Journal of the Korea Academia-Industrial cooperation Society
Vol. 16, No. 9 pp. 6282-6289, 2015

http://dx.doi.org/10.5762/KAIS.2015.16.9.6282
ISSN 1975-4701 / eISSN 2288-4688

바이오인증 기반의 전자서명을 이용한 스마트 뱅킹 시스템 설계

김재우[1*], 박정효[1], 전문석[1]
[1]숭실대학교 컴퓨터학과

A Design of Smart Banking System using Digital Signature based on Biometric Authentication

Jae-Woo Kim[1*], Jeong-Hyo Park[1], Moon-Seog Jun[1]
[1]**Department of Computer Science, Soongsil University**

요 약 최근 공인인증서 유출 사고가 급증하고 있으며 이로 인한 전자금융사기가 빈번하게 일어나고 있다. 공인인증서와 개인키는 파일 형태로 존재하여 접근이 용이하고 쉽게 복사가 가능하기 때문에 PC의 하드디스크나 이동식디스크 등에 저장해두는 경우 악성코드에 의한 파밍, 피싱, 스미싱 등의 해킹 공격에 의하여 유출될 위험이 높다. 따라서 안전한 저장매체인 보안토큰, 저장토큰 등을 권고하고 있지만 분실 위험, 비용 문제 등의 이유로 실제로 사용하는 사람은 소수에 불과하다. 본 논문에서는 이러한 문제를 해결하고 단점을 보완하기 위하여 인증서와 개인키를 인증기관에서 보관하도록 하고 사용자는 본인 소유의 단말에서 바이오인증절차를 거쳐 인증기관에게 기기 고유 식별자와 인증토큰을 전달함으로써 인터넷 뱅킹을 위한 본인확인 및 전자서명을 수행할 수 있는 시스템을 제안한다. 제안하는 시스템은 인증서 비밀번호 입력 없이 바이오인증만으로 인증기관을 통하여 전자서명을 수행할 수 있어 기존 시스템에 비하여 서비스 이용이 간편하며 키로깅, 저장매체 분실, 인증서 유출 등의 위협요소를 무력화시킴으로써 안전한 인터넷 뱅킹 환경을 제공한다.

Abstract Today, there is an increasing number of cases in which certificate information is leak, and accordingly, electronic finance frauds are prevailing. As certificate and private key a file-based medium, are easily accessible and duplicated, they are vulnerable to information leaking crimes by cyber-attack using malignant codes such as pharming, phishing and smishing. Therefore, the use of security token and storage toke' has been encouraged as they are much safer medium, but the actual users are only minimal due to the reasons such as the risk of loss, high costs and so on. This thesis, in an effort to solve above-mentioned problems and to complement the shortcomings, proposes a system in which digital signature for Internet banking can be made with a simply bio-authentication process. In conclusion, it was found that the newly proposed system showed a better capability in handling financial transitions in terms of safety and convenience.

Keywords : Access Token, Biometric Authentication, Certificate Authority, Digital Signature, Smart Banking

1. 서론

온라인에 의한 전자거래가 일반화됨에 따라 인터넷에서 유통되는 정보의 가치가 증대되었으며, 특히 인터넷 상의 비대면 전자거래의 경우, 거래 당사자의 신원확인, 전자적 정보의 위·변조 방지, 거래사실 부인방지 수단이 필요하게 되었다. 이에 따라 온라인 전자거래의 안전·신뢰성 향상을 위하여 전자서명이 등장하였다.

전자서명이란 전자문서에서 종이문서의 인감처럼 사용되는 정보로 전자문서가 위·변조되지 않았음을 보장하는 동시에 전자문서의 서명자를 확인하고 부인 방지하는 기능을 제공한다[1].

*Corresponding Author : Jae-Woo Kim(Soongsil University)
Tel: +82-2-826-6526 email: saypeace@ssu.ac.kr
Received August 21, 2015 Revised September 9, 2015
Accepted September 11, 2015 Published September 30, 2015

현재 우리나라의 인터넷 뱅킹 시스템에서 사용되는 전자서명은 공인인증서를 활용한 공개키 기반 구조(PKI) 암호기술을 적용하고 있다[10][12]. 그러나 최근 해킹 기술의 발달로 공인인증서 유출 사고가 급증하고 있으며, 공인인증서와 함께 개인정보 및 금융정보가 유출될 경우 전자금융사기로까지 이어져 심각한 피해를 주고 있다.

