hee Kim[U], Joo-Seok Song
Dept. of Computer Science, Yonsei University

요 약

전자 신뢰 매커니즘 기반의 정보사회에서는 기밀성과 인증의 확보가 필수적이며, 이를 위해서는 전자서명 기술을 포함하고 있는 공개키 기반의 인증서관리 체계의 확립이 선결되어야 한다.[3] 인증서의 정당성을 검증하기 위해 검증자는 소유자의 인증서와 그 인증서를 인증한 공인인증기관의 인증서를 검증해야 하고, 그 이전에 인증서 폐지 여부를 확인해야 하며, 실제 공개키 기반구조 환경에서 인증서의 유효성을 검증하기 위해서는 인증서 자체 검사와 함께 최상위 인증기관(루트CA)으로부터 사용자에게 인증서를 발행한 단말CA까지의 인증트리를 검증해야 한다[3]. 본 연구에서는 효율적인 인증서 폐지정보의 검증을 위해 다중 CA환경에 적합한 NPKI상에 B-Tree데이터구조를 적용하는 인증서 폐지 검증 방안을 제안하고자 한다.

1. 서 론

최근 전자서명 기술이 발달함에 따라 이 연구된 것이 신뢰기관인 인증기관에 의해 전자 서명된 인증서를 사용하는 인증서 기반의 공개키 기반구조(Public Key Infrastructure: PKI)이다[3]. 실제 PKI환경의 응용체계에 대한 인증서는 인증기관(Certificate Authority: CA)에 의해 전자서명으로 생성되어 각 개체에 대한 암호학적 공개키와 속성, 능력들을 결합하여 형성된 객체이며, 인증서 내용을 검증하기 위해서 검증자는 CA의 공개키를 이용하고 인증서의 폐지 여부 확인을 위해 매우 효율적인 인증서 폐지확인을 위한 검증방안들이 요구되고 있다[4].

2. 연구배경

PKI 운영에 있어서 인증서의 생명주기는 제한적이며, 폐지는 CA 또는 최종사용자에 의해 주기 안에 여러 이유로 필수적으로 발생함으로, 최종사용자의 인증서 검증시 폐지목록의 폐지여부에 대한 빠른 응답을 위해 인증서 폐지방안이 필요하고, 인증서 폐지목록(CRL), 인증서폐지트리(CRT), 인증서폐지시스템(CRS), 온라인 인증서상태확인프로토콜(OCSP)등이 있다[1]. 그러나 종전의 연구기준은 단독 CA에 대해서 다수의 인증서를 발행하고 인증서 폐지정보의 처리를 위해 복수의 CA들 대신에 단독 폐지주체(CA)를 통해 운영되었다. 이것은 모든 폐지 정보를 집합시키는 데는 유리하나, CA들간의 메시지 처리시 통신부하가 발생하고, 복수의 CA들은 폐지주체에게 폐지책임을 위임한다. 즉, 중앙 집중식의 폐지주체는 상호연동이 필요한 CA들이 있는 분산된 PKI에 부적절하다[2]. 또한 검증자는 최종사용자의 공개키를 얻기 위해 인증경로 검증이 필요하며 최종사용자는 경로상의 모든 인증서의 폐지 상태를 검사하고 모든 CA들로부터 폐지정보를 획득하며, 경로상의 CA의 수가 증가할수록 인증서 폐지 검증의 어려움은 더욱 증가됨을 알 수 있다[1].

본 연구에서는 분산된 PKI 환경에서 적합한 다중 CA를 고려한 NPKI(Nested PKI)상에 신속한 인증서 폐지의 검증을 위해 M-ary 검색트리의 특성을 갖고 빠른 검색을 하는 B-Tree 데이터구조를 적용한 효율적인 인증서 폐지 검증 방안을 제안하고 그 성능을 검증하고자 한다.

3. 제안하는 인증서 폐지 검증 방안

PKI환경의 다중CA를 위한 NPKI상에 B-Tree구조를 적용하여 인증서 폐지여부를 검증하는 인증서 검증방안을 연구한다.

3.1 B-Tree 인증 검증 트리

3.1.1 B-Tree 인증 검증 트리 구성

B-Tree는 그림1과 같고, 인증서 검증을 위해 단계별 CA와 최종 사용자간에 모든 인증서 구성은 다음과 같다[1].

