인증서 검증 시스템의 검증시간 비교분석에 관한 연구

김현철° 이옥경 이용준 오해석
숭실대학교 컴퓨터학과
dmzpolice78@korea.com° oklee017@lycos.co.kr yjlee@koscom.co.kr oh@computing.soongsil.ac.kr

A Study on Validation Time Analysis of Certificate Validation System

Hyun-Chul Kim°, Ok-Kyoung Lee, Yong-June Lee, Hae-Seok Oh
Dept. of Computer Science, SoongSil University

요 약

개방형 네트워크인 인터넷에 급속한 발달로 인하여 Offline상에서 처리되던 기존의 업무들이 Online상의 업무로 빠르게 전환되어 가고 있다. 하지만 Online상에서의 업무처리는 항상 개인 정보누출, 개인정보의 위조 및 변조의 문제를 내포하고 있으며, 위와 같은 문제를 해결하기 위한 대안으로 PKI 기반의 인증서 검증 시스템이 제안 되었고 현재도 연구가 계속 되어지고 있다. 본 논문에서는 PKI 기반의 인증서 상태검증 방식 중의 하나인 CRL기반의 인증서 상태 검증 방식과 OCSP기반의 인증서 상태 검증 방식의 대하여 기술하고, 실시간으로 인증서 상태를 검증 할 수 없는 CRL기반의 인증서 상태검증 방식의 단점과 네트워크 상태의 따라 인증서 검증 속도가 달라지는 OCSP기반의 인증서 상태 검증 시스템의 단점을 해결하기 위한 데이터베이스를 이용한 클라이언트-서버 기반의 인증서 상태 검증 시스템을 제안하고, 실제 실험을 통해서 CRL기반의 인증서 검증 시스템과 OCSP기반의 인증서 검증 시스템 그리고 제안하는 데이터베이스를 이용한 클라이언트-서버 인증서 검증 시스템의 검증속도를 비교해 보고자 한다.

1. 서 론

오늘날 개방형 네트워크인 인터넷의 급속한 발전으로 인하여 그동안 오프라인으로 처리되었던 많은 업무들이 온라인 처리로 전환되어 가고 있다. 하지만 개방형 네트워크인 인터넷에서의 업무처리는 개인 정보의 누출, 개인 정보의 위조 및 변조 등과 같은 위협요소를 항상 내포하고 있으며 이러한 개인 정보 노출에 대한 위협요소를 해결하기 위해서 PKI(Public Key Infrastructure) 기반에 인증서 검증 방식이 제안되었고 현재도 연구가 계속 되어지고 있다.

이와 같은 PKI 기반의 인증서 검증 시스템을 사용하기 위해서는 인증서가 유효한지를 검사하는 유효성 검사 즉 검증이라는 과정을 거쳐야 하는데 현재 사용되고 있는 인증서 상태 검증 방식에는 CRL(Certification Revocation List), Delta-CRL, OCSP(Online Certificate Status Procol), SCVP(Simple Certificate Validation Protocol) 등과 같은 방식이 있다.

본 논문에서는 PKI 기반의 인증서 상태 검증 방식 중의 하나인 CRL기반의 인증서 유효성 검증 방식과 OCSP기반의 인증서 유효성 검증 방식의 대하여 2장에서 기술하고, 실시간으로 인증서 상태를 검증 할 수 없는 CRL기반의 인증서 유효성 검증방식의 단점과 네트워크 상태의 따라 인증서 검증 속도가 달라지는 OCSP기반의 인증서 유효성 검증 시스템의 단점을 해결할 수 있는 데이터베이스를 이용한 클라이언트-서버 기반의 인증서 유효성 검증 시스템을 3장에서 제안한다. 4장에서는 실제 실험결과를 통해 CRL기반의 인증서 검증 시스템과 OCSP기반의 인증서 검증 시스템 그리고 제안하는 데이터베이스를 이용한 클라이언트-서버 인증서 검증 시스템의 검증속도를 비교분석해 보고 5장에서 결론을 맺는다.

2. 관련 연구

PKI 기반의 인증서 검증 방식은 공인인증기관에 대한 인증서 발급 및 관리를 하는 ROOT CA(ROOT Certification Authority), 인증서를 발행하거나 취소를 담당하는 CA(Certification Authority), CA의 업무를 분담하여 USER들에 대한 인증서 등록과 발급을 대행하는 RA(Registration Authorith), 인증서와 사용자 관련정보들을 저장하는 장소로 사용하는 Directory, 인증서를 직접 사용하는 USER로 구성된다.[3]

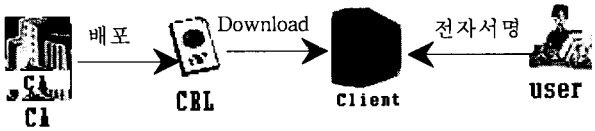
PKI 기반의 인증서 검증 방식은 Public key와 Private

key 한 개의 키 쌍을 이용하여 암호화를 수행하는 방식을 사용한다. 즉 누구나 알 아 볼 수 있도록 공개하는 Public key(암호화키)와 자신만이 알 고 있는 Private key(복호화키)를 이용하여 암호화를 수행하는데 암호화와 복호화에 사용되는 키가 서로 다르기 때문에 암호화 키가 다른 3자에게 공개 되더라도 복호화키를 알지 못하면 암호화된 암호문을 평문으로 만들 수 없도록 하는 방식을 사용하는 암호화 시스템이다.[2]

