공인인증서 시스템의 사용자 인증정책 강화에 관한 연구

김인범* · 황주용* · 박원형*

요 약

본 논문의 목적은 현재 사용되고 있는 공인인증서의 사용자 인증 방식을 살펴보고, 취약점 분석을 통해 사용자 인증을 강화시킬 수 있는 방안을 도출하는데 있다. 공인인증서란, 인터넷 상에서 사용자임을 입증할 수 있는 공개키 기반으로 만들어진 일종의 전자 신분증이다. 공인인증서는 주로 정부 민원·전자상거래·금융 분야에서 사용되었지만, e-sports·부동산·의료와 같은 다양한 분야의 업무 프로세스가 전산화됨에 따라 활용 범위가 확장되고 있다. 이 때문에 인터넷 상에서 사용자 인증 처리의 중요성이 대두되고 있다. 따라서 본 연구는 공인인증서 시스템의 인증 정책을 살펴보고, 취약점을 분석하여 인증 강화 방안을 모색하고자 한다. 이를 위해, 먼저 문헌연구를 통해 공인인증서 시스템의 인증 원리와 정책 구조를 알아보고, 이를 토대로 인증 정책의 한계를 도출하였다. 그리고 도출된 결과를 통해 사용자의 인증을 강화시킬 수 있는 가이드라인을 제공한다.

A Study on Enforce the Policy of User Certification in Public Certificate System

In Bum Kim* · Joo Yong Hwang* · Won Hyung Park*

ABSTRACT

public certification is some kind of electric ID which can prove the valid user, based on open KEY. usually it had been used in the field of government complaint, e-commerce, financial. but recently it expands the its use range through computerization of work process of diversity fields such as e-sports, property, medical industry. because of this reason, importance for user certificate process is gradually rose.

The purpose of this paper is looking at the method for user certification of public certificates and draw a way for enforce the user certification process by Vulnerability Analysis.

To draw the alternative we study the Authentication Principle and policy structure of public certification system by researching references, has drew the limitation for policy of certification. we provide the guideline to enforce the user certification through conclusion which has been drew from previous step.

Key words : PKI, Banking, Authentication, Policy

접수일 : 2010년 10월 25일; 채택일 : 2010년 12월 15일

* 서울과학기술대학교 산업정보시스템공학과

1. 서 론

초기의 금융서비스는 오프라인 상에서 고객과 담당자의 1:1 대면을 통해 이뤄져왔기 때문에 주민등록증, 인감도장 이외에 인증 수단이 필요 없었다. 그러나 오늘날 인터넷이 보급되어 온라인 금융서비스가 상용화되면서 고객과 담당자의 비대면으로 금융거래가 이뤄지기 시작했다.

온라인 금융서비스는 비대면으로 거래가 이뤄지기 때문에 기존의 주민등록증, 인감도장을 대신하여 온라인상에서 사용가능한 새로운 사용자 인증 수단이 필요하다. 또한, 온라인 금융서비스를 이용할 때 전송 데이터가 평문 그대로 전송된 전송된다면, 위조나 변조 같은 문제가 발생할 수 있기 때문에 데이터의 암호화가 필요하다.

이러한 문제를 해결하기 위한 방법으로 공개키 기반의 전자서명이 도입되어 사용되고 있다. 공인인증서는 이 전자서명시스템에서 인감증명서 역할을 하는 중요한 장치이다. 하지만 공인인증서 시스템은 단순히 사전에 정의된 비밀번호의 일치여부만으로 사용자의 인증을 하기 때문에 도용당하기 쉽다. 그리고 과거에는 이메일을 통해 위장 사이트로 유인하여 개인정보를 획득하는 단순한 피싱이 주를 이루었으나, 최근에는 악성코드 유포, 파밍 기법과 결합된 피싱, 웹메일 해킹 등 점차 복잡화·지능화 되고 있어 인증서 도용에 의한 피해가 증가하는 추세이다[1].

