Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.6, Dec. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.6.1503

인터넷은행을 위한 개선된 본인확인 구조

홍 기 석,† 이 경 호‡
고려대학교 정보보호대학원

Advanced Mandatory Authentication Architecture Designed for Internet Bank

Ki-seok Hong,† Kyung-ho Lee‡
Graduate School of Information Security, Korea University

요 약

인터넷은행 환경 조성과 관련하여 금융당국이 발표한 비대면 실명확인 정책은 대면 이상의 정확성을 기하기 위해 다중확인을 원칙으로 하고 있다. 인터넷은행은 기존 인터넷뱅킹과 법적 실체와 사업모델이 다른데, 본인확인 구조로써 인터넷뱅킹의 본인확인 구조를 유지한 채 실명확인만 대면에서 비대면으로 대체하는 것은 최초 가입자에게 불편을 줄 뿐 아니라, 엄격한 대면확인을 거치는 인터넷뱅킹보다 보안위험에 더 노출될 수 있다. 본 연구는 인터넷은행의 서비스 단계를 등급화하고, 등급에 따라 차등화된 서비스등록 및 이용이 이루어지도록 개선된 본인확인 구조를 제안한다. 또한, 인터넷은행에 대해 발생할 수 있는 보안취약점과 공격모델을 수립하고, 각 공격모델에 대한 인증매체의 보안특성과 서비스 단계별 안전성을 분석한 결과 등급에 따라 기존 인터넷뱅킹보다 비슷하거나 더 높은 안전성을 제공하고, 이용자 가입 유도 측면에서 유용함을 확인하였다.

ABSTRACT

Non-face-to-face real name verification policy that financial authorities announced, in order to secure a face-to-face or more of accuracy, are in principle of multi check. The business model and legal entities of Internet banks is different from existing Internet banking. Relpacing real name verification from face-to-facd to non-face-to-face while maintaining the structure of identification can not only cause inconvenience to a first time member, but also can be more vulnerable to verious security risks. In this study, to evaluate a service level of a bank of the Internet, and provide an improved identification of the structure such that the registration and use of differentiated services is performed in accordance with the evaluation. In addition, the security that may occur with respect to Bank of the Internet to establish a vulnerability and attack model, the results of the analysis of the safety of the step-by-step security attributes and services of the authentication medium of each attack model, existing the safer than Internet banking, confirmed the usefulness in user registration guide

Keywords: real name verification, mandatory authentication, internet bank, internet primary bank, attack model

I. 서 론

인터넷은행은 영업점을 소수로 운영하거나 영업점 없이 업무의 대부분을 인터넷 등 전자매체를 통해 영위하는 은행을 말하며, 기존 은행 서비스를 인터넷으로 제공하는 인터넷 뱅킹과는 법적 실체에 있어 구분된다[1]. 인터넷은행은 기존 금융서비스에 핀테크 기술이 결합한 창의적인 사업모델 창출을 목적으로 추진되는데[2,3], 인터넷은행 환경 조성과 관련하여 금융당국의 비대면 실명확인 정책은 대면확인 이상의

Received(11. 03. 2015), Modified(12. 07. 2015), Accepted(12. 08. 2015)
† 주저자, kshong@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

정확성 제고를 위해 다중확인(3중 이상)을 원칙으로 하고 있다[4].

기존 은행의 인터넷뱅킹 서비스는 한번 엄격한 대면확인을 하면 계좌 추가개설, 조회, 이체, 대출 등 주요 은행서비스가 모두 오픈되는 본인확인 구조를 가진다. 그런데 인터넷은행의 본인확인 구조로써, 기존 인터넷뱅킹 본인확인에 실명확인만 대면에서 비대면으로 대체하는 경우, 최초 가입자에게 다중확인(3중이상)을 요구함에 따라 가입 단계별 앱 설치 및 대기시간으로 이용자에게 불편을 줄 수 있다. 또한, 최초 비대면 실명확인만으로도 모든 금융서비스가 오픈되므로, 엄격한 대면확인을 거치는 기존 인터넷뱅킹보다 보안위험에 더 노출될 수 있다. 특히, 영업점이 전국에 촘촘하게 배치된 국내 금융 인프라를 감안할 때, 기존 은행서비스 보다 편의성이나 보안성 측면에서 비교우위를 점하지 못하여 가입자 기반확보 및 창의적인 금융서비스 창출에 어려움을 겪을 수 있다.

