일회용 인증서를 사용한 안전하고 효율적인 영화예매 시스템의 설계 및 구현1)

민성의, 김홍기, 이선호, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail : [mse918, hgkim31, sunho431, imylee]@sch.ac.kr

Design and Implementation of Secure and Efficient Movie Ticket Reservation System Using One-Time Certification

Seong-Ui Min, Hong-Gi Kim, Sun-Ho Lee, Im-Yeong Lee
Deptartment of Computer Software Engineering, Soonchunhyang University

요 약

공인인증서는 10여 년 간 국내 인터넷 뱅킹이나 전자상거래에서 본인인증 수단으로 긴요하게 이용되어 왔다. 그러나 공인인증서는 처음 발급받았던 저장매체에서 사용이 가능하며, 재발급 시에 기존 인증서를 폐기한 후 새로운 인증서를 발급받아야 하는 불편함이 있다. 2010년 행정안전부에서는 2013년부터 하드디스크 내 공인인증서 저장을 금지한다는 방안을 발표하였다. 이에 따라 사용자들은 공인인증서를 이동형 저장매체에 저장한 후 사용이 가능하게 되어 이동형 저장매체의 중요성이 높아지게 되었으며, 분실 위험에 노출되어 있는 이동형 저장매체가 없을 시에도 안전하게 인증서를 사용할 수 있는 시스템이 필요하게 되었다. 본 논문에서는 위와 같은 불편함을 줄이고자 기존에 발급받았던 인증서를 토대로 경량화 된 일회용 인증서를 발급받음으로써 안전하고 효율적인 결제가 가능하도록 하는 시스템을 설계 및 구현하였다.

1. 서론

공인인증서의 발급 건수는 2002년부터 2009년까지 꾸준히 증가하고 있으며, 1999년 등장 이후 10년 만인 2009년에 발급 2,000만 건을 돌파하였다[1]. 그러나 증가하는 사용량에 비례하여 하드디스크에 저장된 공인인증서 해킹으로 인한 피해 사례가 증가하고 있다. 이에 따라 정부는 2013년부터 하드디스크 내 공인인증서 저장을 금지하고 이동형 저장매체에 저장하도록 하는 방침을 내놓았다[2]. 이러한 방침으로 인해 앞으로 USB와 같은 이동형 저장매체에 대한 중요성이 높아질 것이며, 분실 위험이 높은 USB의 특징에 따라 인증서가 저장된 저장매체 없이도 인증서를 사용할 수 있는 방안이 필요하게 되었다.

위와 같은 배경으로 본 연구는 기존에 발급 받은 인증서를 토대로 경량화 된 새로운 인증서를 생성하여 발급함으로써 인증서가 없는 상황에서도 인증서를 안전하고 효율적으로 사용할 수 있도록 일회용 인증서를 생성하였으며, 일회용 인증서를 사용하여 영화 예매를 할 수 있는 시스템을 설계 및 구현하였다.

본 논문의 구성은 2장에서 X.509 인증서의 형식과 발급 및 사용 절차를 기술하고 3장에서는 일회용 인증서 발급 시스템의 보안 요구사항 및 모바일 콘텐츠 요구사항을 기술한다. 4장에서는 이를 만족하는 제안방식에 대하여 기술하고, 5장에서는 제안방식의 구현에 대하여 기술하며, 6장에서는 제안방식을 분석한다. 마지막으로 7장에서 결론을 맺는다.

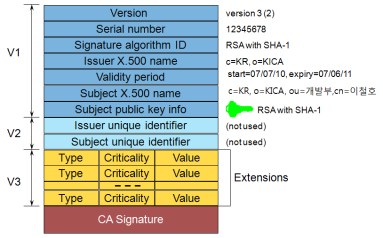
※ 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2010-0022607)

2. 관련연구

본 장에서는 기존 인증서의 발급 절차 및 사용 절차를 알아본다.