공인인증서와 개인키는 파일 형태로 존재하여 접근이 용이하고 쉽게 복사가 가능하기 때문에 PC의 하드디스크나 이동식디스크 등에 저장해두는 경우 악성코드에 의한 파밍, 피싱, 스미싱 등의 해킹 공격에 의하여 유출될 위험이 높다[17]. 정부에서는 이를 막기 위하여 공인인증서를 보안토큰(HSM)에 저장하여 사용하는 방식을 의무화하고 재발급 절차도 강화하는 내용의 전자서명법 시행규칙 개정 방침을 내세우며 공인인증서 유출 방지를 위한 방안을 마련하고 있다.

2013년도 대국민 전자서명 이용실태 결과보고 따르면 공인인증서 가입자 중 절반 이상(63.2%)이 공인인증서 서비스 기관이나, 서버와 같은 제 3자에 의한 공인인증서 보관 서비스가 운영된다면 이용할 의향이 있다고 응답하였다[2].

이에 본 논문에서는 이러한 해킹 공격에 의하여 인증서와 개인키가 유출되는 것을 방지하기 위해 인증서 발급 후 인증서 및 개인키를 개인이 보관하지 않고 인증기관에서 안전하게 보관하도록 하고 이용자는 바이오인증 기술을 이용하여 간편하게 본인확인 및 전자서명을 수행할 수 있는 인터넷 뱅킹 시스템을 제안한다[15,16]. 2장에서는 기존 인터넷 뱅킹 시스템에서 사용되는 전자서명 이용 현황을 살펴보고 취약점을 분석한다. 3장에서는 바이오인증 기반의 전자서명을 이용한 스마트 뱅킹 시스템을 제시한다. 4장에서는 제안 시스템과 기존 방식을 비교분석하여 안전성을 평가하고, 5장에서 본 논문에 대한 결론을 맺는다.

2. 기존 인터넷 뱅킹에서의 전자서명 취약점 분석

2.1 인증서와 개인키 저장 방식

인터넷 뱅킹 사용자들이 금융거래를 위하여 사용자 인증, 조회 및 거래 요청을 하려면 공인인증서와 전자서명 위한 개인키가 반드시 필요하며, 사용자들은 인증기관으로부터 공인인증서와 개인키를 발급받아 사용할 수 있다. 발급받은 공인인증서와 개인키는 유출방지 기능을 갖는 안전한 저장매체에 보관해야하며 인증기관에서 권장하고 있는 저장매체로는 Table 1과 같이 보안토큰, 보안모듈, 저장토큰, 스마트 인증이 있다[5].

공인인증서는 저장매체의 보안성, 사용자 편의성 등을 고려하여 한시적으로 인증서를 하드디스크 및 이동식디스크에 발급할 수 있다. 이 때 하드디스크, 이동식디스크 내 공인인증서 저장위치는 운영체제별 환경에 따라 Table 2와 같이 정의된다[5].

Table 1. Storage Media Type

Type	Description	Storage
Security Token	Hardware device that key generation, digital signature be handled internally	USB Type Token
Security Module	Modules that available safe storage and processing	HW / SW Storage
Storage Token	Electronic card equipped IC or USB drive that support independent file structure	IC Card, USB Key
Smart Authentication	Services or circumstances using mobile device	USIM, eSE

Table 2. Storage location by a storage media

Storage Media	OS	Location
Removable Disk	Windows	(Drive):\NPKI\(CA Identifier)
	UNIX/Linux	(MountDirectory)/NPKI/(CA_Identifier)
	OS X	/Volumes/(Disk)/NPKI/(CA_Identifier)
Hard Disk	Windows	(HardDisk_Lable):\Program Files\NPKI\(CA_Identifier)
	UNIX/Linux	(UserID)/NPKI/(CA_Identifier)
	OS X	(UserID)/Library/Preferences/NPKI/(CA_Identifier)

사용자 인증서와 전자서명키를 이동식 디스크나 하드디스크에 파일로 저장하는 경우에는 정의된 인증서 저장위치 하위의 ‘USER’ 디렉토리 안에 사용자 식별명칭(DN)으로 디렉토리를 생성한 후 그 안에 저장한다.