하지만 인증 정책이 개선될수록 인증이 이루어지는 웹페이지의 보안성 측면만 강조되어 왔고, 공인인증서 자체에는 별다른 개선이 없는 실정이다. 따라서 본 논문은 공인인증서를 이용한 사용자 인증 정책의 현 상황을 진단하고, 문제점을 분석하여 공인인증서 자체의 보안성을 높일 수 있는 방안을 도출하고자 한다.

본문의 구성은 다음과 같다. 제 2장에서는 공인인증서의 정의와 기술동향을 기술하였고, 제 3장은 현 공인인증서의 인증 정책 현황과 한계점 분석에 대한 연구내용을 포함하고 있다. 그리고 제 4장에서 인증 방식의 개선 방안 모색 및 제언이 이뤄지며, 마지막으로 제 5장에서 연구결과를 간략히 정리하였다.

2. 관련 연구

본 장에서는 먼저 공인인증서의 정의와 현재 사용자 인증에 통용되는 기술 및 정책에 대한 선행연구를 알아보고자 한다.

2.1 공인인증서 시스템 개요

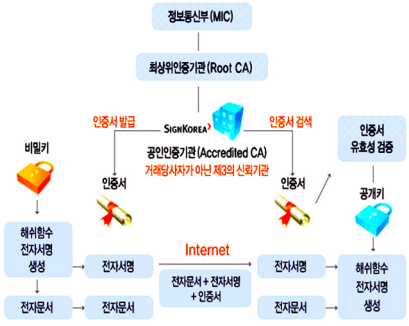
전자상거래시에 신원을 확인하고, 문서의 위조와 변조, 거래 사실의 부인 방지 등을 목적으로 공인인증기관(CA)이 발행하는 전자서명 정보로서, 일종의 사이버 거래용 인감증명서이다. 공인인증서 내에는 인증서 버전, 인증서 일련번호, 인증서 유효 기간, 발급기관 이름, 가입자의 전자서명 검증정보, 가입자 이름 및 신원 확인정보, 전자서명 방식 등의 정보가 포함되어 있다.

활용 범위는 인터넷 뱅킹, 인터넷 증권, 보험 가입 및 대출 서비스, 기업금융 서비스 등 금융 부문과 인터넷 쇼핑, 기업 간 정보 유통, 각종 예약, 화물 운송, 전자 세금계산서, 전자무역 등 전자상거래 부문 그리고 행정민원 사무, 인허가 신청, 조세행정, 전자공증 및 내용증명, 수출입 통관, 전자출원, 전자입찰 등 공공 부문 등이 있다[2].

2.1.1 전자서명

전자서명은 비밀키(Private Key)와 공개키(Public Key)로 구성된 공개키 기반구조(Public Key Infrastructure : PKI)로 이루어진다. 비밀키는 개인이 보관하고 공개키는 누구나 알 수 있게 공개하여, 비밀키로 암호화된 전자서명을 공인인증기관에 의해 공개키로 전자서명의 유효성을 검증하는 방식

이다. 따라서 공인인증기관은 공개되어있는 공개키와 개인정보를 공인인증서의 형태로 발급하여 공개키의 안정성을 보장한다.



(그림 1) 공개키 기반의 인증 체계[3]

(그림 1)과 같이 전자상거래 이용 시 비밀키를 입력하면 전자서명이 생성되어 공인인증서와 함께 첨부되고, 공인인증기관 내에 저장된 동일한 인증서와 공개키를 이용하여 수신된 인증서의 유효성을 검증하게 된다.