2.1 X.509 인증서의 형식

현재 사용하고 있는 공인인증서는 X.509 인증서로써, 1,2,3 버전이 있으며 통상적으로 버전3을 사용한다. 버전이 높아질수록 인증서가 포함하는 형식의 속성들이 많아진다.



(그림 1) X.509 인증서 형식

기본적인 속성으로는 버전, 일련번호, 서명 알고리즘, 발급자, 유효기간의 시작과 끝, 주체, 공개키, 기관 키 식별자 등이 있다(그림 1 참조)[3].

2.2 발급 절차

기존 인증서의 발급은 오프라인과 온라인으로 이루어진다. 사용자는 오프라인으로 등록기관에 방문하여 인증서 신청서를 작성하면 등록기관에서는 온라인상으로 가입자 등록 정보를 인증기관에 보낸다. 인증기관은 가입자 등록 정보를 저장하여 참조번호와 인가코드를 생성하여 등록기관에 전송한다. 참조번호와 인가코드를 받은 사용자는 전자서명 키 쌍을 생성하고, 인증서 요청 형식을 생성한 후 인증기관에 인증서 발급을 요청한다. 인증서 발급을 요청받은 인증기관에서는 발급 신청자를 확인하고 인증서를 발급한 후, 사용자에게 인증서가 저장되어 있는 URL을 전송함으로써 인증서 발급이 완료된다[4].

2.3 사용 절차

발급받은 인증서를 사용할 수 있는 분야는 다양하지만 쉬운 이해를 돕기 위해 은행으로 송금을 하고자 할 때의 예를 본다. 사용자가 A은행에서 B은행으로 송금을 하고자 할 때, 사용자는 은행 홈페이지에 로그인을 하고 거래를 선택하게 된다. 먼저 거래신청서를 작성하고 송금을 신청하면, A은행은 B은행에 송금하기 전에 인증기관을 통해 인증서를 검증한 후 B은행에 송금을 한다. 송금을 받은 B은행은 A은행에 송금 결과를 전송하고 A은행은 사용자에게 송금 처리를 통보하고, 사용자는 거래신청서를 통해 이체 처리를 확인한 후, 로그아웃을 함으로써 송금을 완료한다[4].

그러나 인증서가 저장된 저장매체가 없을 시에는 인증서를 사용할 수 있는 방안이 없다는 문제점이 있다.

3. 보안 요구사항

본 장에서는 기존 인증서를 토대로 일회용 인증서를 발급받아 사용하는 제안방식에 대한 보안 요구사항을 알아본다.

3.1 보안 요구사항

본 연구는 기밀성, 무결성, 사용자 인증, 부인방지에 대하여 다음과 같은 보안 요구사항을 가진다.

- 기밀성 : 일회용 인증서를 클라이언트에 전송하기 위해 제 3자가 일회용 인증서를 취득하지 못하도록 기밀성이 보장되어야 하며, 제 3자의 도용을 방지할 수 있어야 한다.
- 무결성 : 기존 인증서의 내용과 일회용 인증서의 내용이 일치해야 한다. 따라서 사용자가 인증서를 발급받거나 인증서를 사용하는 과정에 있어서 인증서 전송도중 인증서의 내용에 대한 위·변조 및 삭제 등과 같이 인증서가 변경되지 않아야 한다.
- 사용자 인증 : 일회용 인증서는 기존에 발급받은 인증서를 토대로 생성되는 것이므로 기존 인증서 사용자의 일회용 인증서라는 것을 검증하여 신원을 확인할 수 있어야 한다.
- 부인방지 : 서버가 인증서를 보낸 사실에 대해 부인을 방지 할 수 있어야 하며, 클라이언트는 인증서를 받은 사실에 대해서 부인을 방지할 수 있어야 한다.

3.2 모바일 콘텐츠 요구사항

본 연구의 시스템은 윈도우 모바일을 통하여 일회용 인증서를 발급받아 사용되므로 일반적인 모바일 콘텐츠로써의 요소를 필요로 하여 다음과 같은 요구사항을 가지게 된다.