그림1 B-TREE (M, L=5)

1) 인증서의 형식은 ITU-T X.509 v3를 준용한다.[3]
2) 인증서 폐지목록은 ITU-T X.509 v2를 준용한다.[3]
3) 각 노드는 인증서와 인증경로의 해쉬로 구성하며, "충돌회피"와 "강한 일 방향" 성질을 갖는 해쉬함수(SHA-1)로 인증서와 공개키 및 시간정보를 해쉬를 통해 생성, 이용된다.
4) B-Tree의 형제노드의 해쉬값(HV)은 그 부모노드의HV를 얻기 위해 함께 루트노드의 생성시까지 해싱되고 루트노드의 HV와 시간정보는 CA에 의해 서명된다.
5) 인증서 경로 검증은 루트CA로부터 종단CA까지 사용자가 순차적으로 모두 검증하며, 아래의 조건을 만족하면서 n개의 인증서가 있다고 가정한다[3].
- {1,(n-1)}에 속하는 모든 x에 대하여, 인증서x의 소유자는 인증서 x+1을 인증한다.
- x=1(루트CA)인 인증서는 자기 스스로가 인증한다.
- x=n인 인증서는 최종의 마지막 사용자 인증서이다.
6) 트리는 신규 CA를 위해 증가되고 기존 CA를 위해 단 1회에 모두 생성이 가능하고 매일 규칙적으로 증분되며 갱신된다.
7) 각 노드의 CA키는 2048-4096 bit로 하며 CA키의 변화시 CA는 신규 키로 기존 루트노드를 재 서명한다.
8) 인증서 검증을 루트CA키 갱신 절차는 RFC 2459를 준용한다[3].

3.1.2 분 석

1) 트리 검색을 위한 공통의 인덱스구조를 증가시켜 분리된 폐지정보를 유지하는 비용을 감소하기 위해 CA에 의해 분배되는 모든 인증서를 B-Tree 데이터구조에 생성한다[1].
2) 경로를 검증하는데 요구되는 HV와 인증서를 포함하는 노드로부터 루트노드까지의 경로를 "인증서를 위한 인 증경로(Cert Path)"라고 한다.
3) 사용자의 인증서 요구시 Root노드의 HV에 서명이 있는 인증서의 인증경로를 추가로 제공하며 이 정보는 인증서의 최신 갱신정보가 유효한지를 증명한다.

3.2 다중 CA를 위한 NPKI

3.2.1 Nested 인증서 및 인증서 폐지 원리

NPKI(Nested certificate based on PKI)는 Nested 인증서를 기초로 하며, 다른 인증서에 대한 인증서로써 이런 인증서를 Subject인증서라고 하며 CA는 Nested 인증서를 발행하기 전에 Subject 인증서를 검증해야 하며 CA는 NPKI에서 자식노드에 의해서 발행되는 각 인증서에 대해 하나의 Nested 인증서를 발행한다[2].

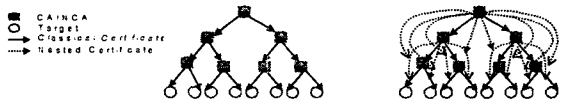

그림2 PKI / NPKI

그림3 기존 인증서경로 / Nested 인증서경로

그림2, 3에서 PKI와 NPKI를 비교, 설명한다.[2] CA는 Nested 인증서를 발행하기 전에 종속되는 인증서를 증명한다. 여기서 NPKI의 인증서 폐지 규칙은 다음과 같다.[2]
1) NPKI의 Leaf노드의 기존 인증서는 폐지가능하며 이런 인증서에 주어진 보증(guarantee)은 폐지 후에 무효화된다.
2) 기존 폐지인증서가 있는 Nested 인증서경로는 무의미하므로 경로상의 모든 인증서들은 별도로 폐지할 필요가 없다.
3) 폐지된 Nested 인증서가 있는 경로 상에서도 다른 인증서의 사용이 여전히 사용 가능하다. 그림4에서 CA,b가 NC_1의 폐지 전인 $T_2 > T_1$에 NC_2를 발행했으므로 유효한 NC_2의 Subject 인증서로서 여전히 NC_1을 검증할 수 있고, a의 위조품은 키 손상 후 $T_3 > T_2$에 불필요한 정보 NC_3를 발행할 수 있는데 b와 다른 유효한 CA들은 NC_3를 검증할 수 없으며 즉, Nested경로의 첫 번째 인증서로 암호학적으로 검증이 불가하므로 인증서는 의미가 없다.