2.1.2 공인인증기관(Certificate Authority : CA)

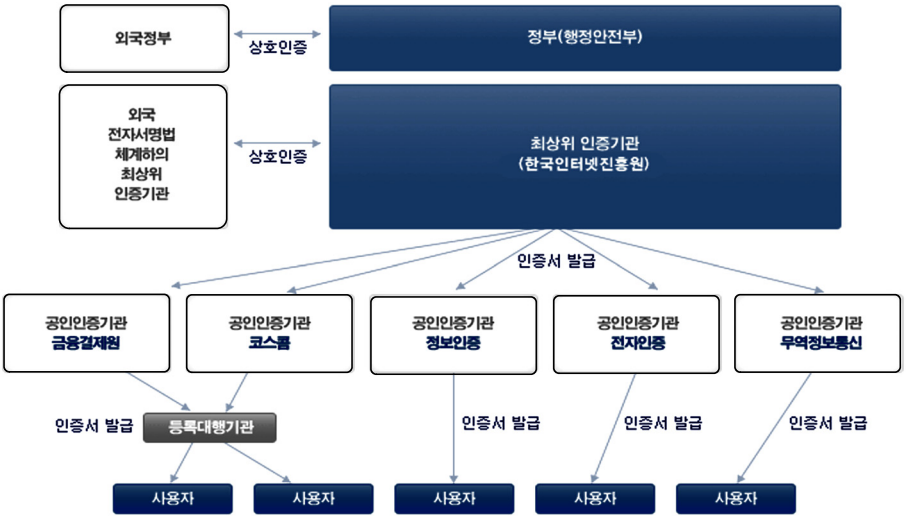
전자서명법에 따라 거래 사실을 공정하게 관리·보증할 수 있는 공신력과 인증 시스템을 안전하게 구축·관리할 수 있는 인력·기술력·자금력을 갖춘 기관으로, 공인인증서의 관리 및 유효성 검증을 수행한다. 금융결제원, 한국전산원, 한국증권전산, 한국정보인증, 한국전자인증, 한국무역정보통신 등이 있다.

2.1.3 등록대행기관

공인인증서 발급시 공인인증기관을 대신하여 인증서 가입자와 직접 대면을 통해 신원을 확인하고, 인증서 발급·정지·폐기 등의 신청을 등록하는 업무를 수행하는 기관으로 대부분의 금융기관이 이에 속한다.

2.1.4 인증기관의 트러스트 체인

인증기관이 발행한 전자인증서를 확인하기 위해서는 인증기관의 공개키를 확인할 수 있는 방법이 필요하다. 그러나 많은 인증기관이 존재하기



때문에 이들 각각의 공개키를 모두 신뢰해야 하는 어려움이 있다. 이러한 어려움을 해결하기 위한 기법이 인증기관의 트러스트 체인이다.

(그림 2)와 같이 하위계층 인증기관의 공개키는 상위 인증기관이 전자인증서를 발행하여 인증하고, 최상위 계층 인증기관의 공개키는 루트 인증기관이 전자인증서를 발행하여 인증한다. 이러한 트러스트 체인의 구조는 다양한 형태를 취할 수 있으며, 결국 사용자들은 루트 인증기관의 공개키 하나만을 신뢰함으로써 하위의 모든 인증기관들이 발행하는 인증서를 확인할 수 있다.

2.2 기술 동향

공인인증서 시스템을 이용한 사용자 인증방식은 사용자의 인증부터 결제까지 전부 하나의 단말기에서 이루어졌기 때문에 보안성의 문제가 제기되었다. 따라서 (그림 3)과 같은 별도의 물리적인 보안매체를 사용하여 인증과정과 결제과정을 분리하려는 동향을 보이고 있다. 대표적인 보안매체로는 보안카드와 OTP가 있다.