2.2 인증서와 개인키 저장 방식의 이용현황 및 취약점

앞 절에서 살펴본 바와 같이 이동식디스크나 하드디

스크에 공인인증서와 개인키를 저장하는 경우 기술규격에 따라 정해진 위치에 저장되어 접근이 쉽고 파일 복사만으로 이용이 가능하다. 따라서 인증기관에서는 공인인증서와 개인키를 유출방지 기능을 갖는 안전한 저장매체인 보안토큰, 보안모듈, 저장토큰 등에 보관할 것을 권고하고 있다.

하지만 이동매체의 경우 휴대 및 컴퓨터 연결이 불편하고, 인증서 데이터의 삭제 및 분실/파손의 위험 등의 이유로 아직도 많은 이용자들은 하드디스크를 저장매체로 이용하고 있으며, 비용 문제, 소프트웨어 설치 요구, 이용의 불편함 등의 이유로 보안토큰 대신 이동식디스크를 이용하고 있다.

2013년 대국민 전자서명 이용실태 결과보고서를 살펴보면 공인인증서 가입자중 63.1%가 저장매체로 이동식디스크를 이용하고 있었으며, 42.1%(중복응답 가능)는 PC의 하드디스크에 공인인증서를 보관하고 있었다. 안전한 저장매체인 보안토큰(1.4%)이나 스마트카드(0.7%)를 이용하는 가입자는 소수에 불과하였다[2]. 그렇기 때문에 현재 수많은 공인인증서 이용자들이 공인인증서와 개인키 유출의 위협에 노출 되어 있다고 볼 수 있다.

3. 바이오인증 기반의 전자서명을 이용한 스마트 뱅킹 시스템

3.1 제안 시스템 개요

3.1.1 시스템 개요

앞 장에서 살펴보았듯이 인증서와 개인키를 PC의 하드디스크, 이동식디스크 등의 안전하지 못한 매체에 보관할 경우에 유출의 위협이 있으며, 보안토큰과 같은 저장매체는 비용문제, 분실/파손 등의 위험이 존재한다. 따라서 제안하는 시스템에서는 인증서 발급 후 인증기관에서 인증서와 개인키를 관리하도록 하고 본인인증 혹은 전자서명이 필요한 경우 바이오인증을 이용하여 간편하게 디바이스에서 인증을 수행하고 인증토큰을 전송하여 인증기관에 전자서명을 요청하는 방식의 스마트 뱅킹 시스템을 제안한다[11].

3.1.2 용어 정리

(1) 참조번호 (Reference Value) : 공인인증서 발급시 메시지 출처인증을 위해 이용되는 값으로 인가코드를 식별하기 위해 사용된다.

(2) 인가코드 (Secret Value) : 메시지 출처인증을 위해 이용되는 값으로 인증서 관리 프로토콜 메시지의 메시지 인증 코드를 생성하기 위해 사용된다.

(3) UDID (Unique Device IDentifier) : 기기마다 가지고 있는 디바이스의 고유한 식별자이다.

(4) 보안 영역 (Secure Storage) : 개인 소유 기기의 안전한 하드웨어 보안 영역으로 인증토큰, 바이오인증정보 템플릿을 저장한다.

(5) 인증 토큰 (Access Token) : 인증기관에 보관되어 있는 인증서와 개인키에 접근하기 위해 사용되는 토큰으로 사용자마다 고유한 값을 갖는다.

3.2 세부 프로토콜

시스템은 인증서 발급, 사용자 인증, 조회 및 거래 단계로 구분된다. 세부 절차에서 통신이 이루어지는 각 구간은 안전한 채널로 가정하며 추가적인 암호화 및 보안 과정은 생략한다.