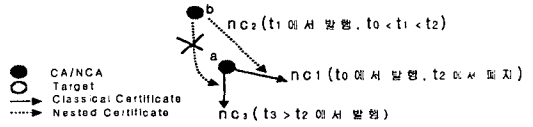

그림4 Nested 인증서 폐지의 예

4) Nested인증서는 사용자의 공개키에 대한 인증 대신 서명과 Subject인증서의 원천 내용의 관계만을 인증하므로 Nested 인증서 폐지는 그 인증서의 CA가 Subject인증서의 서명을 더 이상 증명할 수 없지만 그 인증서의 서명은 발행자의 공개키를 이용하여 암호학적으로 검증이 가능하다.

3.2.2 다중 CA를 위한 NPKI 분석

1) 검증자는 경로길이에 관계없이 경로상의 2개의 인증서 폐지상태를 검사한다. 하나는 검증된 첫 번째 Nested 인증서로써 허위의 인증서에 대한 검증을 방지하고자 검사되며 두번째 인증서는 경로상의 마지막 인증서이다. 이유는 기존 인증서와 폐지 인증서는 사용되어 질 수 없기 때문이다.
2) 인증서의 폐지로 인해 그 공개키는 무효하므로 폐지시간 후에는 검증 불가하지만 폐지된 키에 의해 발행된 기존 인증서가 Nested 인증서를 가지고 있다면 기존 인증서에 대한 유효함도 검증될 수 있다.
3) Nested 인증서는 기존 인증서보다 작게 발행해도 무방하다. 이것은 기존 인증서가 없어도 발행할 수 있기 때문에 제한된 신뢰정보로도 발행할 수 있다. 즉 Nested CA는 CA의 공개키를 알기 때문에 인증서의 서명의 유효함을 검증할 수 있으나, 인증서 내용은 신뢰할 수 없다. 결국 Nested CA는 각 개체에 대한 기존 인증서는 발행할 수 없고 기존 인증서에 대한 Nested 인증서는 발행이 가능하다. 그 이유는 기존 인증서에 대한 서명의 유효성은 검증가능하나, Nested 인증서에 대한 서명의 정확성은 보장이 안 된다.

4. 검 증

4.1 기존 인증서 폐지 스킴과의 성능 비교[1][2][4]

표1 기존스킴과의 비교

구 분	CRL	CRT	CRS	OCSP	제안방안
성능 (요구율)	×	○	△	○	○
적시성	×	△	△	○	○
확장성	×	×	×	×	○
보안성	×	×	×	×	○
관리성 (복잡성)	○	○	△	○	×

1) CRL은 폐지목록을 정기적으로 발행하지만 수행성능이 낮고(목록크기 다량 요구) 다중CA를 고려하지 않았다. 그러나 분할(segmentation)하여 확장성(scalibility), Delta-CRL 갱신을 통해 적시성(timeliness)을 높이고 과잉발행을 통해 클라이언트의 최대 요구율을 감소시킴으로써 적응성과 표현력을 증가시킨다.

2) OCSP는 실시간 폐지스킴이 아니라 요구/응답스킴으로 제한적이고(응답 생성시 매번 전자서명 필요) 서버(Responder)를 구성해야 하므로 프로세싱 부하가 많고 외부 공격 위협이 크다.

3) CRT를 제외한 대부분이 특정한 폐지정보의 포함하는 표현력이 부족하고 CRT발행자는 정보 갱신시 모든 트리를 재 계산해야 하므로 상태 정보 배포시 많은 시간을 소요한다.

4) 기존 폐지 검증 방안은 분리된 폐지 데이터를 유지하는 비용과 개별적인 인증서 서명이 요구되는 비효율성이 있다.

4.2 검증결과

4.2.1 성능 검증

1) B-Tree의 인증 검증트리의 데이터구조를 아래와 같은 조건에 따라 성능을 검증한다.