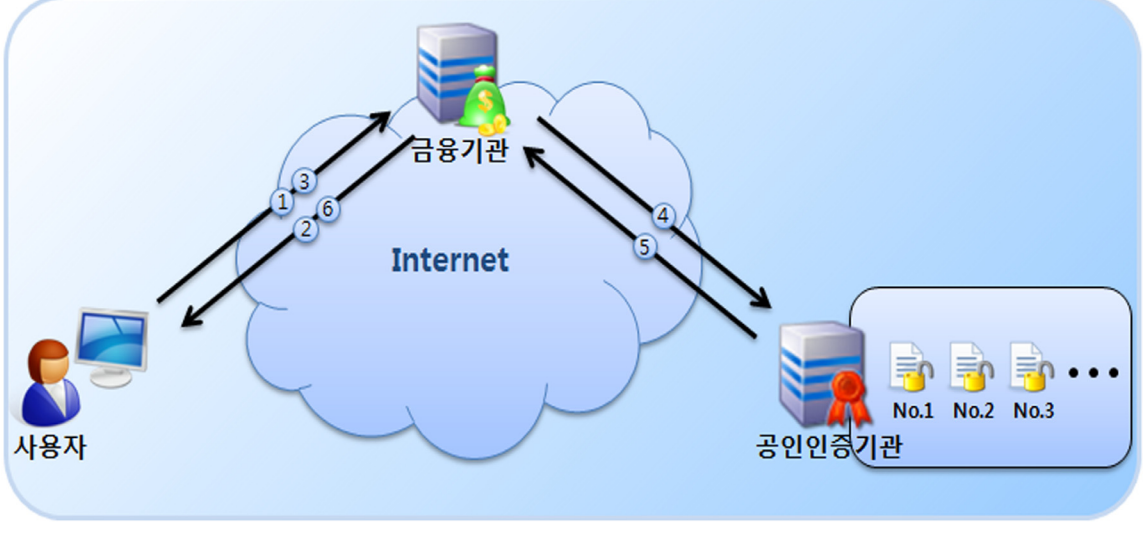
(그림 3) 물리적 보안매체

3. 연구 분석

본 장에서는 수집한 자료를 통해 공인인증서를 이용한 사용자 인증 절차 및 정책을 살펴보고, 현 인증 정책의 한계점를 도출하고자 한다. 분석 결과는 제 4장에서 개선 방안 제언시 사용된다.

3.1 공인인증서 시스템 인증절차

앞서 제 2장의 선행연구에서 살펴본 공인인증서를 이용한 사용자의 인증은 대행기관과 인증기관을 통해 이루어진다. (그림 4)는 이러한 사용자 인증 과정을 간략하게 나타낸 흐름도이고, 그 세부적



(그림 4) 공인인증서를 이용한 사용자 인증 흐름도

인 인증 절차는 다음과 같다.

① 사용자가 금융기관에 인터넷 금융서비스를 요청한다.

② 서비스 요청을 받은 금융기관은 사용자에게 인증서의 전자서명을 요구한다.

③ 사용자는 인증서에 비밀번호를 입력하여 전자서명을 하고, 서명된 인증서를 금융기관에 전송한다.

④ 금융기관은 인증기관에 수신된 인증서의 유효성 여부 확인을 요청한다.

⑤ 인증기관은 유효성 여부 결과를 금융기관에 전송한다.

⑥ 인증서의 유효성 여부에 따라 사용자가 요청한 인터넷 금융서비스를 처리한다.

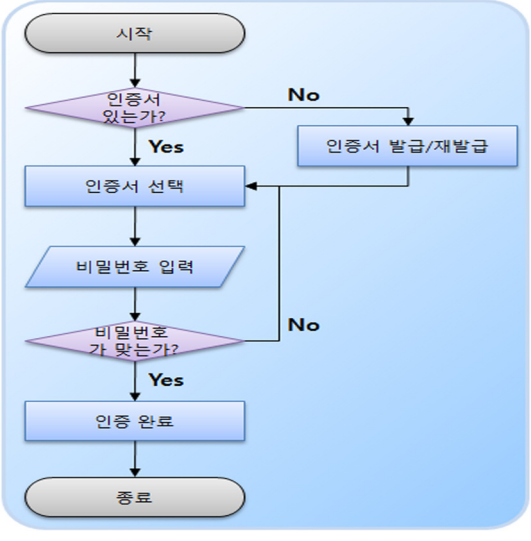
3.2 공인인증서 시스템 정책

현재 사용되고 있는 공인인증서는 정책에 따라 다음 <표 1>과 같은 인증서 관리 기능을 이용하여 사용자가 직접 인증서를 관리할 수 있다. 그리고 인증서가 효력 정지되거나 폐기되지 않는 이상 1년 365일 어디서든지 인증 가능한 상태로 설정되어 있다.