3.2.1 인증서 발급

사용자는 디바이스에 본인인증을 위한 바이오인증정보를 등록하고 인증기관(CA)에 인증서 발급을 요청한다. 인증기관은 인증서 발급 후 인증서와 개인키는 인증기관에 보관하며 사용자 확인을 위한 인증토큰을 생성하여 사용자에게 전달한다. 수신한 인증토큰은 보안 영역에 보관하고 있다가 인증기관에 전자서명을 요청할 때 사용자 인증 및 식별 값으로 사용된다. 세부적인 인증서 발급 절차는 Fig. 1과 같다.

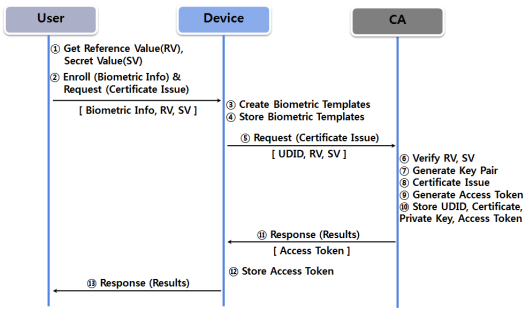

Fig. 1. Certificate Issue

1) 참조번호, 인가코드 획득 : 등록기관에서 신원확인 후 참조번호, 인가코드를 획득한다.

2) 바이오인증정보 등록 및 인증서 발급 요청 : 디바이스에 본인의 바이오인증정보를 등록하고 참조번호(RV), 인가코드(SV)를 입력한다.

$$\{\ Biometric\ Info\ ||\ RV\ ||\ SV\ \}$$

3) 바이오인증정보 템플릿 생성 : 입력받은 바이오인증정보를 이용하여 바이오인증정보 템플릿을 생성한다.

4) 바이오인증정보 저장 : 생성된 바이인증정보 템플릿을 보안 영역에 저장한다.

5) 인증서 발급 요청 : 입력받은 참조번호, 인가코드와 UDID를 인증기관에 전송한다.

$$\{\ UDID\ ||\ RV\ ||\ SV\ \}$$

6) 인증서 발급 요청 검증 : 수신한 참조번호와 인가코드를 이용하여 인증서 발급 요청을 검증한다.

7) 키 쌍 생성 : 인증서 발급을 위하여 공개키, 개인키 쌍을 생성한다.

8) 인증서 발급 : 생성된 사용자 공개키를 인증기관의 개인키로 서명하여 인증서를 발급한다.

9) 고유 인증토큰 생성 : 사용자 인증을 위한 고유한 인증토큰(Access Token)을 생성한다.

10) 인증서, 개인키, UDID, 인증토큰 보관 : 발급된 인증서, 개인키, UDID, 인증토큰을 저장한다.

11) 처리 결과 응답 : 인증토큰을 사용자에게 전달한다.

$$\{\ Access\ Token\ \}$$

12) 인증토큰 저장 : 수신한 인증토큰을 보안 영역에 저장한다.

13) 결과 전달 : 사용자에게 인증서 발급 처리 결과를 보여준다.

3.2.2 사용자 인증

사용자가 디바이스에 바이오인증정보를 입력하면 디바이스는 검증 후 본인 확인을 위한 정보를 금융기관에 전송하며 사용자 인증을 요청한다. 금융기관은 디바이스로부터 수신한 정보를 인증기관에 전달하여 사용자 식별 및 인증에 필요한 정보를 요청한다. 인증기관은 수신한 인증정보를 확인하고 사용자의 인증서, 개인키를 찾아낸 뒤 인증정보를 전자서명하여 금융기관에게 전송한다. 금융기관은 수신한 인증서, 전자서명값을 검증한 뒤 사용자 조회 및 본인확인 후 인증 결과를 전송한다. 세부적인 사용자 인증 절차는 Fig. 2와 같다.