본 연구는 계좌개설, 조회, 이체, 대출 등 인터넷은행 서비스 단계를 등급화하고, 등급에 따라 차등화된 실명확인, 서비스등록 및 이용이 이루어지도록 개선된 본인확인 구조를 제안한다. 또한 인터넷은행에 대해 발생할 수 있는 보안취약점에 대하여 가로채기, 메모리해킹, 단말제어 등의 공격모델을 수립하고, 본인확인 인증매체의 보안특성과 서비스 단계별 안전성을 분석한 결과, 등급에 따라 기존 인터넷뱅킹과 비슷하거나 더 높은 안전성을 제공하고, 이용자 가입유도 측면에서 유용함을 확인한다.

II. 연구배경 및 기존연구

2.1 연구배경

2.1.1 인터넷은행이란

인터넷은행은 영업점을 소수로 운영하거나 영업점 없이 업무의 대부분을 ATM, 인터넷 등 전자매체를 통해 영위하는 은행을 말한다[1]. 설립 초기에는 완전 무점포 형태의 온라인 위주로 이루어져 Direct Bank, Pure-play Internet Bank, Internet-only Bank 등의 명칭을 쓰고 이후 오프라인 시설을 보완적으로 이용하는 경우가 증가하면서 인터넷전문은행(Internet Primary Bank)이라는 명칭으로도 불린다[1].

인터넷은행은 은행서비스를 인터넷으로 제공하는 영업방식을 지칭하는 인터넷 뱅킹(Internet Banking)과는 법적 실체에 있어 구분되는데[1], 금융위원회는 예금, 대출, 결제 등 모든 은행업무에 핀테크를 접목하여 다양하고 창의적인 사업모델 출현 유도를 위해 인터넷은행 도입을 발표하였고[2], 예비인가 심사에서 혁신성 등 사업계획에 가장 큰 비중을 두고 있다[3].

2.1.2 실명확인과 본인확인의 개념

실명확인은 「금융실명거래 및 비밀보장에 관한 법률」(이하 "금융실명법")에 따라 거래자가 "실지명의"로 금융거래를 하는지 확인하는 것[4]으로, 성명과 실명번호 뿐 아니라 실명확인증표에 포함된 사진 등에 의하여 본인 여부를 확인하는 절차이다[5,6].

위에 따르면 금융실명법에서 정한 요건에 따라 본인확인을 할 때 실명확인이 성립[5,6]되므로, 본인확인이 실명확인을 포괄하는 개념이며, 실명확인은 법정 절차에 따른 본인확인의 특정된 방법이 된다.

계좌개설, 어음할인 등은 실명확인 대상이고, 실명이 확인된 계좌에 의한 계속거래, 보험 등은 실명확인 대상에서 제외하여 일반 금융관행에 따라 거래하도록 정하고[5] 있는데, 이에 대해 국내 은행들은 금융거래의 안전성을 기하기 위해 신분증, 공인인증서 등으로 본인확인을 하고 있다.

2.1.3 비대면 실명확인 방법

인터넷은행은 기존 은행 영업점의 대면 방식으로 신분증 제시를 통한 실명확인 및 전자금융서비스 신청·등록을 인터넷 등 비대면 방식으로 수행하므로 타인 명의 도용에 의한 계좌개설 및 전자금융서비스 신청·등록 위험이 상대적으로 높다. 이러한 위험을 감안하여 금융당국은 실명확인 합리화 정책으로써 비

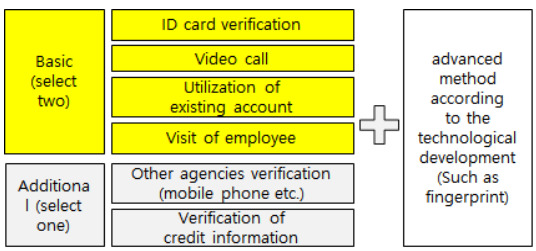

Fig. 1. Configuration of the non-face-to-face real name verification [7]

대면 실명확인 방식을 허용하되, 기본확인과 추가확인으로 구성된 방법을 다중(3개이상) 조합하도록 의무화 하였는데[7], 그 내용은 다음과 같다.

