이용자 인증정보 재사용 방지를 위한 연구 : 전자서명을 중심으로

우기준O, 김동국*
O전남대학교 정보보안협동과정
*전남대학교 전자컴퓨터공학부
e-mail: 1510796@fsec.or.krO, dkim@jnu.ac.kr*

Study on The Prevention of User Authentication Information Reuse : Focusing on Electronic-Signature

Ki-jun WooO, Dong-gook Kim*
ODept. Information security course, Chonnam National University
*Dept. of Electronic Computer Engineering, Chonnam National University

● 요 약 ●

인터넷환경에서 금융회사는 홈페이지 사용자의 신원확인, 부인방지 등의 목적으로 공개키 기반구조(PKI: Public Key Infrastructure) 환경의 공인인증서를 홈페이지 로그인, 전자금융거래 등의 업무에 적용하고 있다. 사용자의 공인인증서를 이용하여 생성된 전자서명이 악성코드 감염 등으로 인하여 유출 시 사용자가 과거에 서명했던 전자서명이 재사용(로그인, 전자금융거래 등)될 수 있는 취약점이 존재하기에 인터넷 상에서의 전자서명 재사용에 대한 원인, 방지 절차 및 방법을 제안 하고자 한다.

키워드: 전자금융거래(E-financial transaction), 웹 해킹(Web hacking), 웹 취약점(Web vulnerabilities), 전자서명(Electronic signature), 재전송 공격(Replay attack)

I. Introduction

인터넷의 발달로 금융회사들은 홈페이지를 통해 인터넷 뱅킹, 온라인 주식매매, 대출, 보험 가입/보상/증명서 발급, 카드 신청/결제 등의 서비스들을 제공하고 있다. 금융회사는 홈페이지를 통한 안전한 전자금융 서비스 제공을 위하여 높은 수준의 보안을 유지하고 있다. 금융회사 서버 사이드에는 방화벽(Firewall), 침입탐지시스템(IDS), 침입방지시스템(IPS), 웹 애플리케이션 방화벽(WAF) 등의 보안시스템들을 설치운영하고 있으며, 사용자 PC에서 동작되는 웹브라우저에는 키보드 보안, 메모리 해킹방지, 백신, 웹 암호화 등의 보안 프로그램을 설치하여 웹 해킹에 대응하고 있다. 또한 인터넷 상에서의 전자금융거래 업무를 처리하기 위하여 고객의 신원을 확인하고 전자금융거래의 부인방지 등의 목적으로 공인인증서를 적용하고 있다.

금융서비스 전달채널별 업무처리비중
(입출금 및 자금이체 거래기준)

(%)

기간[1]	창구	CD/ATM	텔레뱅킹	인터넷뱅킹	전체
2016. 3월	10.8	37.9	11.2	40.1	100.0
2016. 6월	10.3	38.2	11.3	40.2	100.0
2016. 9월	10.1	36.2	10.9	42.7	100.0
2016.12월	10.9	35.7	11.3	42.1	100.0
2017. 3월	11.3	37.4	10.6	40.7	100.0
2017. 6월	10.6	37.8	10.5	41.1	100.0
2017. 9월	10.2	36.4	10.0	43.4	100.0
2017.12월	**10.0**	**34.7**	**9.9**	**45.4**	**100.0**

Fig. 1. Percentage of Business Process by Transfer Channel of Financial Services [1]

2017년말 현재 국내은행의 인터넷 뱅킹(모바일뱅킹 포함) 등록 고객수는 1억 3,505만명으로 전년말 대비 10.2% 증가하였고, Fig 1의 표를 보면 금융서비스 전달채널은 창구, CD/ATM, 텔레뱅킹 및 인터넷뱅킹으로 구분하였고 인터넷 뱅킹이 차지하는 비율이 매우 크다는 것을 알 수 있다. [1] 인터넷 뱅킹 서비스를 이용하고자 하는 고객은 해당 은행 홈페이지에서 공인인증서를 발급/등록해야 한다.

금융회사는 전자금융감독규정에 의거하여 공개용 홈페이지의 취약점 분석평가를 연2회(반기 1회) 실시 후에 금융위원회에 보고하고 있다 [2] . 또한 2018년 1월 금융당국과 금융보안원, 금융회사, 과학기술정보통신부에서 지정한 정보보호 전문서비스 기업들과 공동으로 취약점 분석평가 항목을 제정 [3] 하여 운영하고 있다. 하지만 날로 지능화 되고 고도화 되어가는 해킹 기술의 발달과 일반 개인들도 접하기 쉬운 해킹툴로 인하여 홈페이지 관련 보안 사고는 계속해서 발생되고 있다.