2-1 CRL(Certification Revocation List)

현재 사용되고 있는 인증서는 CCITT에서 제정한 X.509v3이다. 인증서 유효기간은 인증서 발급일로부터 1년이며 USER에 개인키가 노출 되었을 때, USER가 인증서 취소를 요청 했을 때, 상위 CA의 비밀키가 노출되었을 때, USER가 인증서를 발행했던 조직으로부터 퇴직 했을 경우와 같이 몇 가지 이유로 인해 인증서 유효기간 이전에 폐지 될 수 있다. 위와 같이 폐지된 인증서가 불법적으로 사용되거나 도용되는 것을 막기 위해 폐지된 인증서를 하나의 리스트로 모아놓은 것이 CRL(인증서 폐지 목록)이다.[1,3]

하지만 CRL은 인증서의 발급이 증가할수록 폐지되는 인증서의 양도 증가하기 때문에 CRL을 보관하기 위한 파일에 크기 또한 기하급수적으로 증가한다는 단점과 하루에 한번씩 인증서 폐지목록을 다운 받기 때문에 실시간으로 인증서 상태를 검증 할 수 없다는 단점이 있다.[1] CRL을 이용한 인증서 검증 방식에 대한 처리과정은 [그림1]와 같다.



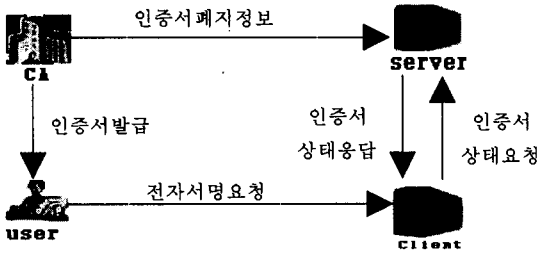
[그림 1] CRL기반의 인증서 검증 방식 수행과정

2-2 OCSP(Online Certificate Status Protocol)

OCSP는 CRL기반의 인증서 검증 방식에 문제점인 인증서에 대한 실시간 상태 검증을 해결하기 위해 제안된 인증서 상태 검증 방식으로 1999년 6월 IETF RFC2560 문서에 의해 공포되었다.[4]

OCSP기반의 인증서 검증 방식은 OCSP클라이언트가 CRL을 요청하지 않고 인증서의 현재 상태를 검증하기 때문에 실시간으로 인증서에 대한 상태 검증을 할 수 있다는 장점이 있는 반면 실시간으로 인증서에 대한 유효성 검사를 수행해야 하기 때문에 많은 통신량으로 인한 네트워크 과부하 문제를 발생시킨다는 단점과 네트워크 상태의 따라 인증서 유효성 검사의 수행시간이 달라진다는 단점이 있다.

OCSP 인증서 상태 검증 방식은 USER가 CA로부터 인증서를 발급받은 후 USER가 정해진 포맷으로 OCSP 클라이언트에게 전자서명을 요청하면 OCSP 클라이언트는 정해진 포맷으로 OCSP서버에게 인증서 상태를 요청하고, OCSP서버는 요청받은 인증서에 대한 상태 정보를 검색하여 전자 서명을 수행한 후 수행 결과의 대한 응답을 OCSP 클라이언트로 넘겨줌으로써 실시간으로 인증서의 대한 유효성 검사를 수행하는 방식이다.[4,5] OCSP 기반의 인증서 검증 방식 수행과정은 [그림2]와 같다.



[그림 2] OCSP기반의 인증서 검증 방식 수행과정

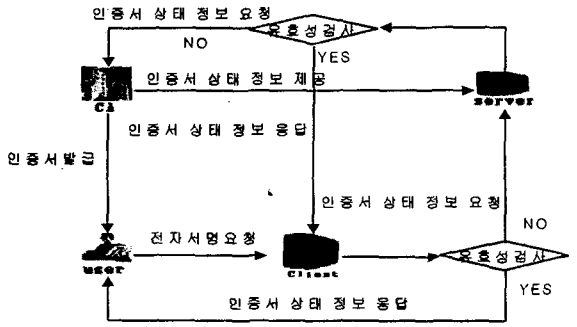
3. 제안하는 시스템

3.1 클라이언트

전자서명을 요청한 USER에 대한 인증서 상태가 클라이언트 데이터베이스에 등록이 되어 있으면 클라이언트 자체적으로 인증서 유효성 검사를 수행하고, 만약 클라이언트 데이터베이스에 요청한 인증서 상태가 없다면 서버로 인증서 상태를 요청, 응답의 결과를 클라이언트 데이터베이스에 저장함으로써 반복적인 인증서 상태 조회의 따른 인증서 상태 검증 속도를 개선시킬 수 있다.

