한국컴퓨터정보학회 하계학술대회 논문집 제23권 제2호 (2015. 7)

안전한 통합 인증 시스템 연구

박 재경°
*°한국과학기술원 사이버보안연구센터
e-mail : wildcur@kaist.ac.kr°

A Study of Secure Total Authentication System

Jae-Kyung Park°
*°Cyber Security Research Center of KAIST

● Abstract ●

본 논문에서는 기존 인증체계의 문제점을 살펴보고 이를 개선하기 위한 방안을 제안한다. 현재 국내에서 금융관련 서비스에서 공인인증서를 사용하는 서비스가 대부분이나 실용성 및 보안 문제로 인해 최근 정부에서는 공인인증서 사용 의무제도를 폐지하기에 이르렀지만 현재 공인인증서를 대체할만한 안전한 수단을 확보하지 못했고 기존의 OTP나 보안카드로 공인인증서의 공백을 메우기에는 역부족이다. 따라서 공인인증서를 대체할 수 있는 인증방안에 대해 제안하고 이를 통해 보다 안전한 인터넷 전자상거래를 유도하고자 한다.

키워드: 공인인증서(Certificate), 전자상거래(Electronic Commerce), 인터넷뱅킹(Internet Banking), 인증(Authentication)

I. Introduction

최근 대규모의 개인정보가 유출되는 사건이 빈번하게 발생하고 있으며 개인정보 및 전자거래 보안에 대한 불안심리가 커지고 있다. 게다가 피싱이나 해킹 등으로 유출된 은행 공인인증서가 4년 새 100배나 증가한 것으로 나타났다[1]. 또한 전자상거래에 대한 직관적인 인증서비스로 보다 실용적이고 불안을 덜 수 있는 기술 및 제도가 필요한 시점이다. 2014년 전자금융 거래법 및 전자서명법이 개정되어 해킹사고 발생 시 과실입증 책임이 금융기관에 귀속되었으며 공인인증서를 이용한 강제적 전자상거래 조항도 삭제되었다[2]. 하지만 공인인증서를 대체할만한 보안 수단이 마련되지 않은 상태에서 대체수단을 마련하는 것이 매우 시급한 실정이다. 현재의 보완 수단으로 사용되고 있는 기존 OTP(One Time Password) 및 스마트 OTP 역시 보안안전성 측면에서 미흡하다는 조사결과가 나왔다[5]. OTP는 보조적인 역할 일뿐 실제 전자상거래를 할 경우 핵심 비밀번호를 다시 입력해야 하는 문제는 여전히 남아 있다[3]. 본 논문에서는 인증서를 대체하고 기존의 보안 장치의 보안성을 뛰어넘는 통합인증 방안을 제안하고자 한다. 통합인증 서비스는 향후 비대면 서비스가 활성화될 것을 고려하여 선제적이고 개방형 형태의 표준화 방안을 제안하고자 한다.

II. 관련연구

1. Related works

핀테크(FinTech) 는 금융을 뜻하는 파이낸셜 (financial)과 기술(technique)의 합성어로 모바일 결제 및 송금, 개인자산관리, 크라우드 펀딩 등 정보기술(IT)을 기반으로 한 새로운 형태의 금융 기술을 말한다. 핀테크 비즈니스 모델과 사업 영역을 분류하는 기준은 크게 은행업 및 금융 데이터 분석(Banking & Data Analytics), 지급결제(Payment), 자본시장 관련 기술(Capital Market Tech), 금융자산 관리(Finance Management) 등 4가지 영역으로 정리돼 가고 있다. 핀테크의 등장은 기존의 금융 질서를 파괴하며 창의와 혁신에 바탕을 둔 비즈니스 모델들을 쏟아내고 있다. 통화의 종류, 결제 시스템 같은 기존의 장벽을 허물고 보다 간편하고 보안 이슈까지 잡은 기술들이 속속 등장하기 때문이다. 최근 들어서는 단순한 결제나 송금 서비스뿐만 아니라 고객의 개인정보·신용도·금융사고 여부 등을 빅 데이터 분석으로 정확하게 파악하는 알고리즘 기술까지 등장해 개인 자산 관리 서비스까지 그 영역을 확대 중이다[4].