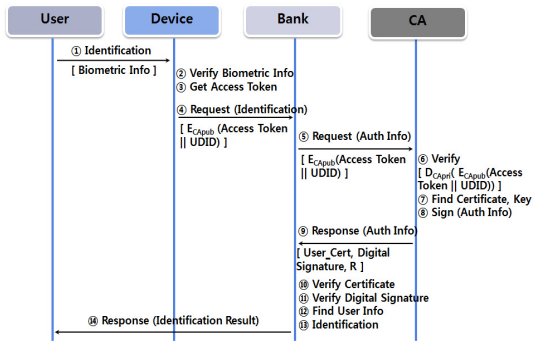

Fig. 2. User Authentication

1) 본인 확인 : 본인 확인을 위해 디바이스에 바이오인증정보를 입력한다.

$$\{\ Biometric\ Info\ \}$$

2) 바이오인증정보 검증 : 입력된 바이오인증정보와 보안 영역에 저장되어 있는 바이오인증정보 템플릿을 비교하여 검증한다.

$$Biometric\ Info\ =?\ Biometric\ Info\ Template$$

3) 인증토큰 획득 : 본인확인에 성공하면 보안 영역에서 인증토큰을 획득한다.

4) 사용자 인증 요청 : 사용자 인증을 위해 인증기관의 공개키로 인증토큰과 UDID를 암호화하여 금융기관에 전송한다.

$$\{\ E_{CApub}(Access\ Token\ ||\ UDID)\ \}$$

5) 사용자 인증정보 요청 : 금융기관은 수신한 정보를 인증기관에 전달하여 사용자 인증정보를 요청한다.

6) 수신정보 검증 : 인증기관은 수신한 인증토큰과 UDID가 올바른지 검증한다.

$$D_{CApri}(E_{CApub}(Access\ Token\ ||\ UDID))$$

7) 사용자 인증서 획득 : 수신정보를 가지고 사용자의 인증서와 개인키를 찾는다.

8) 전자 서명 : 사용자의 개인키를 이용하여 인증 전문에 전자서명한다.

$$E_{USERpri}(Authentication\_Info)$$

9) 사용자 인증정보 전송 : 사용자 인증서와 전자서명값, 식별번호를 이용한 본인확인을 위해 개인키에 포함된 R값을 전송한다.

$$\{\ User\_Cert\ ||\ E_{USERpri}(Auth\_Info)\ ||\ R\ \}$$

10) 사용자 인증서 검증 : 사용자 인증서의 유효기간 확인, 경로 검증, 상호연동정책 검증, 폐기 여부

확인 등을 통해 인증서를 검증한다.

11) 전자서명 검증 : 사용자 인증서에서 추출된 공개키를 이용하여 전자서명을 검증한다.

$$D_{USERpub}(E_{USERpri}(Auth\_Info))$$

12) 사용자 조회 : 사용자 인증서의 SerialNumber, SubjectDN으로 사용자 정보(ID, 주민등록번호)를 조회한다.

13) 본인확인 : 식별번호(주민등록번호)를 이용한 본인확인을 위해 전송된 R값과 사용자의 식별번호를 이용하여 인증서에 포함된 VID값을 검증한다.

14) 결과 전달 : 사용자 인증 결과를 전달한다.

3.2.3 조회 및 거래

계좌 및 거래 내역 조회는 사용자 인증 후에 별도의 추가 인증 없이 이루어진다. 사용자가 금융거래를 요청할 시에는 거래정보와 암호화 된 인증토큰을 금융기관에 전달하고, 금융기관은 인증기관에게 해당 거래정보에 대한 전자서명을 요청한다. 인증기관은 수신한 정보를 검증한 뒤 거래정보를 전자서명하여 금융기관에게 전송한다. 금융기관은 수신한 인증서, 전자서명값을 검증한 뒤 요청한 거래를 처리하고 결과를 사용자에게 전송한다. 세부적인 조회 및 거래 절차는 Fig. 3과 같다.

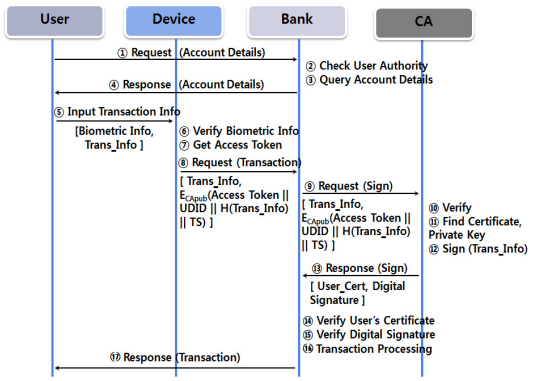

Fig. 3. Request Accounts & Transaction

1) 조회 요청 : 계좌/거래 내역 조회를 요청한다.