첫 번째, 신분증 확인은 고객이 신분증을 촬영 또는 스캔하여 인터넷(휴대폰 포함)을 통해 제출 하면 금융회사가 신분증 발급기관에 진위여부를 확인한다. 두 번째, 영상통화는 금융회사 직원이 이용자와 영상통화를 하면서 육안 및 안면인식기술을 통해 신분증상 사진과 고객 얼굴을 대조한다. 세 번째, 기존계좌 활용은 타 금융회사에 실명확인을 거쳐 이미 개설된 계좌로부터 소액이체 등을 통해 고객의 동 계좌 거래권한을 확인한다. 네 번째, 직원 방문은 현금카드, OTP발생기 등을 고객에게 우편 등으로 전달 시 은행직원 또는 전달업체 직원이 증표를 통해 실명을 확인한다. 추가인증 방법으로써 타 기관 확인결과 활용은 인증기관 등 타 기관에서 신분확인 후 발급한 휴대폰 번호, 공인인증서, 아이핀 등을 활용한다. 또한 다수의 개인정보 검증은 고객이 제공하는 개인정보와 신용정보사 등이 보유한 정보를 대조한다.

그런데 인터넷은행의 본인확인 구조를 인터넷뱅킹 본인확인 구조와 유사하게 적용하는 경우, 최초 계좌개설 시 신청자에게 높은 수준의 다중확인을 요구함에 따라, 생애 최초 예금개설 희망자나 신용불량자는 비대면 가입이 불가능하게 되고[8], 다중 단계별 앱 설치 및 대기시간이 발생하여 이용자에게 불편을 줄 수 있다. 한편, 인터넷은행은 휴대폰을 이용한 모바일뱅킹 이용이 주를 이룰 것으로 예측되는데, 국내 전자금융 통계에 따르면, 20대~60대 이상 휴대폰 보유율(97.7%)은 높으나, 모바일뱅킹 이용율(36.8%)은 낮게 나타났다. 낮은 이용율의 원인으로 정보유출 및 보안우려, 안전장치 불신, 실수로 인한 손실우려 등 보안에 대한 불신이 가장 높았고, 동시에 사용 미숙과 구매절차 복잡 등 불편성 또한 모바일뱅킹의 주된 불만 요소이다[9].

또한 한번 실명확인을 하고 전자금융서비스 이용자 등록을 하면, 계좌조회, 이체, 대출 등 모든 서비스가 오픈되어 대면확인을 통해 서비스를 오픈하는 기존 인터넷뱅킹 보다 해킹 위험에 더 크게 노출 될 수 있다.

Table 1. Feature of non face-to-face real name verification methods

Classification	Advantage	Disadvantage
ID card verification	Easy to use and accurate	Verification is difficult if damaged
Video call	Reliable due to visually	Cost of video call occurs
Utilization existing account	Held by the majority of users	There exists the possibility of spoofing by fishing, etc.
Visit of employee	Face-to-face confirmation possible	Time to ship
Other agencies verification	Versatility excellence	Risk of exposure via hacking, misplacement
Verificaion of a large number of credit info.	Most convenient to user	Risk of identify theft in case of personal information leakage

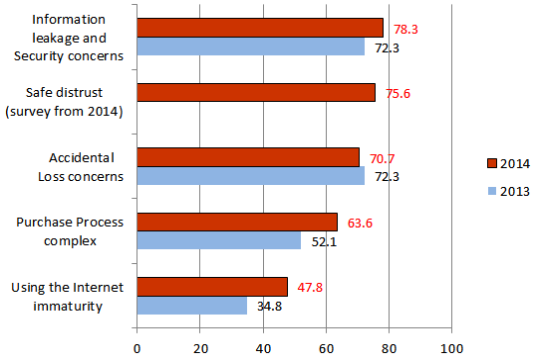

Fig. 2. The reason for mobile banking[9]

2.2 기존연구

지금까지 인터넷은행의 본인확인에 관한 연구는 크게 실명확인 제도 및 본인확인 기술 측면에서 이루어져 왔다. 특히, 정부가 2002년과 2008년 인터넷 전문은행 설립 및 제도 마련을 추진하면서 금융실명제도 개선 및 생체기술 및 금융인증 수단 등을 활용한 본인확인 방법의 보안성 측면에서 다양한 연구가 이루어졌다.