- 상호작용성 : 클라이언트와 서버간의 원활한 통신이 이루어져야 한다. 서버는 클라이언트로부터 받은 데이터로 사용자를 인증하고 인증서를 생성할 수 있어야 하며, 클라이언트는 서버로부터 받은 데이터를 이용함으로써 시스템 사용에 영향을 줄 수 있어야 한다.
- 즉시연결성 : 사용자는 시간 및 공간의 제약 없이 모바일을 이용하여 서버와의 통신이 가능해야 하며, 서비스를 원활히 제공 받을 수 있어야 한다. 모바일 콘텐츠의 가장 큰 장점 이라고도 할 수 있는 즉시연결성을 만족함으로써 인증서가 저장된 저장매체 없이도 서비스를 제공 받을 수 있어야 한다.

4. 제안방식

본 연구에서 제안하는 방식은 기존에 발급받은 인증서를 토대로 한번만 사용할 수 있는 일회용 인증서를 발급받아 인증서가 저장된 저장매체 없이도 인증서를 사용할 수 있는 방안을 설계하였다. 따라서 이 장에서는 제안방식의 시나리오, 일회용 인증서의 형식, 일회용 인증서의 요구사항을 설명한다.

4.1 일회용 인증서 형식

본 연구에서 제안하는 일회용 인증서는 기존 인증서를 토대로 만들어지지만, 보다 원활한 통신과 보안상의 안전을 위해, 기존 인증서의 중요한 몇 개의 속성으로 구성하여 인증서를 경량화 하였다. 일회용 인증서의 속성으로는 일련번호, 서명 알고리즘, 발행자 ID, 유효시간, 공개키 소유자 ID, 공개키 정보 등이 있으며, 기존 인증서와의 연관성을 검증하기 위하여 기존 인증서의 일련번호를 추가적으로 포함하고 있다.

4.2 시스템 계수

- * : 참여 개체 (S:서버, C:클라이언트)
- KU* : *의 공개키
- KR* : *의 개인키

・KS : 서버와 클라이언트 간의 세션키
・E*[ ] : *의 키로 암호화
・D*[ ] : *의 키로 복호화
・VID : 가상식별번호

4.3 세션키 분배

영화예매 웹사이트 사용자 등록, 일회용 인증서 발급을 위해 PKI를 이용한 세션키 분배를 통하여 안전한 통신을 수행하며 프로토콜은 다음과 같다.

Step 1. 웹 클라이언트 프로그램은 서버에 세션키 분배를 요청한다.

Step 2. 서버는 웹 클라이언트에게 서버의 개인키로 Accept 메시지를 서명하여 전송한다.

E_{KRs}[Accept]

Step 3. 웹 클라이언트는 서버의 공개키로 해당 메시지를 복호화 하여 Accept 메시지를 확인한다.

$D_{KUs}[E_{KRs}[Accept]] = Accept'$

$Accept \stackrel{?}{=} Accept'$

Step 4. 클라이언트는 서버와의 대칭키 암호화 통신을 위한 세션키를 생성하여 해당 세션키와 VID값을 자신의 개인키로 서명하고 이를 다시 서버의 공개키로 암호화하여 전송한다.

$E_{KUs}[E_{KRc}[SK||VID]]$

Step 5. 서버는 해당 메시지를 서버의 개인키로 복호화하고 클라이언트가 서명한 세션키와 VID값을 확인한다.

$D_{KRs}[E_{KUs}[E_{KRc}[SK||VID]]] = E_{KRc}[SK||VID]$

$D_{KUc}[E_{KRc}[SK||VID]] \stackrel{?}{=} SK||VID'$

Step 6. *Step 5.*의 결과를 클라이언트에게 세션키로 암호화 전송한다.

E_{SK}[YES/NO]]

Step 7. 해당 메시지를 세션키로 복호화하여 서버의 처리 결과를 확인한다.