2) 요청 사용자 확인 : 요청 사용자의 인증여부 및 권한을 확인한다.

3) 조회 : 사용자가 요청한 내역을 조회한다.

4) 조회 결과 전송 : 조회한 내용을 사용자에게 전달한다.

5) 거래 정보 입력 : 원하는 거래 정보와 바이오인증정보를 디바이스에 입력한다.

$$\{\ Biometric\ Info\ ||\ Trans\_Info\ \}$$

6) 바이오인증정보 검증 : 입력된 바이오인증정보와 보안 영역에 저장되어 있는 바이오인증정보 템플릿을 비교하여 검증한다.

$$Biometric\ Info\ =?\ Biometric\ Info\ Template$$

7) 인증토큰 획득 : 바이오인증정보 검증에 성공하면 보안 영역에서 인증토큰을 획득한다.

8) 거래 요청 : 거래정보와 CA의 공개키로 암호화된 인증토큰, UDID, 거래정보 해쉬값, 타임스탬프를 금융기관에 전송하여 거래를 요청한다.

$$\{\ Trans\_Info\ ||\ E_{CApub}(Access\ Token\ ||\ UDID\ ||\ H(Trans\_Info)\ ||\ TS)\ \}$$

9) 거래정보 전자서명 요청 : 거래정보를 확인한 후 인증기관에게 해당 정보에 대한 전자서명을 요청한다.

10) 수신정보 검증 : 인증기관은 수신한 정보를 개인키로 복호화하여 인증토큰, UDID를 검증하고 거래정보를 해쉬하여 수신된 해쉬값과 비교함으로써 거래 정보의 무결성을 검증한다.

$$D_{CApri}(E_{CApub}(Access\ Token\ ||\ UDID\ ||\ H(Trans\_Info)\ ||\ TS))$$

$$H(Trans\_Info)\ =?\ H'(Trans\_Info)$$

11) 사용자 인증서 획득 : 수신정보(인증토큰, UDID)를 가지고 사용자의 인증서와 개인키를 찾는다.

12) 전자 서명 : 사용자의 개인키를 이용하여 거래정보를 전자서명한다.

$$E_{USERpri}(Trans\_Info)$$

13) 거래정보 전자서명값 전송 : 사용자 인증서와 전자서명 값을 전송한다.

$$\{\ User\_Cert\ ||\ E_{USERpri}(Trans\_Info)\ \}$$

14) 사용자 인증서 검증 : 사용자 인증서의 유효기간 확인, 경로 검증, 상호연동정책 검증, 폐기 여부 확인 등을 통해 인증서를 검증한다.

15) 전자서명 검증 : 수신한 사용자 인증서에서 추출된 공개키를 이용하여 전자서명을 검증한다.

$$D_{USERpub}(E_{USERpri}(Trans\_Info))$$

16) 거래 처리 : 요청한 거래를 처리한다.

17) 결과 전달 : 거래 처리 결과를 전달한다.

4. 제안 시스템 분석

제안 시스템은 공인인증서와 개인키를 인증기관에서 발급 후 보관함으로써 악성코드 감염에 의한 파밍, 피싱, 스마트폰의 스미싱과 같은 해킹 공격에 의하여 공인인증서와 개인키가 유출되는 문제를 해결하였다[13,14]. 사용자의 공인인증서와 개인키는 인증기관에 안전하게 암호화하여 보관되고 있으며, 전자서명이 필요한 경우 사용자가 인증서와 개인키를 전달받아 직접 서명하는 것이 아니라 기기에서 바이오인증정보를 이용하여 본인확인 후 보안영역에 저장되어 있던 인증토큰과 기기 고유 식별자(UDID)를 전달하여 인증기관에서 확인한 뒤 전자서명이 이루어지기 때문에 인증서와 개인키가 유출될 염려가 없다.