2.2.1 실명확인 제도관련 연구

각 연구들을 살펴보면 먼저, 구본성(2008)은 인터넷전문은행 도입과 관련하여 금융실명법을 개정하지 않는 범위 내에서 수용될 수 있는 비대면 실명확인 대안으로써 은행직원 방문, 업무제휴 대행기관을 통한 실명확인, 공인인증서를 통한 계좌개설, 인터넷

Table 2. Preceding research on real name finantial transaction system

researcher	contents
Bon-Seong Gu(2008)	The seek alternatives that can accommodate a range not to amend the financial real name Act
Tae-Ho Kim (2008)	It is necessary law of legislation on the prohibition of the transfer act of financial transaction account
Yong-Jae Kim (2013)	Duplicative face-to-face real name verification procedure unnecessary and claims of account opening in after a tough face-to-face confirmed via bank
Jae-Hoon Lee(2013)	Deposit people and accounts in order to ensure face-to-face resistance. There is a need to ensure the identity of the Yeti is the premise. and The proposed non-face-to-face real name verification scheme to maintain face-to-face resistance

동영상을 통한 대면확인 방법을 제시하였다[10]. 김태호(2008) 등은 인터넷은행이 공인인증서를 통한 온라인 계좌 개설시 예상되는 리스크와 대응방안을 제시하였다[11]. 김용재(2013)는 현행법상의 실명확인 절차가 구체적인 정합성과 타당성을 갖는지를 해외 주요국가와 비교법적으로 검토하고, 은행에서 최초의 계좌 개설 시 엄격한 대면확인절차를 완료했다면 그 이후의 금융계좌 개설은 완화된 실명확인절차를 거치도록 금융실명제도 개선방안을 제시하였다[12]. 이재훈(2013) 등은 금융실명제가 요구하는 실명확인 대면 절차가 유용한지를 판례에 비추어 분석하고 이에 따른 온라인 계좌개설을 위한 금융실명법 개선방안 및 대면성을 유지하는 비대면 실명확인 방법으로써 공인인증서 사용, 신분증의 우편 및 온라인 전송, 휴대전화 인증 방법 등을 제시하였다[13].

2.2.2 본인인증 기술관련 연구

방걸원(2002) 등은 생체인식기술인 지문인식과 문자인식기술을 접목하여 주민등록상의 지문이미지를 생체지문과 비교판별하는 본인확인 방법을 제안하였다[14]. Burr(2004) 등은 미국 연방기관 정보자원 접근을 위한 대면·비대면 실명확인 및 비대면 본인확인을 위한 가이드라인을 제안하였고, NIST는 이를 표준으로 제정하였다[15]. 정찬주(2008)는 웹사이트 회원가입시 본인확인방법으로 사용하고 있는 공인인증서, 전자서명, 휴대폰SMS, 신용카드정보 및 금융계좌정보 인증방식을 비교하고 금융보안 OTP를 이용한 온라인 본인확인 방안을 제시하였다[16]. Peotta(2011) 등은 인터넷뱅킹의 전형적인 공격모델과 취약점을 제시하였다[17]. 유한나(2011) 등은 인터넷뱅킹 본인인증 시, 사용자 PC와 Mobile 기기에서 이중으로 인증받는 Two Channel 인증방식을 제안하였다[18]. 이재식(2013)은 안전한 인터넷뱅킹 본인확인을 위하여 OTP발생번호를 스마트기기를 통하여 입력하는 기술구조를 제안하였다[19]. 이한욱(2013)은 메모리 해킹 악성코드에 의한 공격유형을 도출하고 메모리 해킹에 대해서도 안전한 사용자 인증수단을 제시하였다[20].

Table 3. Preceding research on mandatory authentication technology

researcher	contents
Geol-Won Bang(2002)	Reliable identification method presented a combination of character recognition and fingerprint recognition
Burr (2004)	Standardization of face-to-face and non-face-to-face real name verification and authentication guidelines for access to information resources of the United States federal government
Chan-Ju Jeong (2008)	In identity verification method at the time of membership registration of the web site, it presents the authentication method using the financial security OTP
Peotta (2011)	Presenting a typical attack models and vulnerabilities of Internet banking
Han-Na You (2011)	Proposal of Tow-Channel authentication method for the identification in the Internet banking confirm
Jae-Sik Lee (2013)	The proposed technology structure to enter through the smart equipment OTP password to the identification of secure Internet banking
Han-Wook Lee (2013)	The proposed secure user authentication means from memory hacking of Internet banking
Byeong-Cheol Cho (2015)	Analyzes the advanced technology and patent trends plurality of biological-based authentication technology, domestic technology development challenges presented

III. 인터넷은행의 본인확인 구조

3.1 제안하는 본인확인 구조

제안하는 본인확인 구조는 본인인증 모델, 실명확인 등급, 인증매체 등급으로 나누어진다. 미국 국립기술표준원의 Electronic Authentication 모델[15]을 참조하여 계좌개설, 조회, 이체, 대출 등 서비스 단계별로 증가하는 리스크에 대해 실명확인, 서비스 등록(인증매체 발급) 및 본인인증을 하도록 구성하였다.