- 요구조건
  - 데이타 블록 : 8,192bytes(Key : 32bytes)
  - B-Tree Total Size : (32M-32bytes)+M Branch
  - 분기(Branch) Size : 4Mbytes(1branch=4bytes)
  - Non-Leaf Node Total 메모리 요구량: 36M-32bytes
  - 데이터 레코드 : 256bytes · 16 < leaf < 32 record
- 성능 결과
  - Disk Block을 위한 M의 최대값 = 228
    : (36*228)-32=8176 < 8192bytes(32*256)
  - 블록 당 32 레코드(L=32)
  - 각 내부노드(Root를 제외)는 최소 114개로 분기

즉, 500만 레코드를 검증하려면 312,500 leaves가 필요하며 최악의 경우 leaf들이 Level 4에 있다면 접근 수는 $Log_{m/2}N$이 된다. (Root와 Level 2는 주 메모리에 캐쉬 되므로 디스크 접근은 Level 3 이하 Level에서만 요구함) 즉, 이진트리(Log_2N)에 비해 M-ary 검색 트리를 갖는 B-Tree 데이터구조는 Log_MN의 성능을 나타낸다.

2) OCSP 스킴과의 성능비교(30,000만 메시지처리/1일)

표2 서명 및 검증 성능 비교

구분	OCSP	제안 방안
서명	1,250대 / 초	높이: 30, Hash: 20
검증		(최상위 10단계 캐싱): 3대/초

4.2.2 결 과

1) 성능 : Nested 인증서를 통해 검증자는 기존 인증서 CA의 서명 유효성과 인증서 폐지 여부를 공개키 없이도 검사할 수 있는 다중 CA를 위한 신뢰체계를 지원한다. 또한 많은 서명을 검사하는 검증자에 대해 디렉토리의 통신부하는 B-Tree의 상위부분의 캐싱을 이용하여 감소되고 인증서 정보를 보유하고 있는 데이터구조의 높이를 단축하고 분기를 증가시켜 검색 수행시간을 Log_M N까지 향상될 수 있다.

2) Security : CA는 B-Tree의 Root와 부합되는 서명과 필요한 인증서의 인증경로를 저장하므로 기밀성, 무결성을 보장하고 CA키의 변화 시 CA는 신규 키로 기존 루트를 서명하고 기존 Root의 현재 서명을 검사함으로서 인증서의 부인방지를 보장하고 Attacker로부터의 안전성을 위해 2048~4096bits키를 이용하며 CA는 신규 키쌍을 생성하고 인증을 통하여 신규 공개키를 브로드캐스트한다. 신규 개인 키로 현재 Root값에 서명한 후 다음의 서명을 위해 신규 개인 키를 이용하므로 협상이 될 CA의 개인 키로 인증서 생성 위조를 방지한다.

3) 검증계산능력 : 개별적인 인증서의 서명이 불필요하므로 CA의 계산처리 부하가 감소되고 처리속도가 증가한다. 또한 인증서의 서명에 대한 검증을 감소하는 것은 CA와 디렉토리 간의 프로세스 부하의 감소 및 클라이언트 요구에 대한 더 빠른 응답을 제공할 수 있다.

4) 통신속도 및 부하 : B-Tree에서 해쉬기법(SHA-1)을 통한 압축형태로 폐지정보를 전송하고 폐지상태의 최소한의 근거를 최종사용자에게 제공하는 것으로 클라이언트의 요구에 대한 OCSP의 프로세싱 부하와 CRL에 포함된 통신부하를 다소 해결할 수 있다.

5) Off-Line(스마트카드) 이용 가능 : 최종사용자는 현재 루트 CA와 최종사용자간의 인증경로를 저장하여 스마트카드를 이용하여 Off-Line검증을 함으로써 온라인 검증을 하는데 필요한 요구 소요를 감소시킨다.

5. 결 론

분산된 PKI환경에서 다중 CA를 위한 적응을 위해 Nested PKI상에 B-Tree 데이터구조를 적용한 효율적인 인증서 폐지검증 방안은 기존 인증서 폐지스킴 보다 수행성능과 검증계산능력, 통신속도 면에서 뛰어나며 안전성 면에서도 만족한다. 향후에는 본 연구를 토대로 한 알고리즘 시스템성능 구현 및 상호연동기반에서의 인증에 관한 연구를 수행할 것이다.

6. 참고문헌

[1] I. Gassko, P. Gemmell, P. MacKenzie, "Efficient and Fresh Certification", 2000

[2] Albert Levi, Cetin Kaya koc, "Reducing Certificate Revolution Cost using NPKI", 1998

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

[4] Moni Naor, Kobbi Nissim,"Certificate Revocation and Certificate Update",7th USENIX Security symposium, 1998