본 논문에서는 웹 애플리케이션 보안 취약점 분성평가 항목 중에 고객이 금융회사 홈페이지에 로그인하여 전자금융거래 서비스 이용 시에, 사용자 PC에 악성코드 감염으로 인해 사용자의 전자서명 정보가 탈취되어 발생할 수 있는 이용자 인증정보 재사용 취약점의 원인과 상세한 조치방법을 설명하고, 웹 응용프로그램 개발자들에게 공인인증서와 전자서명의 이해를 높이고자 한다.

논문의 구성은 다음과 같다. II장에서는 공인인증서 내에 주민등록번호 주입 절차와 전자서명 구조에 대하여 설명하고, III장에서 공인인증서를 사용한 로그인 보안 절차에 대하여 상세히 제안하고, 마지막으로 IV장에서 본 논문의 결론과 향후 연구에 대해서 서술한다.

II. Related works

1. Definition of terms

전자서명법 법에 따르면 전자서명이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다. [4] 공인인증서는 공인인증기관이 발급하는 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다. 인터넷 상에서 공인인증서를 이용한 본인확인 시 주민등록번호(사업자등록번호)를 이용하는 경우에 해당 정보(이하, 식별번호)의 노출 없이 안전하게 관련 정보를 생성하여 공인인증서에 포함하여 사용하고 있다. [5]

2. Information injection procedure for identification number

Table 1.의 단계를 거쳐 공인인증서 내에 식별번호 관련 정보를 주입하여 생성하게 된다. [5] 단계 ④의 가상 식별정보(이하, VID)는 난수(이하, R) 및 해쉬 함수(이하, h)를 사용하여 실제로 공인인증서에 포함될 식별번호 관련 정보는 VID = h(h(식별번호, R))와 같이 계산하며 여기서 사용되는 해쉬 함수는 모두 동일한 해쉬 함수를 사용한다. 단계 ⑤의 암호화는 단계 ①에서 획득한 공인인증기관의 인증서에서 추출한 알고리즘과 공개키를 사용한다.

Table 1. Describe the procedure for inserting an identification number within a public certificate

Step	Principal	Explanation
①	Subscriber	Public certification authority Acquire a certificate
②		Generate subscriber electronic signature keys (private key, public key)
③		Random Number Generation
④		Create virtual identification
⑤		Virtual identification and random number encryption
⑥		Generate and send a certificate request message
⑦	Public certification authority	Process Certificate Request Messages
⑧		Decode message and validate VID
⑨		Injecting VID within a public certificate
⑩		Send public certificate

3. Procedure for identifying the customer through a certificate

Table 2. Describe the procedure for verifying information regarding the identification number in the certificate

Step	Principal	Explanation
①	client	Identification number, random number transmission
②		Send a user's public certificate
③	finance com.	Extract the VID and hash algorithm from the certificate
④		VID' = h(h(Identification number, random number)) Calculation
⑤		VID and VID' Check for equalization

금융회사의 고객이 해당 금융회사 전자금융 서비스를 이용하기 위해서는 홈페이지에서 공인인증서를 등록하여야 하는데 이는 공인인증서 내에 개인의 식별번호 관련 정보가 포함되어있기 때문에 가능하다. 이에 금융회사는 공인인증서를 통해 고객의 신원을 확인하는 절차는 Table 2를 통해 설명한다. [5]

4. Electronic signature process

금융회사의 전자금융거래 및 로그인을 위해서 고객의 공인인증서를 통한 전자서명을 적용하고 있다. Table 3을 통해 전자서명의 과정과 정보를 설명한다. 일반적으로 전자서명이라 하면 단계 ④에서 전송되는 정보인 원문, 암호화된 해쉬값, 공인인증서 정보를 말한다. 전자서명 재사용 취약점이 발생하는 근본적인 이유는 단계 ①의 원문정보가 변경되지 않기 때문이다. 동일한 인증서로 동일한 원문을 전자서명하게 되면 동일한 결과 값이 생성되기 때문이다.

Table 3. Electronic signature process and information

Step	Principal	Explanation
①	client	Create original (data to perform signature)
②		Hashes the value generated by ① as a hash function
③		Encrypts the hash value generated in ② with the customer's public certificate
④		Send ① and ③ values and certificate information
⑤	finance company	Hash function for ①
⑥		③ value is to be disclosed from the public certificate and is to be compounded
⑦		Verification of the hash value of ⑤ versus the hash value of ⑥

III. Proposal

사용자가 금융회사 홈페이지에서 전자금융거래 업무를 하려면 공인인증서를 이용하여 로그인을 해야 한다. 이 과정에서 사용자가 과거에 로그인하기 위해 사용했던 전자서명 값이 재사용(reuse)될 수 있는 취약점을 제거하기 위해 웹 애플리케이션 서버는 사용자가 로그인하는 시점에 일회성 정보를 포함하여 사용자가 전자서명을 하게 하여야 한다. [6] 이에 Table 4와 같이 공인인증서를 사용한

홈페이지 로그인 보안 절차에 대해서 제안한다.