〈표 1〉 공인인증서 관리 기능[5]

기능	설명
발급	등록대행기관을 통해 인증서를 발급받을 수 있습니다.
재발급	기존 인증서의 유효기간과 동일한 유효기간으로 새로운 인증서를 발급받는 것입니다.
갱신	현재 가지고 있는 인증서를 계속 사용하기 위하여 인증서의 유효기간을 1년 연장하는 것을 말합니다.
폐기	만료일까지 인증서가 필요 없거나 정보 누출로 해당 인증서 사용이 위험하다고 판단된 경우 해당 인증서를 사용할 수 없도록 하는 것입니다.
효력정지	유효한 공인인증서의 효력을 일시적으로 정지시키는 절차로 공인인증서를 발급받은 등록대행기관(은행)을 통해 신청 가능합니다.
효력회복	효력 정지된 공인인증서의 효력을 회복하는 절차를 말합니다. 효력정지 후 6개월 이내 한하여 가능합니다.

또, 아래 (그림 5)와 같이 인증서 유무, 비밀번호 일치여부만으로 사용자의 인증이 이루어지는 구조를 가지고 있다.



(그림 5) 공인인증서의 인증 순서도

3.3 공인인증서 인증 정책의 한계

앞서 살펴보았듯이 현재의 인증서는 1년 365일 항상 인증 가능한 상태이며, 실사용자임을 인증하는 절차는 인증서의 유무·비밀번호 일치여부만으로 이루어져 있다. 또한, 정책 구조상 인증서 도용과 같은 사고대응에 대한 대책이 미미하고, 주로 사후대응에 초점이 맞춰져 있기 때문에 도용을 사전에 탐지할 수 있는 방법이 없다.

이러한 인증 정책은 보안적인 측면으로 보면 매우 위험한 상태이다.

2007년 1월 국내 유명 금융기관 홈페이지를 사칭하여 금융정보 및 비밀번호를 입력하도록 강요

하는 피싱사이트로 인해 공인인증서가 유출되는 사고가 발생하였다[6].

이와 같이 온라인상에서 Backdoor, Phishing 등의 침해사고가 빈번하게 발생하는 상황에서, 비밀번호 비교만으로 사용자를 인증하는 것은 비밀번호가 노출되면 바로 피해로 이어질 수 있다. 그리고 피해당하기 전까지 비밀번호가 노출 되었는지 알 수 있는 시스템이 전무하다.

이에 따라 사고대응에 대한 대책이 없다고 판단되어 현 인증 정책의 개선 방안을 제안하고자 한다.

4. 개선방안 연구

본 장에서는 제 3장에서 도출된 자료를 토대로 사용자의 인증을 강화할 수 있는 인증 정책의 개선방안을 제언하고자 한다.

4.1 개선요소

4.1.1 인증 가능 상태의 초기값 변경

기존의 인증서는 항시 인증 가능한 상태이다.

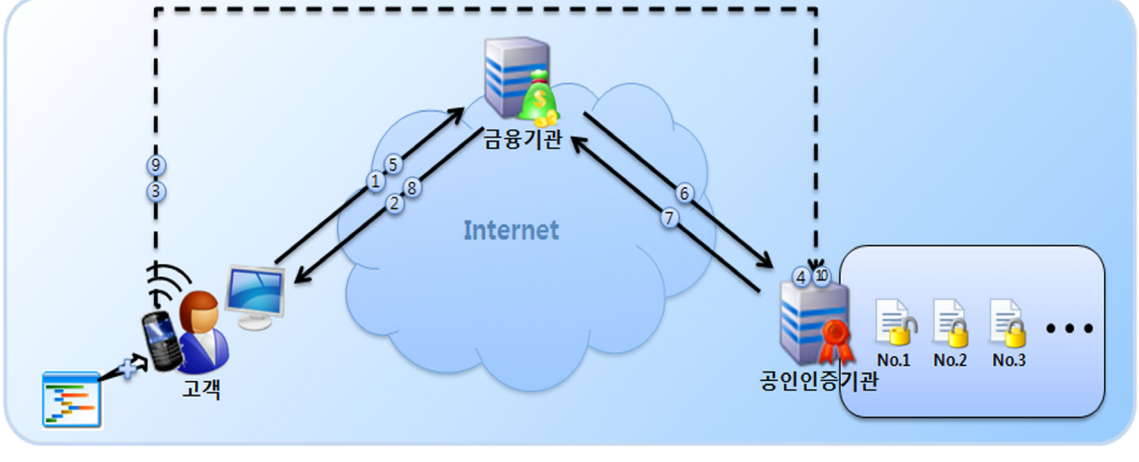
이 점은 사용자에게 언제든지 사용할 수 있다는 편리성을 제공함과 동시에 언제든지 비밀번호만 알면 인증가능하다는 점 때문에 보안성을 해치는 요소라고 판단된다. 따라서 인증 가능 상태의 초기값을 deny로 변경하고, 사용자의 특정한 Action에 따라서 allow로 변경하게 하여 보안성을 높일 수 있다.