3.2 서버

서버에서는 CA에서 제공하는 인증서 정보를 데이터베이스에 가지고 있으며, 클라이언트에서 인증서 상태 정보를 요청하면 서버 자신의 데이터베이스를 검색하여 요청한 인증서 상태 정보가 데이터베이스에 있다면 클라이언트로 인증서 정보를 넘겨주고 인증서 상태 정보가 데이터베이스에 없다면 CA에게 인증서 정보를 요청 응답의 대한 결과를 클라이언트에게 넘겨줌으로써 인증서 상태 정보를 실시간으로 반영할 수 있다. 제안하는 시스템은 [그림 3]과 같다.



[그림 3] 제안하는 시스템 인증서 검증 방식 수행과정

4. 실험 및 평가

4.1 전제 조건

본 논문에서는 CRL 기반의 인증서 상태 검증에 관한 수행 시간을 측정하기 위해서 인증서 상태 검사를 수행할 CRL은 이미 클라이언트 컴퓨터상에 다운로드 되어 있으며, 인증서 유효성 검증에 모든 처리 과정 즉 전자서명을 요청하고 전자 서명 요청에 대한 검증을 수행하는 모든 과정이 클라이언트 컴퓨터상에서 이루어진다는 전제하에 CRL 기반의 인증서 유효성 검증 수행 시간을 측정하였으며 또한 OCSP 기반의 인증서 검증에 관한 수행 시간 측정은 현재 실제 사용되고 있는 OCSP 기반의 인증서 검증 시스템에서의 인증서 유효성 검사 시간을 측정 하였다.

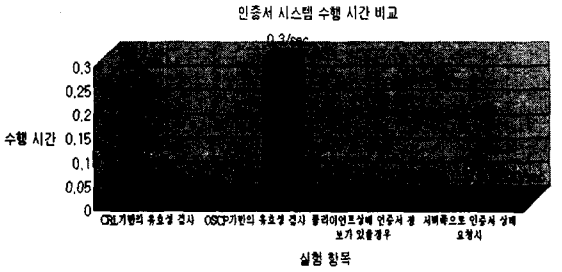
4.2 실험 및 평가

본 논문에서는 CRL기반의 인증서 상태 검증 방식의 인증서 상태 검증 시간, OCSP기반의 인증서 상태 검증 방식의 인증서 상태 검증 시간 그리고 본 논문에서 제안하는 데이터베이스를 이용한 클라이언트-서버 방식의 인증서 상태 검증 방식에 대한 인증서 상태 검증 시간을 측정 하였으며, 실험 내용의 대한 결과는 아래와 같다.

CRL처리를 하였을 때의 인증서 상태 검증 시간을 측정 하였을 때 수행 시간은 0.000151/sec, OCSP상에서의 인증서 상태 검증 시간 측정을 하였을 때 0.3/sec가 소요되었다. 제한하는 시스템에서는 두 가지 경우에 대하여 인증서 검증 시간을 측정 하였다.

첫째 : 클라이언트 데이터베이스에 인증서 상태 정보가 있을 경우에 인증서 유효성 검사 수행 시간은 0.000006/sec 이다.

둘째 : 클라이언트 데이터베이스에 인증서 상태 정보가 없어서 서버 쪽으로 인증서 상태 정보를 요청하고 서버로부터의 결과 응답까지의 수행 시간은 0.000020/sec이다. [그림4] 각 실험 항목에 대한 결과를 나타내고 있다.



[그림 4] 각 항목별 수행 시간 비교

5. 결론

본 논문에서는 PKI 기반의 인증서 시스템에서의 CRL 기반 인증서 상태 검증 방식과 OCSP기반 인증서 상태 검증 방식에 대한 이론적인 배경을 기술하였고, CRL기반 인증서 상태 검증 방식의 단점인 실시간 처리를 할 수 없다는 점과 OCSP기반 인증서 상태 검증 방식의 단점인 네트워크 상태의 따른 인증서 상태 검증 시간이 달라지는 문제를 해결하기 위한 데이터베이스를 이용한 클라이언트-서버 기반의 인증서 상태 검증 방식을 제안하였다.

본 논문에서의 실험결과는 로컬 시스템 상에서 이루어졌다는 점에서 문제가 있을 수 있다. 따라서 향후에는 본 연구 결과를 토대로 다수의 시스템 상에서 본 논문에서 제안한 방식을 적용할 수 있도록 계속 연구를 진행해 나갈 것이다.

참 고 문 헌

[1] J. Willemson "Certificate Revocation Paradigms" Technical Report, Cybernetica. 1998

[2] Russ Housley & Tim Polke "Planning for PKI" WILEY. 2001

[3] 권태경, 강명호, 김승주, 서정욱, 진승헌 "정보 보호 표준 개론" 한국정보통신기술협회. 2002

[4] M.Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. "Internet X.509 Public key Infrastructure On-line Certificate Status Protocol-OCSP",RFC2560, 1999

[5] M.Myers, R. Ankney, C. Adams, S. Farrell and C. Covey "Online Certificate Status Protocol, Version2" draft-ietf-pkix-ocspv2-02, March 2001.