일반적으로 공인인증서와 개인키 파일이 유출되었다고 하더라도 개인키는 PKCS #5에 따른 패스워드 기반 암호화(PBE)기법에 의하여 암호화되어 저장이 되어 있기 때문에 패스워드를 알지 못하면 복호화가 불가능하다[9]. 하지만 기존 시스템에서는 공격자가 배포한 악성 프로그램이 사용자의 기기에 설치된 경우, 키로깅 툴에 의하여 패스워드가 노출 될 수 있다. 이에 비하여 제안 시스템에서는 전자서명을 위하여 공인인증서 비밀번호를 입력하는 과정 없이 바이오인증만을 이용하기 때문에 키로깅을 무력화시켜 안전성을 제공한다.

Table 3은 기존의 인터넷 뱅킹 시스템 사용되는 공인인증서 저장매체와 제안하는 시스템에서 사용하는 방식의 위협요소에 대한 안전성을 비교 분석하였다.

Table 3. Security Analysis

Storage	Key Logging	Certificate Loss	Certificate Leak
Hard Disk	X	X	X
Removable Disk	X	X	X
Security Token	O	X	O
Storage Token	O	X	O
Proposed System	O	O	O

우선 하드디스크나 이동식디스크의 경우 공인인증서와 개인키 파일 유출 및 키로깅에 의한 패스워드 노출의 위험이 있기 때문에 가장 취약한 것을 볼 수 있다. 보안토큰 경우 키 생성 및 전자서명이 토큰 내부에서 이루어지고 외부로 복사되지 않기 때문에 유출될 염려가 없고 별도의 보안토큰 패스워드를 사용하기 때문에 키로깅에 의한 패스워드 노출도 일어나지 않는다. 그러나 보안토큰 역시 이동식 매체이기 때문에 휴대 및 분실의 우려가 있다. 반면의 제안하는 시스템의 경우 공인인증서와 개인키가 인증기관에 안전하게 저장이 되어 분실이나 유출의 위험이 없으며 전자서명을 요청할 때에도 바이오인증정보를 이용한 본인확인을 하기 때문에 키로깅과 같은 해킹 프로그램에도 안전하다.

5. 결론

본 논문에서는 기존의 인터넷 뱅킹 시스템에서 본인확인 및 전자서명에 사용되는 공인인증서와 개인키 유출을 방지하기 위하여 인증서 발급 후 사용자가 아닌 인증기관에서 보관하도록 하고 전자서명이 인증기관에서 이루어지는 구조의 스마트 뱅킹 시스템을 제안하였다.

사용자는 인증서 발급 시에 수신한 인증토큰을 기기의 안전한 하드웨어 보안 영역에 저장해 두었다가 본인확인이나 전자서명이 필요한 경우 ID, 비밀번호 등을 입력할 필요 없이 간편하게 바이오인증만으로 인증기관에게 인증토큰을 전달하여 본인확인 및 전자서명을 요청할 수 있다.

제안하는 시스템은 공인인증서와 개인키를 인증기관에서 안전하게 보관하기 때문에 PC나 스마트폰에서 파밍, 피싱, 스미싱 등의 해킹 공격에 의하여 공인인증서와 개인키 파일이 유출되는 문제를 해결할 수 있다. 또한 보안토큰과 같은 이동매체의 단점인 휴대의 불편함, 분실위험, 비용 문제 등을 보완할 수 있다.

이전까지는 소수의 사용자들만이 바이오인증이 가능한 기기들을 사용하여 이러한 시스템 적용에 어려움이 있었다. 하지만 최근 출시되는 스마트폰은 대부분 지문인식을 이용한 본인인증기능을 탑재하고 있으며, 앞으로는 홍채, 심전도 등의 바이오인증기술까지 적용한 더 많은 제품들이 출시될 것이다. 따라서 향후 바이오인증기술을 연계한 전자금융거래에 관한 연구가 더욱 활발해질 것으로 기대된다.

References

[1] Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1988, September 1998.