4.1.2 사용자의 인증 의사반영

기존의 사용자의 인증은 인증서 유무·비밀번호 일치여부만으로 이루어졌다. 하지만 최근 발생하고 있는 각종 침해사고로 미루어보아 더 이상 비밀번호만으로는 사용자임을 인증하기에는 무리가 있다고 판단된다. 따라서 비밀번호 외에 사용자의 의사도 반영할 수 있는 시스템이 필요하다.

4.1.3 도용탐지 시스템 구축

현재의 인증서는 인증과정에서 별다른 도용탐지에 대한 시스템이 없고, 오로지 웹사이트의 보안시스템에 의존하고 있는 구조이다. 따라서 인증과정에서 사용자가 특정한 Action을 취하지 않고, 인증 시도를 할 경우에 사용자에게 직접 경고를 함



(그림 6) 개선된 사용자 인증 흐름도

으로써 도용에 대한 사전대응을 할 수 있는 시스템 구축이 필요하다.

4.2 개선방안 구체화

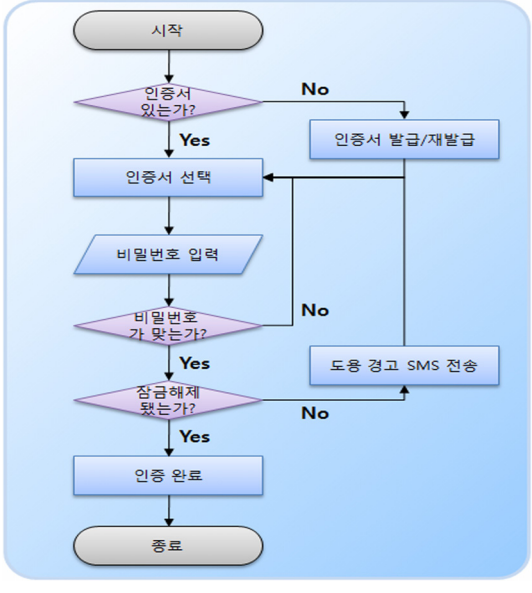
앞서 제시한 개선요소들을 고려하여 사용자 인증이 강화된 새로운 인증 절차 및 구조를 제안한다. (그림 6)은 새로운 사용자 인증 과정을 간략하게 나타낸 흐름도이고, 그 세부적인 인증 절차는 다음과 같다.

① 사용자가 금융기관에 인터넷 금융서비스를 요청한다.
② 서비스 요청을 받은 금융기관은 사용자에게 인증서의 전자서명을 요구한다.
③ 사용자가 모바일기기에 설치된 인증서 활성화 프로그램을 실행하여, 인증기관에 인증서의 잠금해제를 요청한다.
④ 인증기관에서 해당 인증서를 잠금해제 한다.
⑤ 사용자는 인증서에 비밀번호를 입력하여 전자서명을 하고, 서명된 인증서를 금융기관에 전송한다.
⑥ 금융기관은 인증기관에 수신된 인증서의 유효성 여부 확인을 요청한다.
⑦ 인증기관은 유효성 여부 요청 결과를 금융기관에 전송한다.
⑧ 인증서의 유효성 여부에 따라 사용자가 요청한 인터넷 금융서비스를 처리한다.
⑨ 사용자가 인증서 활성화 프로그램을 종료하여, 인증기관에 인증서의 잠금을 요청한다.
⑩ 인증기관에서 해당 인증서를 잠금 설정한다.

