축약 서명 기반의 효율적인 인증서 상태 검증 시스템에 관한 연구

김현철° 이광형 백주호 오해석
숭실대학교 컴퓨터학과
dmzpolice78@korea.com° loke7777@hotmail.com baekjuho@hanmail.net oh@computing.soongil.ac.kr

A Study on Efficient Certificate Status Validation System of Reduction Signature Basis

Hyun-Chul Kim° Kwang-Hyoung Lee Ju-Ho Baek Hae-Seok Oh
Dept. of Computer Science, SoongSil University

요 약

개방형 네트워크인 인터넷에서의 모든 정보 교환은 항상 정보의 노출 및 정보의 위조 및 변조 등의 위협요소를 배후에 내포하고 있다. 이러한 인터넷에서의 중요 정보 보호를 위해서는 모든 정보 교환에 있어서 정보의 불법노출을 방지하기 위한 기밀성, 정보의 위조 및 변조 여부를 판단하는 무결성, 정보의 송신자와 수신자 사이에 송수신 사실을 부인하지 못 하도록 하는 부인방지, 전송된 정보의 송신자와 수신자를 확실하게 증명해주는 인증 등의 기능들이 제공되어야한다. PKI 기반의 인증서 상태 검증 시스템은 위와 같은 4가지의 기능을 제공해 준다. 하지만 실시간으로 인증서의 대한 상태 정보를 제공하지 못 한다는 단점과 인증서 상태 검증을 위해 많은 정보를 전송해야 하기 때문에 네트웍 과부하에 문제가 발생한다. 그로 인해 인증서 상태 검증에 소요되는 처리 속도가 느리다는 단점이 있다. 본 논문에서는 기존 방식의 문제점인 인증서 상태 정보의 실시간성 반영 문제 및 인증서 상태 검증 시간의 향상을 위한 인증서 자체의 Serial과 UserDN만을 이용한 축약 서명 기반의 효율적인 인증서 상태 검증 시스템을 제안하고, 실제 실험을 통하여 기존의 시스템과 제안하는 시스템의 인증서 상태 검증 속도를 비교해 보고자 한다.

1. 서 론

2003년 기준 우리나라 전체 인구의 약 67%인 3000만명 정도가 인터넷을 사용하고 있으며 이는 2002년과 비교했을때 약 15%정도인 400만명이 증가한 수치이다. 이와같은 인터넷의 급격한 발전은 네트워크를 이용한 정보 교환의 증가를 가져오게 되었다.

정보의 교환은 단순히 각각의 사용자 단둘만의 개인적인 정보만을 교환하는 방식뿐만 아니라 기업과 기업, 국가와 국가간의 정보를 포함하여 쇼핑몰을 통한 정보 및 상품의 교환까지도 가능하게 되었다. [1]

그러나 개방형 네트워크인 인터넷에서의 모든 정보 교환은 항상 중요 정보의 노출, 중요 정보의 위조 및 변조등과 같은 위협요소를 내포하고 있다. 따라서 위와 같은 중요 정보의 보호를 위한 정보보호의 필요성이 대두되기 시작하였다

이러한 인터넷에서의 중요 정보 보호를 위해서는 모든 정보 교환에 대하여 중요 정보의 불법노출을 방지하기 위한 기밀성(Confidentiality), 정보의 위조 및 변조 여부를 판단하는 무결성(Integrity), 정보의 송신자와 수신자 사이에 송·수신 사실을 부인하지 못 하도록 하는 부인방지(Non-Repudiation), 전송된 정보의 송신자와 수신자를 확실하게 증명해주는 인증(Authentication)등의 기능들이 제공되어야 한다.[1]

PKI(Public Key Infrastructure)기반의 인증서 상태 검증 시스템은 위와 같은 4가지의 기능을 제공해 주지만 실시간으로 인증서의 대한 상태 검증을 제공하지 못 한다는 점(CRL(Certification Revocation List)방식의 인증서 검증 시스템)과 실시간성은 제공하지만 처리 속도가 다소 느리다는 단점(OCSP(Online Certificate Status Protocol)방식의 인증서 검증 시스템)이 있다.

본 논문에서는 실시간으로 인증서에 대한 상태 정보를 제공하고 더불어 인증서 상태 검증 시간을 향상 시킬 수 있는 인증서의 Serial과 UserDN을 이용한 축약 서명 기반의 효율적인 인증서 상태 검증 시스템을 제안하고자 한다.