Table 4에서 제안한 단계 중 응용 프로그램에 필수적으로 반영되어야 할 내용에 대해 추가 설명을 한다. 최근 금융회사 홈페이지의 서버 응용 프로그램은 자바라는 프로그래밍 언어를 사용하여 구현하고 있다.

Table 4. Explanation of login security procedures using a public certificate

Step	Explanation
①	User requests login web page to web application server (hereinafter referred to as server)
②	Servers generate one-time information
③	Store one-time information generated by ② in a server session
④	Send one-time information generated by ② to the user, including it in the contents of the login webpage
⑤	Electronic signature including one-time information sent from the server (②) when electronic signature is provided with the user's public certificate
⑥	Server requests for verification of electronic signatures
⑦	The server validates the user's certificate validity (OCSP or CRL) and validates the electronic signature.
⑧	Extract the one-time information contained in the original electronic signature
⑨	Extract one-time information stored in ③
⑩	Check ⑧ and ⑨ for information matching
⑪	Initializing one-time information stored in ③
⑫	Send the login complete web page to the user when ⑦ to ⑩ validation is OK

②의 단계에서 생성하는 일회성 정보는 자바 API(Java application programming) 1.5 버전부터 제공되는 UUID 클래스 라이브러리 객체를 사용하여 생성할 수 있다.

UUID(Universal Unique ID) 객체는 128비트수의 32개 16진수로 표현되는 문자열을 리턴한다. String형으로 리턴받기 위해 아래의 코드로 프로그래밍하면 된다.

String setUuid = UUID.randomUUID(). toString()

단계 ③은 사용자(웹 브라우저)의 세션ID값을 이름으로 해서 아래의 내용으로 프로그래밍하면 된다.

session.setAttribute((String)session.getId(), ②의 단계에서 생성된 일회성 정보)

전자서명 및 서명검증 관련하여 ㈜코스콤 공인인증센터에서 제공하는 SignKorea 인증서비스 적용을 위한 함수 가이드 [7] 를 참고하여 ⑤,⑦ 단계를 설명한다. 단계 ⑤의 전자서명을 한 결과 값에는 원문(서명을 수행할 데이터), 원문 해쉬 값에 대한 암호화된 값, 서명자의 인증서가 포함된다. SignDataB64 함수는 사용자 인증서의 DN, 전자서명정보, 신원 확인용 난수 정보를 리턴한다. 단계 ⑦은 Base64 형태로 사용자가 서명한 전자서명에 대해 VerifyDataB64 함수를 사용하여 서명검증을 하면 사용자 인증서의 DN, 서명을 수행한 데이터 원문(⑧), 인증서 고유번호, 발급일, 만료일 등의 정보가 리턴된다. 단계 ⑨는 아래의 내용으로 프로그래밍하면 된다.

String getUuid = (String) session. getAttribute((String)session.getId())

단계 ⑪은 session.setAttribute((String) session.getId(), null)와 같이 초기화 처리한다.

IV. Conclusions

본 연구는 사용자PC에서 공인인증서를 이용한 금융회사 홈페이지 로그인 시에 사용되었던 전자서명 값 재사용 공격 취약점에 대한 보안 절차 및 응용 프로그램 작성 시 필수적으로 포함되어야 하는 내용에 대하여 제안하였다. 홈페이지 로그인뿐만 아니라 공인인증서를 사용하는 인터넷 뱅킹, 온라인 주식매매, 대출, 보험 가입/보상/증명서 발급, 카드 신청/결제 등의 전자금융거래 업무 시에도 Table 4의 보안 절차를 준수하여야 이용자 인증정보 재사용 위협에 대한 보안성을 유지할 수 있을 것이다. 향후에는 스마트 폰에서 사용되고 있는 모바일 뱅킹, 모바일 주식매매 등에 사용되고 있는 인증서 사용 취약점에 대하여 연구를 진행할 예정이다.

REFERENCES

[1] The Bank of Korea, "South Korea's Internet banking service use status in 2017", 2018.

[2] Electronic Financial Supervisory Regulations

[3] Financial Security Institute, "E-financial infrastructure vulnerability analysis item", 2018.

[4] Electronic signature method

[5] KISA, "Standard for User Identification using Identificati on Number", 2009.

[6] Financial Security Institute, “Financial security vulnerabili ty check guide, web application", 2016.

[7] KOSCOM Authorized Certification Center, "Developer Guide for Signature Korea Certification Service," 2017.