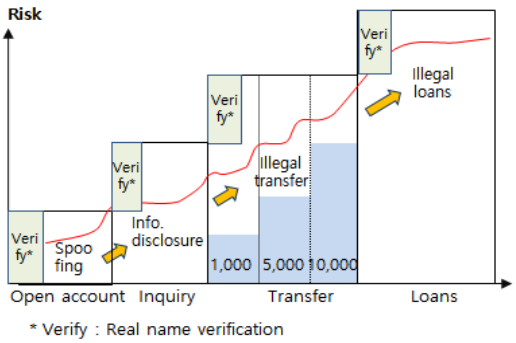

Fig. 3. Advanced mandatory authenticaion structure

3.2 본인확인 모델

본인확인 모델은 계좌개설 단계의 실명확인과 서비스 이용 단계의 본인확인으로 구성한다. 기존 비대면 실명확인이 확실한 신뢰성을 기반으로 최초 1회만 실시하고, 이후 인터넷뱅킹 서비스 이용을 위한 본인확인 절차가 분리된 구조인 반면, 제안하는 본인확인 구조는 비대면 실명확인과 본인확인을 서비스 단계별 등급관리를 하도록 통합한다. 본인확인 구성요소별 역할은 다음과 같다.

1) User : PC, 스마트폰 등으로 계좌개설 및 서비스를 이용하는 이용자를 의미한다.

2) Registration Agency(RA) : 이용자가 제출한 정보를 통해 실명확인하고, CA에 인증매체 발급 및 실명확인 등급 부여를 요청한다.

3) Certificate Agency(CA) : RA 요청에 따라 인증매체를 발급하고, 실명확인 등급을 부여한다.

4) Internet Banking System(IBS) : 인터넷을 통한 계좌개설, 조회, 계좌이체, 대출 등 금융서비스를 제공하는 시스템이다.

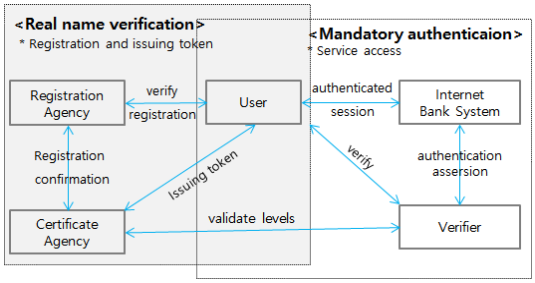

Fig. 4. Advanced mandatory authentication model[15]

5) Verifier : IBS의 요청에 따라 이용자가 제출한 인증매체를 통해 본인확인 서비스를 제공한다.

3.3 서비스 등급

서비스 등급은 서비스 등록시 필요한 실명확인 등급 및 서비스 이용시 필요한 본인확인(인증매체) 등급을 정의한다. 서비스 등급별 실명확인 및 본인확인 등급을 차등화 함으로써, 이용자가 본인에게 적합한 서비스 등급을 선택하고, 그에 따라 서비스에 등록하고 인증매체(본인확인 방법)를 지정하도록 구성한다.

1등급은 계좌개설 단계로서 실명확인 1등급 등록 후 계좌생성, 전자금융서비스 신청·등록이 이루어지고, OTP, 현금카드를 발급하여 직원이 전달한다. 2등급은 계좌조회 단계로서 실명확인 2등급 서비스

Table 4. Service levels (levels of real name verification and mandatory authentication)

Level		Service	Registration (real name verification)	Issuing token (mandatory authentication)
1		Openning accounts	Copy of ID cards	ID/password
2		Account Inquiry	Mobile phone auth.	Mac of terminals
3	a	Transfer	Utilization existing account	Security cards +SMS
	b			OTP + SMS
	c			Security cards +SMS + Certificate
4		Loans	Video call	Transaction linked OTP +SMS

등록 후, 2등급 인증매체를 발급한다. 3등급은 계좌 이체 단계로서 실명확인 3등급 서비스 등록 후, 이용자가 선택한 이체한도 금액에 따라 각각 3a, 3b, 3c 등급 인증매체를 발급한다. 4등급은 대출이 실행되는 단계로서 실명확인 3등급 등록 후, 4등급 인증매체를 발급한다. 금융실명법상 대출(여신)은 실명확인 대상이 아니나[5], 대출취급 업무의 리스크를 감안하여 정확한 차주(빌리는 사람) 확인을 위해 실명확인 수준의 본인확인으로써 영상통화를 한 후 4등급 서비스 등록을 한다.