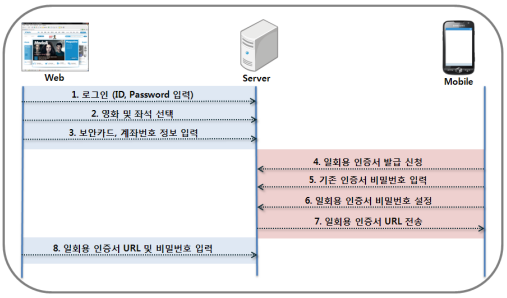
$D_{SK}[E_{SK}[YES/NO]] \stackrel{?}{=} YES/NO'$

4.4 시나리오

제안방식은 웹과 모바일이 클라이언트로서 서버와 연동하여 진행된다. 영화 웹 사이트를 통해 상영하고자 하는 영화를 선택하고 계좌정보를 입력한 후, 모바일을 통해 일회용 인증서 비밀번호 설정 및 일회용 인증서 발급을 받고, 다시 웹 사이트에 발급받은 일회용 인증서 정보를 입력함으로써 인증서를 사용하는 방법을 제공한다(그림 2 참조)[5-8].

Step 1. 웹 클라이언트는 영화 예매 웹사이트에 접속하여 회원가입 후, ID와 Password를 입력하고 서버에 전송하여 로그인을 한다.

Step 2. 정상적인 로그인이 완료되면 상영하고자 하는 영화에 대한 정보와 좌석을 선택한다.



(그림 2) 제안방식 시나리오

Step 3. 결제를 위하여 거래은행, 계좌번호, 계좌비밀번호, 보안카드 정보를 입력한다.

Step 4. 모바일 기기를 통하여 서버에 일회용 인증서 발급 요청을 한다.

Step 5. 기존 인증서와의 연관성 검증 및 사용자를 인증하기 위하여 기존 인증서의 비밀번호를 입력하고 서버에 전송한다.

Step 6. 일회용 인증서 사용 시 사용자를 인증하기 위해 새로 발급받을 일회용 인증서의 비밀번호를 설정한다.

Step 7. 정당한 사용자임을 인증하고 일회용 인증서 비밀번호 설정이 완료되면 서버에서는 전송받은 클라이언트의 정보를 이용하여 일회용 인증서를 생성하고 생성한 인증서의 URL을 암호화하여 모바일 클라이언트에 전송한다.

Step 8. 일회용 인증서 발급을 완료한 사용자는 웹 사이트에 접속하여 일회용 인증서의 비밀번호 및 URL을 입력하여 사용자를 인증하고 인증서를 사용한다.

5. 제안방식 구현

4장에서 설계한 내용을 기반으로 일회용 인증서를 사용한 안전하고 효율적인 영화 예매 시스템을 구현하였다.

5.1 서버 현황 및 클라이언트 접속

서버에서는 전반적인 통신의 흐름을 알 수 있으며, 클라이언트의 접속 및 전송받는 데이터의 내용을 알 수 있다(그림 3 참조).

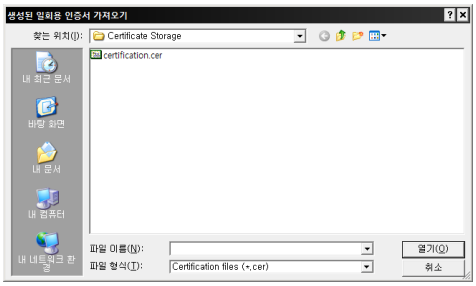
5.2 일회용 인증서 발급

일회용 인증서 발급은 모바일을 통하여 이루어진다. 그림 4와 같이 기존 인증서 암호를 입력하여 사용자를 인증하고, 일회용 인증서 암호를 설정함으로써 일회용 인증서 발급이 완료된다.