본 논문에 구성은 2장에서 관련연구에 대해서 기술하고 3장에서 제안하는 시스템인 축약 서명을 이용한 인증서 상태 검증 시스템에 대하여 기술한다. 4장에서는 실험 및 평과를 5장에서 결론을 맺는다.

2. 관련연구

2.1 공개키 기반구조

공개키 기반구조는 공개키의 인증 문제를 해결하여 정보의 기밀성, 접근제어, 무결성, 부인방지, 인증을 제공하는 정보 보호 기반구조이다.[2]

공개키 기반구조는 아래 [그림 1]과 같은 형태로 구성되어진다.

2.2 공개키 기반구조 구성요소

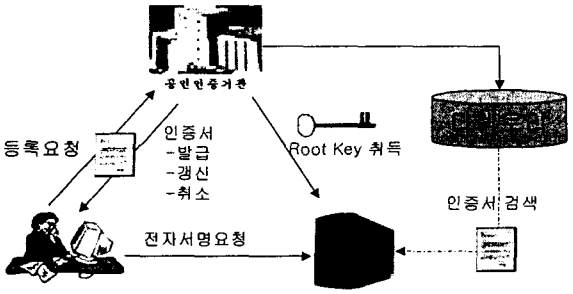
① CA(Certificate Authority) 인증기관

종단 실체(End Entity)와 다른 인증기관에게 인증서를 발행해주는 신뢰성이 보장된 실체. 인증기관은 인증서와 CRL을 저장소(repository)를 통해 여러 실체들에게 공표한다.[2][5]

② RA(Registration Authority) 등록기관

인증기관과 인증서 주체가 될 실체 사이의 중간 매개체 역할을 수행하는 실체. 등록기관은 사용자의 신분을 확인하는 것을 인증기간으로부터 위임받아 수행한다.[2][5]

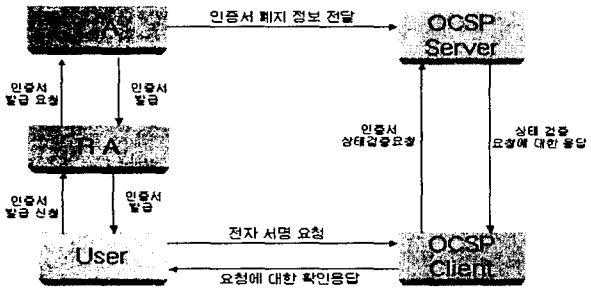
③ Directory
인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서 폐지 목록 등을 저장·검색하는 장소이다.[2]
④ CRL(Certification Revocation List)인증서 폐지 목록
공개키 기반구조에서 사용자 혹은 인증기관의 인증서가 만료되지 않은 시점에서 주체의 소속 변경 혹은 개인키의 노출 등의 이유로 무효화된 인증서에 대한 목록을 알리기 위하여 이들 정보를 인증기관의 개인키로 서명한 데이터 구조.[2][5]
⑤USER
인증서를 사용하는 실제 사용자.[2]



[그림 1] 공개키 기반구조

2.3 OCSP(온라인 인증서 상태 프로토콜)기반 방식

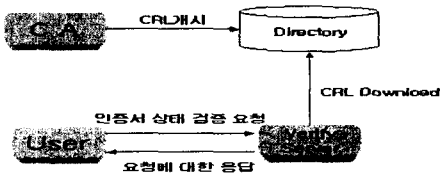
공개키 기반구조 내에서 인증서에 대한 상태 정보를 알기 위해 서버에게 문의하는데 사용되는 프로토콜로서, 인증서 상태 정보를 요구하는 질의 메시지와 인증서 상태 정보 요구에 응하는 응답 메시지로 구성되는 프로토콜기반의 인증서 상태 검증 시스템이다.[2][4]
인증서 상태 정보를 실시간으로 반영한다는 점에서 현재 가장 유용하게 쓰이는 인증서 상태 검증 방법이나 실시간으로 인증서에 대한 상태 검증을 수행해야 하기 때문에 네트워크 과부하 문제가 야기 될 수 있다는 단점이 있다. OCSP 기반의 인증서 상태 검증 시스템의 수행과정은 [그림 2]와 같다.