3.4 실명확인 등급

인터넷은행은 기존 은행 제휴 영업점을 운영하는 온·오프라인 옴니채널 형태도 존재하는 관계로, 대면과 비대면 방식을 모두 포괄하여 정의한다. 대면 실명확인 1~4등급은 기존 영업점 실명확인과 동일하다. 비대면 실명확인 1등급은 신분증진위확인 시스템을 통해 이용자가 신분증 촬영, 스캔 등으로 제출한 신분증 사본의 성명, 식별번호, 발급일자와 사진이 발급기관 정보와 일치여부를 확인하고, 사용자 단말의 Mac값을 등록한 후, 공식주소(주소, 이메일, 휴대폰)로 실명확인 내역을 통지한다. 2등급은 휴대폰번호, 실명번호가 통신사 저장 정보와 일치하면 휴대폰으로 인증코드를 전송하고, 신청자가 인증코드를 제시하여 등록한다. 3등급은 기존에 실명 확인된 타행 계좌로부터 이체 거래를 통해 계좌번호 및 실명번호를 확인한 후 등록한다. 4등급은 영상통화자 얼굴과 신분증 사진을 대조하는 안면인식을 통해 등록하고, 등록사실 부인방지를 위해 영상통화 내역을 녹화한다.

Table 5. Level of real name verification

level	Face-to-Face	Non Face-to-Face
1	ID cards (scan and check authenticity)	Coyp of ID cards(transfer by mobile phone and check authenticity)
2	Equals to level 1	Level 1 + mobile phone auth.
3	Equals to level 1	Level 2 + utilization existing account
4	Equals to level 1	Level 2 + video call

3.5 본인확인 등급

인증매체는 알고 있는 것, 가지고 있는 것, 신체의 일부 3가지 유형으로 나누어진다[15]. 안전성 또한 알고 있는 것, 가지고 있는 것, 신체의 일부 순서로 높아지며, 이러한 특징을 반영하여 본인확인을 한다. 1등급은 최초 계좌개설(실명확인)으로, ID/비밀번호가 이용된다. 2등급은 1등급에 더하여 실명확인 시 등록한 이용자 단말의 Mac값을 추가 확인한다. 3등급은 이용금액 한도에 따라 a, b, c로 나누어지며 2등급에 다음과 같이 추가 확인한다. 3a는 보안카드를 통해 추가 확인하여 일일 최고 1천만원까지 이체한다. 3b는 OTP를 추가 확인하여 일일 최고 2억 5천만원까지 이체한다. 3c는 기존 인터넷뱅킹 이체 시 본인확인에 준하는 수준으로서, 공인인증서를 추가 확인하여 일일 최고 5억원까지 이체한다. 4등급은 영상통화를 통해 추가 확인하여 대출을 실행한다. 4등급 인증매체는 2가지를 제안한다. 첫 번째는 수취인 계좌번호나 거래금액에 따라 비밀번호가 생성되는 거래연동 OTP이다. 두 번째는 범용적 활용체계가 갖춰지지 않았으나, 비대면 실명확인 정책[7]의 창의적인 방법에 포함되고, 은행권 공동구축 방안이 연구되고 있는 지문인식을 추가적으로 포함하여 검토한다.

Table 6. Level of mandatory authentication

Level	Tokens	Remarks (unit: ten million Won)
1	ID/password	-
2	Level 1 + Mac	-
3a	Level 2 + SMS + Security card	(One time) 1 (One day) 1
3b	Level 2 + SMS + OTP token	(One time) 5 (One day) 25
3c	Level 2 + SMS + Certificate + OTP	(One time) 10 (One day) 50
4	Level 2 + SMS + Transaction linked OTP token or, level 2 + fingerprint	Depends on collateral