[2] Korea Internet & Security Agency, Research on the Actual condition of Electronic Signature System usage, Dec. 2013.
[3] Financial Security Agency, Financial sector encryption technology Administration Guide, Jan. 2010.
[4] Korea Internet & Security Agency, "KCAC.TS.CM -Certificate Management in Mobile Device" v1.30, Feb, 2012.
[5] Korea Internet & Security Agency, "KCAC.TS.UI-User Interface Specification for the Interoperability between Accredited Certification Authorities", v2.10, Apr. 2015.
[6] Korea Internet & Security Agency, "KCAC.TS.CMP-Accredited Certificate Management Protocol Specification", v1.21, Sep. 2009.
[7] National Assembly, "Digital Signature Act(DSN)", Mar, 2013.
[8] S.R. Cho, D.S. Choi, S.H. Jin, H.H. Lee, "Passwordless Authentication Technology-FIDO", Electronics and Telecommunications Trends, Vol. 29, No. 4, pp.101-109, Aug. 2014.
[9] RSA, "PKCS #5 v2.0 : Password-Based Cryptography Standard", Mar. 1999.
[10] S.O. Hwang, "On the Security Proof of the Cramer-Shoup Public Key Cryptosystem," *The Journal of The Institute of Webcasting, Internet Television and Telecommunication,* Vol. 8, No. 6, pp. 15-20, 2008.
[11] Jong-Gun Song, Tae-Yong Kim, Hoon-Jae Lee, Won-Tae Jang, "A new password authentication scheme using two-way password in Smartphone Banking," *The Journal of The Institute of Webcasting, Internet and Telecommunication,* VOL. 12, No. 3, pp. 195-200, 2012. DOI: http://dx.doi.org/10.7236/JIWIT.2012.12.3.195
[12] Min-Sup Kang, "Design of Security-Enhanced RFID Authentication Protocol Based on AES Cipher Algorithm," T*he Journal of The Institute of Webcasting, Internet Television and Telecommunication* Vol. 8, No. 6, pp. 83-89, 2012.
[13] Soeui Kim, Duri Choi, Beongku An, "Detection and Prevention Method by Analyzing Malignant Code of Malignant Bot," *The Journal of The Institute of Internet, Broadcasting and Communication,* Vol. 13 No. 2, pp. 199-207, 2013. DOI: http://dx.doi.org/10.7236/JIIBC.2013.13.2.199
[14] Jang-Il Kim, Hee-Seok Lee, Yong-Gyu Jung, "Malware Behavior Analysis based on Mobile Virtualization," *The Journal of The Institute of Internet, Broadcasting and Communication,* Vol. 15 No. 2, pp. 1-7, 2015. DOI: http://dx.doi.org/10.7236/JIIBC.2015.15.2.1
[15] Jae-Kwan Choi, Ki-Young Lee, "Design and Implementation of the Security System using RFID and Biometric Information," *The Journal of The Institute of Webcasting, Internet and Telecommunication,* Vol. 10, No. 6, pp. 251-256, 2010.
[16] Farkhod Alisherov, "The Security in the Vehicular Ad Hoc Network (VANET) Using Expedite Message Authentication Protocol (EMAP)," *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, ISSN:2383-5281, Vol. 1 No. 1, pp. 99-106, Dec. 2011. DOI: http://dx.doi.org/10.14257/AJMAHS.2011.12.03"
[17] C.-W. Park, J.-W. Son, H.-K. Hwang, K.-C. Kim, "Detection of systems infected with C&C Zeus through technique of Windows API hooking," *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, Vol. 5 No. 2, pp. 297-304, Apr. 2015. DOI: http://dx.doi.org/10.14257/AJMAHS.2015.04.11

김 재 우(Jae-Woo Kim) **[정회원]**

- 2007년 2월 : 서울과학기술대학교 컴퓨터공학과 (공학사)
- 2009년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2009년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정 (수료)

<관심분야>
멀티미디어 보안, PKI, 바이오 인증

박 정 효(Jeong-Hyo Park) **[정회원]**

- 2009년 2월 : 숭실대학교 컴퓨터학과 (공학사)
- 2011년 2월 : 숭실대학교 정보보안학과 (공학석사)
- 2011년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정 (수료)

<관심분야>
익명 인증, 바이오 인증, 암호 이론

전 문 석(Moon-Seog Jun) **[정회원]**

- 1989년 2월 : University of Maryland Computer Science 박사
- 1989년 9월 ~ 1991년 2월 : New Mexico State University Physical Science Lab. 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 정교수

<관심분야>
정보보호, 네트워크 보안, 인증 시스템, 암호학