[그림 2] OCSP기반의 인증서 상태 검증 방식 수행 과정

2.4 CRL(인증서 폐지 목록)기반 방식

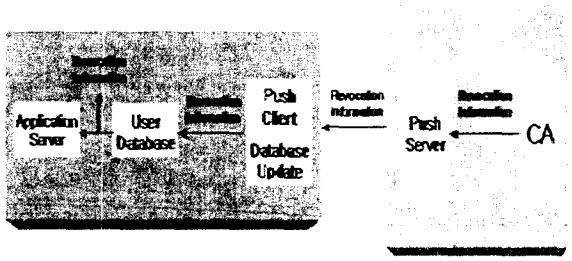
하루에 한번씩 폐지된 인증서 목록을 디렉토리에서 다운받아 인증서에 대한 상태 검증을 수행하는 시스템이다.
인증서 처리 속도 측면에서는 인증서를 다운 받아서 상태검증을 수행하기 때문에 다른 방식에 비해 월등히 빠르나 폐지된 인증서를 다운 받는 과정에서 네트웍 과부하가 많이 발생하며, 하루에 한번씩 폐지된 인증서를 다운 받기 때문에 인증서 상태 정보를 실시간으로 반영할 수 없다는 최대 단점이 있다.[3][5] [그림 3]은 CRL 기반의 인증서 상태 검증 시스템의 수행과정을 보여주고 있다.



[그림 3] CRL기반의 인증서 상태 검증 방식 수행 과정

2.5 PUSH 방식

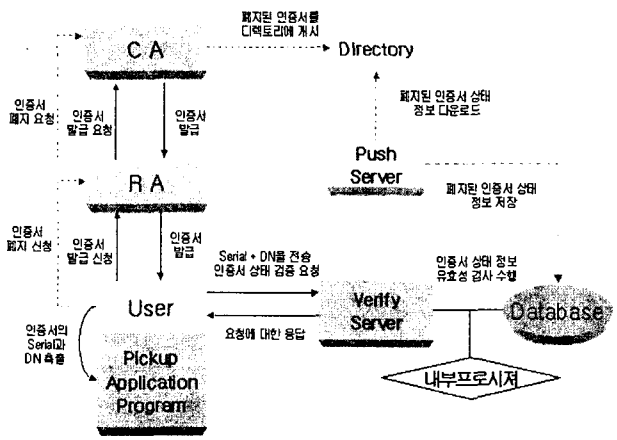
CRL기반의 인증서 상태 검증 시스템의 실시간성 문제를 해결하기 위한 대안으로 실시간으로 인증서 폐지 정보(폐지, 정지 정보)를 Push하는 시스템이다. Push System의 구성은 [그림 4]와 같다.



[그림 4] Push System 구성

3. 제안하는 시스템

본 논문에서 제안하는 축약 서명을 이용한 인증서 상태 검증 방식은 인증서 자체에서 인증서 시리얼 번호와 UserDN만을 축출하여 인증서 상태 검증을 수행한다. 즉 기존의 인증서 상태 검증 방식 시스템에서는 인증서 상태 검증을 요청할 때 약 1330BYTE크기에 인증서를 모두 전송해서 인증서의 대한 상태 검증을 수행하지만 본 논문에서 제안하는 축약서명 기법을 이용한 인증서 검증 시스템에서는 인증서 상태 검증을 요청할 때 약 330BYTE에 정보만을 필요로 하기 때문에 기존의 인증서 상태 검증 시스템에 비해 인증서 상태 검증 속도를 향사 시킬 수 있다.
본 논문에서 제안하는 전체 시스템구조는 [그림 5]와 같으며 전체 흐름은 아래와 같다.
① 사용자가 RA에게 인증서 발급을 신청한다.
② RA는 다시 CA에게로 인증서 발급을 요청한다.
③ CA는 인증서를 발급하고 RA에게 응답한다.
④ RA는 CA의 응답을 다시 사용자에게 응답한다.
⑤ 사용자는 인증서 상태 검증을 요청하기 전에 Pickup Application을 이용해 인증서에 Serial과 UserDN을 축출한다.
⑥ 사용자는 인증서에서 축출한 Serial과 UserDN을 Verify server로 전송하고 인증서 상태 검증을 요청한다.
⑦ Verify Server는 Push Server에서 실시간으로 제공한 CRL과 비교해서 사용자가 요청한 인증서의 상태 검증을 수행한다.
⑧ 사용자가 요청한 인증서가 유효한 인증서라면 사용자에게 유효 응답을 전송하고 유효하지 않다면 사용자에게 유효하지 않는다는 응답을 전송한다.



[그림 5] 축약 서명을 이용한 인증서 상태 검증 시스템

Serial : **인증서 고유 번호를 의미**
UserDN : **시스템이 사용자를 구별 할 수 있도록 하는 유일한 값**

3.1 Pickup Application Program

사용자의 인증서에서 인증서 Serial과 UserDN을 축출하며 또한 축출한 정보를 Database에 저장하고 Verify server에게 인증서 상태 검증을 요청하는 역할을 담당하는 사용자 프로그램이다.