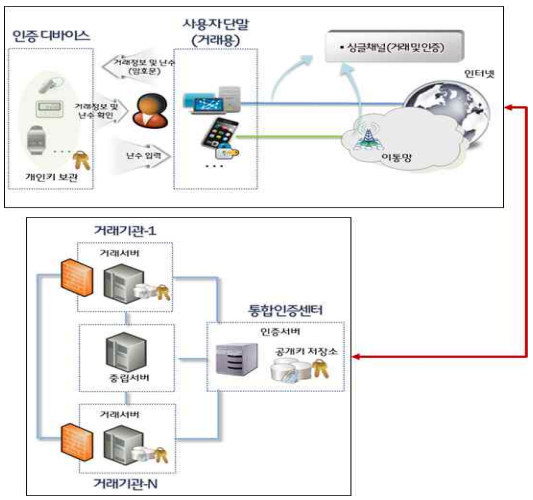
III. The Proposed Scheme

본 논문에서 제안하는 통합인증의 개념으로 그림 1과 같이 제안하며 본인확인, 접속인증, 거래인증 등의 범용적인 통합인증 서비스를 제공하는 것을 목표로 한다.

Target System of Total Authentication

본 논문에서 제안한 통합인증의 시스템 구성은 단말을 통해 인터넷으로 본인인증이나 거래를 할 사용자는 인증디바이스를 통해 거래에 필요한 인증값을 받아 거래기관에 제출하여 안전하게 거래를 진행할 수 있다. 본 논문에서 제안한 개념은 기존의 공인인증 방식과는 달리 거래시점에 사용자가 외부 기관을 통해 실시간으로 인증을 받는다는 점이 상이하다. 다만 사용자가 거래를 위한 임의의 값을 입력해야하지만 이 부분은 기술적으로 얼마든지 자동화가 가능하다. 즉, 향후 도입되는 스마트워치나 착용 디바이스 등을 활용하면 가능하며 현재의 스마트폰에서도 자동 인식 기능을 추가할 경우 자동화가 가능하다. 즉, 스마트폰과 사용자가 고유하게 보유하고 있는 디바이스를 상호 인식시켜 인증에 활용할 경우 복제나 해킹이 불가능하다.

그림 2와 같이 기존의 공인인증서 방식이 아닌 공개키 방식을 사용하므로 보안의 비도는 높게 유지하면서 사용자는 간편하게 거래를 위한 인증을 받을 수 있다. 따라서 근본적인 해킹이나 복제가 불가능한 서비스를 제공할 수 있다.



System Diagram

IV. Conclusion

본 논문에서 제안한 통합인증 서비스는 기존의 공인인증서 방식의 문제점을 해결하고 추가적인 인증 디바이스를 제안하여 보안성과 편의성을 모두 해결하였다. 공인인증서 제도를 폐지함에 따라 거래서비스를 제공하는 사업자나 기관은 별도의 인증 방식을 마련해야 한다. 이때 사용자가 간편하게 소유할 수 있는 인증 디바이스를 제공하여 통합인증 서비스를 수행한다면 비대면 서비스에서도 대면 서비스 못지않은 인증을 수행할 수 있다고 판단한다. 다만, 인증서버에 공개키를 저장하기 위한 초기 등록 절차를 보다 간편하게 할 수 있는 방안을 마련해야 할 것이다. 통합인증 서비스를 활용한다면 전자 신분증 제도로도 활용이 가능하다는 것이 매우 큰 장점이라고 할 수 있다.

References

[1] http://news1.kr/articles/?1906344
[2] http://opennet.or.kr/e-finance-e-signature-reform.pdf
[3] http://biz.chosun.com/site/data/html_dir/2015/04/20/2015042003040.html
[4] http://terms.naver.com/entry.nhn?docId=2118001&cid=42107&categoryId=42107
[5] Seongmin Yoo, Jinseung Yu, Haegjin Jang and Jaecheol Ryou, “A Study on OTP Generation Method based on Software,” Journal of the HCI Society of Korea, HCI 2011, No. 1, pp. 173-176, 2011.