IV. 안전성 및 유용성 분석

4.1 안전성 분석

4.1.1 공격모델 수립

인터넷은행을 대상으로 한 공격모델은 전형적인 인터넷뱅킹 공격 모델[17]에 신종 전자금융사기수법으로써 국내 피해사례 보고가 급증하고 있는 메모리 해킹[20,21]을 반영하여 3가지 공격트리를 수립한다. Type A는 가로채기로 PC, 스마트폰 등 이용자 단말에 입력된 값에 접근하여 데이터를 공격자에게 전송하고 공격자가 이를 재사용하여 공격한다. Type B는 메모리 해킹으로 이용자 단말에 입력된 정보와 단말내에서 처리되는 연산에 접근하여 데이터를 공격자에게 전송하고 이용자 단말의 정상적인 금융거래를 방해하는 동안 공격자 단말에서 비정상적인 금융거래를 실행한다. 공격자 단말 내에서 계좌이체 금액과 수취인 계좌번호 등의 금융거래 정보를 변조한 후, 보안카드, 단순형 OTP와 같이 허용시간 동안 본인확인 공격에 성공한다. Type C는 단말제어 공격으로 이용자 단말에 입력된 정보와 단말내에서 처리되는 연산에 접근하여 공격자 지시에 따라 이용자 단말 내에서 계좌이체 금액과 수취인 계좌번호 등의 금융거래 정보를 변조한 후, 보안카드, 공인인증서, OTP[1] 같은 본인확인 수단 공격에 성공한다.

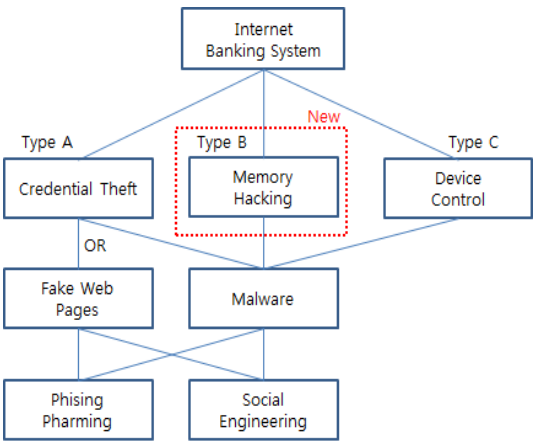

Fig. 5. Advanced attack tree

1) OTP의 경우 메모리해킹이나 단말제어 공격으로 탈취한 숫자를 허용시간 동안 공격에 성공할 수 있음

Table 7. Behavior of the attacker[20]

Class	Attack model	Behaviors of attacker			Location of attack
		Access to info	Data falsify	Device control	
Type A	Credential cheft	○	X	X	User's terminal
Type B	Memory hacking	○	○	X	Attacker's terminal
Type C	Device control	○	○	○	User's terminal

4.1.2 인증매체별 보안특성

인증매체별 보안특성은 각 공격모델에서 공격자가 입수하지 못한 정보에 대해서 무작위 공격 실행을 가정하여 비교분석 한다. 반대로, 공격자가 인증정보 및 인증매체를 확보하면 공격에 성공한 것으로 가정한다. 한편, 최대한의 안전성 분석을 위해, 일반적인 이용자 단말 상황과는 달리, 공격자가 단말에 악성코드를 주입하여 운영체제 메모리에 접근 가능하고, 이용자 단말을 장악하여 원격제어 가능한 강력한 공격수단을 확보한 것으로 가정한다.

(서비스 등록단계) 실명확인 1등급 휴대전화 인증은 공격자가 휴대폰번호(11), 주민번호(13) 조합으로 공격할 때 성공률 $P_1 = 10^{-23}$ 이다. 2등급 신분증 사본은 성명(6Byte), 주민번호(13), 발급일자(6)의 조합으로 공격할 때 성공률 $P_2 = 2^{-48}\times10^{-13}\times10^{-6} = 2^{-48}\times10^{-19}$ 이다. 3등급은 타행으로부터 계좌이체에 필요한 공인인증서(6), 보안카드(4), 계좌비밀번호(4)의 조합으로 핸드폰을 장악하여 계좌이체 SMS 인증을 확보한 것으로 가정하여

Table 8. Property of real name verification method

Token	Composition	Stored
Mobile phone auth.	Mobile phone number, regtistration number	Human memory
Copy of ID cards	Name, registration number, date of issue	Mobile phone, etc
Transfer	Certificate, password of account, security cards, SMS	Human memory, mobile phone, etc
Video call	Face patterns	Part of body
Fingerprint	Finger patterns	Part of body

공격할 때 성공률 $P_3 = 10^{-6}\times30^{-2}\times10^{-4} = 10^{-10}\times30^{-2}$ 이다. 4등급은 영상통화 시 안면패턴의 FAR(타인의 안면이 성공할 확률)은 10^{-2}[22]이나, 영상이미지 획득 뿐 아니라 상담원과의 불특정 질의응답 및 안면패턴에 대한 타임스탬프 등으로 인하여 공격 성립이 불가능하여 성공률 $P_4 = 0$ 이다.