3.2 Verify Server

사용자로부터의 인증서 상태 정보 요청에 대한 검증 처리를 수행하고 처리 결과를 다시 사용자에게 보내는 기능을 수행한다. 또한 Push 서버에서 전송되어 오는 인증 서 상태 정보를 Database에 저장하는 기능도 수행한다.

3.3 Push Server

인증서 상태 정보에 대한 현재성을 제공하기 위해 필요한 서버로 CA로부터 개시되어진 CRL을 다운 받아 검증서버에 실시간으로 인증서 폐지 목록을 Push해주는 기능을 수행한다. 단 Push Server에서 반영하는 인증서 폐지 정보는 CA의 Revoked Status Table을 따른다.

3.4 내부 프로시저

내부 프로시저는 프로그램이 처음 실행될 때 한번 만 컴파일 되고 컴파일 결과를 시스템내의 캐쉬에 저장한다는 점에서 Verify Server에서 인증서 상태 검증을 수행할 때 인증서 검증 수행 시간을 향상 시키기 위한 목적으로 사용된다.

4. 실험 및 평과

본 논문에서는 OCSP기반의 인증서 상태 검증 방식과 제안하는 시스템과 같은 방식을 사용하지만 인증서 상태검증 요청시 인증서의 모든 정보를 가지고 인증서 상태 검증을 수행 하였을 때 마지막으로 본 논문에서 제안하는 인증서 Serial과 UserDN만을 가지고 인증서 상태 검증을 수행 하였을때의 수행시간을 측정하였다.

OCSP 기반의 인증서 상태 검증 방식 수행시간은 0.3초가 걸리며, 제안하는 시스템과 동일한 방법이지만 인증서의 모든 정보를 가지고 인증서 상태 검증을 수행했을때 수행시간은 0.294초가 걸린다. 마지막으로 본 논문에서 제안하는 축약서명을 이용했을때의 수행시간은 0.183초가 소요된다. 아래 [표1]은 실험 내용 및 결과를 보여주고 있다.

[표 1] 실험 내용 및 결과

	전송되는 데이터크기	수행시간
OCSP방식	1330BYTE	0.300SEC
제안시스템 (인증서 모든 정보 전송)	1330BYTE	0.294SEC
제안시스템 (Serial + DN 전송)	330BYTE	0.183SEC

5. 결론

본 논문에서 제안하는 시스템인 축약 서명 기반의 효율적인 인증서 상태 검증 시스템은 기존의 인증서 모든 정보를 보내는 상태 검증 시스템과 달리 인증서에 Serial과 UserDN만을 전송하고 인증서 상태 검증을 요청함으로써 네트웍의 걸리는 부하를 감소시키며 그에 따른 결과로 인증서 상태 검증시 검증 수행 속도가 향상됨을 실험을 통해 증명 할 수 있었다.

또한 폐지된 인증서에 대한 정보를 Verify Server로 전송해주는 Push Server를 둠으로서 인증서 상태 정보에 대한 실시간성을 확보 할 수 있었다.

본 논문에서는 기존 인증서 상태 검증 시스템의 문제점인 인증서 정보의 실시간성 반영 문제 및 인증서 상태 검증 시간의 향상을 위해 인증서 Serial과 UserDn을 이용한 축약서명 기반의 효율적인 인증서 상태 검증 시스템을 제안하였다. 향후 본 연구 결과를 토대로 실제 응용이 가능하도록 계속적인 연구를 진행해 나갈 것이다.

참 고 문 헌

[1] 권태경, 강명호, 김승주, 서정욱, 진승헌 "정보 보호 표준 개론" 한국정보통신기술협회. 2002
[2] "정보보호기술전문용어집" 한국정보보호진흥원. 2002
[3] J.Dankers, T.Garefalakis, R.Schaffelhofer and T.Wright "Public key infrastructure in mobile systems" ELECTRONICS & COMMUNICATION ENGINEERING JOURNAL. OCTOBER 2002
[4] Vishwa Prasad, Sreenivasa Potakamuri, Michael Ahern, Michah Lerner, Igor Balabine, Partha Dutta "Scalable Policy Driven and General Purpose Public Key Infrastructure(PKI). IEEE 2002
[5] Chu Yae Liau, Stephane Bressan, Kian-Lee Tan "Efficient Certificate Revocation : A P2P Approach" ASIAN 2002 Workshop on Southeast Asian Computing Research. (ASIAN 2002).