위 절차에서 잠금해제가 되지 않은 인증서로 인증 시도를 할 경우 경고 시스템이 작동하게 되어 실사용자에게 SMS문자가 전송이 된다.

(그림 7)은 개선된 인증 순서를 나타낸 것으로 인증서 유무, 비밀번호 일치여부 외에 잠금해제 여부도 비교함으로써 실사용자가 인증하려는 의도까지 반영되었다.

몇 가지 절차가 추가되었지만 개선요소를 모두 만족함으로써 사용자 인증이 강화될 것으로 기대된다.



(그림 7) 개선된 인증 순서도

4.3 기대효과

사용자가 원할 때만 인증 가능한 상태가 되기 때문에 사용자의 불안감을 해소시켜 주고, 별도의 보안매체가 아닌 일상생활에서 필수로 쓰이는 모바일기기를 사용함으로써 사용자의 편의성이 증대될 것이다. 그리고 피해를 당하기 전에 경고 시스템이 작동하기 때문에 사전대응이 가능해져 도용에 대한 피해가 감소할 것으로 기대된다.

5. 결 론

공인인증서 시스템은 미래의 IT산업과 전자상거래의 발전에 원동력으로 발전 가능성이 높아 정

부는 물론, 학계와 정보보호 관련 업계에서 많은 연구와 개발이 진행되고 있다. 하지만 공인인증서의 도용이 끊임없이 발생하면서 사용자의 개인정보를 보호하는데 부족한 점을 보이고 있다. 사용자는 자신의 개인정보가 침해받지 않으면서도 편리하게 사용하길 원하기 때문에 공인인증서의 보안성을 유지하면서 사용자의 편리성을 증대시키는 연구가 필요하다.

이에 따라, 본 논문은 기존의 공인인증서 인증 방식에 어플리케이션 구동을 추가하여 사용자의 편리성을 최대한 유지함과 동시에 공인인증서 자체의 보안성을 강화시킬 수 있는 방안을 제안하였다. 그리고 제안한 사용자 인증 방안이 실현되기 위해서는 향후 소프트웨어적인 구현과 새로운 인증서비스를 제공하는 네트워크 인프라 개발이 연구되어야 할 것이다.

참 고 문 헌

[1] 김인석, 김태호, 강형우, 이정호, 홍기석 공저, “전자금융 이러면 안전할까?”, 2010.
[2] 전자서명 인증서 프로파일 기술규격, 정보보호진흥원, 2004.
[3] “공인인증서란?”, (주) 코스콤 공인인증센터, 공인인증기관 웹사이트.
[4] 국내 공인인증 체계, 금융결제원 전자인증센터, 공인인증기관 웹 사이트.
[5] 공인인증서의 관리기능, 금융결제원 전자인증센터, 공인인증기관 웹 사이트.
[6] 사이버 침해사고 사례 분석, 국가사이버안전센터, 2008.
[7] 국가정보보호백서, 국가정보원, 2010.

김 인 범

2005년 서울과학기술대학교 산업정보시스템공학과 입학
2009년 KISA 정보보호동아리 융합보안연구회 초대회장
현재 서울과학기술대학교 산업정보시스템공학과 네트워크보안 Lab 연구원

황 주 용

2006년 서울과학기술대학교 산업정보시스템공학과 입학
현재 KISA 정보보호동아리 융합보안연구회 부회장
현재 서울과학기술대학교 산업정보시스템공학과 네트워크보안 Lab 연구원

박 원 형

2010년 서울과학기술대학교 산업정보시스템공학과 겸임교수