(그림 3) Server 현황

(그림 4) 모바일 클라이언트

(그림 5) 생성된 일회용 인증서 속성



(그림 6) 생성된 일회용 인증서 파일

5.3 일회용 인증서 발급 확인 및 사용

생성된 일회용 인증서를 확인하기 위해 그림 5의 일회용 인증서 가져오기 버튼을 클릭 시 그림 6와 같은 화면이 나타나고, 인증서가 저장되어 있는 경로의 폴더를 열면 certification.cer이라는 인증서가 생성된 것을 볼 수 있으며, 그림 6에서 속성 값을 확인할 수 있다.

6. 제안방식 분석

본 연구의 제안방식은 보안 요구사항을 충족함으로써 다음과 같은 이점을 제공한다. 본 장에서는 3장에서 언급한 요구사항에 따라 제안방식을 분석한다.

· 기밀성 : 외부의 공격으로부터 안전하기 위해 공개키 방식을 이용하여 클라이언트는 서버에게 서버의 공개키를 요청하고 서버는 클라이언트에게 자신의 공개키를 전달한다. 클라이언트는 서버에게 자신의 개인키로 서명한 인증서 요청 형식을 서버의 공개키로 암호화 하여 보냄으로써 제3자가 일회용 인증서를 취득하지 못하도록 하여 기밀성을 제공한다.

· 무결성 : 해쉬함수를 사용하여 인증서의 해쉬값을 생성하고, 생성된 해쉬값을 서명자의 개인키로 암호화 하여 전자서명을 생성하여 전송한다. 전자서명을 서명자의 공개키로 복호화하고 검증대상 인증서의 해쉬값을 비교함으로써 무결성을 제공한다.

· 사용자 인증 : 웹 클라이언트의 ID 및 Password를 바탕으로 사용자 인증 기능을 제공하며, 부가적으로 보안카드번호를 포함한 계좌정보를 비교하여 인증한다. 모바일 클라이언트에서는 기존에 발급받았던 인증서의 비밀번호를 이용하여 사용자 인증을 제공한다.

· 부인방지 : 공개키 기반 구조를 토대로 전자서명을 생성하게 되는데, 이때 클라이언트의 개인키는 클라이언트만이 가지고 있으므로 부인방지를 제공한다.

7. 결론 및 향후 연구 방향

본 논문에서는 기존에 발급받은 인증서를 토대로 일회용 인증서 생성 및 발급 시스템을 구현하고, 모바일을 통하여 일회용 인증서를 발급 받을 수 있는 모바일 시스템을 구현하였으며, 발급받은 일회용 인증서의 사용을 보여주기 위한 웹 사이트를 구현하여 일회용 인증서를 사용한 안전하고 효율적인 영화 예매 시스템을 구현하였다. 또한 인증서가 저장된 저장매체가 없을 경우에도 인증서를 사용할 수 있는 대응책이 없던 사용자에게 보다 안전하게 인증서를 사용할 수 있도록 할 뿐만 아니라, 기존의 인증서 사용 시 인증서가 저장된 저장매체의 부재 시에도 인증서를 사용할 수 있는 방안을 제시하였다.

향후 지속적으로 증가할 공인인증서 사용자를 위해 일회용 인증서 외에도 다양한 인증서 사용 방안에 대한 연구가 필요할 것으로 사료된다.

참고문헌

[1] 동아일보 “공인인증서 발급 건수 추이” 2010.1.15
[2] 보안뉴스 “공인인증서 PC 저장 금지 추진” 2010.1.16
[3] 이철호, “공개키 기반구조(PKI)”, 한국정보인증
[4] 박해룡, “알기쉬운 공인인증서”, 한국정보보호진흥원, 2009.5.13
[5] 최용락, 소우영, 이재광, 이임영, “컴퓨터통신보안 3rd”, 그린출판사, 2006
[6] 이시환, “뇌를 자극하는 ASP.NET 2.0”, 한빛미디어, 2009
[7] 최재규, “C# Programming Bible with .Net framework 3.0”, 영진닷컴, 2009
[8] 장시형, “C# 과 닷넷 플랫폼 Second Edition”, 사이텍미디어, 2005