(서비스 이용단계) 본인확인 1등급은 ID(6), 비밀번호(8) 조합으로 공격할 때 성공률 $Q_1 = (26+10)^{-6}\times(26+10+21)^{-8} = 36^{-6}\times57^{-8}$ 이다. 2등급은 실명확인 2등급 실행 시 등록한 핸드폰 Mac(48bit)으로 공격할 때 성공률 $Q_2 = 2^{-48}$ 이다. 3등급 a는 보안카드(4)와 SMS(6) 조합으로 공격할 때 $Q_{3a} = 30^{-2}\times10^{-6}$ 이다. 3등급 b는 OTP발생기(6)와 SMS(6) 조합으로 공격할 때 $Q_{3b} = 10^{-6}\times10^{-6} = 10^{-12}$ 이다. 3등급 c는 공인인증서(8)와 보안카드(4), SMS(6)의 조합으로 공격할 때 $Q_{3c} = (26+10+21)^{-8}\times10^{-6}\times10^{-6} = 57^{-8}\times10^{-12}$ 이다. 4등급은 거래연동 OTP발생기(수취인계좌번호, 금액, 비밀번호)와 SMS(6) 조합으로 공격할 때 $Q_{3c} = 10^{-27}\times2^{-240}$ 이나 거래연동 OTP 해킹사례가 아직 없고 현실적으로 불가능하므로 0 이다. 4등급 인증매체로 추가 검토하는 지문인식의 경우 FAR은 10^{-4}[22] 이나 지문패턴 생성 시 타임스탬프등으로 인하여 공격 성공이 어려우므로 성공률 $P_4 = 0$ 이다.

Table 9. Property of mandatory authentication tokens

Token	Composition	Stored
ID	Alpharbet,number (6)	Human Memory
Password	Alpharbet,number, special characters (8)	Human Memory
MAC of terminal	48bit	Terminal
SMS	Number(6)	Phone
Security cards	Number(4)	Cards
OTP token	Number(6)	Tokens
Certificate	Alpharbet,number, special characters (8)	Terminal
Transfer linked OTP	Benificiary account number, Transfer amount, OTP generated number	Tokens
Fingerprint	Fingerprint patterns	Part of body

4.1.3 서비스등록(실명확인) 단계의 안전성

최대한의 안전성 분석을 위해, 공격자가 악성코드를 주입하여 메모리공격 및 원격 단말제어가 가능한 상태에서 아래과 같다.

(Type A 가로채기) 1등급은 공격자가 신분증 사본 및 개인정보를 취득하여 타인명의 계좌개설이 가능하다. 따라서, 계좌개설 직후 직원이 방문하여 현금카드 등을 전달하는 과정에 신분확인을 하는 후속대책을 적용할 필요가 있다. 2등급 휴대폰 인증은 휴대폰 번호 취득은 가능하나 휴대폰을 소지하지 못하므로 추가공격이 필요하다. 3등급 계좌이체는 타행 계좌이체에 필요한 인증매체를 소유하지 않은 상태에서 공격으로부터 안전하다. 4등급 영상통화는 영상 및 이미지 취득이 가능하나, 은행측의 신분증 진위확인서비스(성명, 실명번호, 사진이미지를 발급기관 DB와 대조)를 통한 실명확인 성공은 어려우므로 안전하다.

(Type B 메모리해킹) 1등급 신분증 사본을 통한 인증은 Type A와 동일하다. 2등급 휴대폰 인증은 휴대폰 번호 취득이 가능하나 가입자식별모듈(USIM)을 소지하지 못하여 추가 공격이 필요하다. 3등급 계좌이체는 타행 계좌이체에 필요한 인증매체를 소유하지 못하여 추가 공격이 필요하다. 4등급 영상통화는 영상 및 이미지 취득이 가능하나, 은행측의 신분증 진위확인서비스(성명, 실명번호, 사진이미지를 발급기관 DB와 대조)를 통한 실명확인 성공은 불가능하고, 지문정보는 취득이 가능하나, 은행창구에서 등록한 지문과 대조를 통한 타인에 의한 실명확인으로부터 안전하다.

Table 10. Safety of real name verification

Service level	Attack success rate[2)]		
	Credential theft	Memory hacking	Device control
Openning account (1)	100% [0]	100% [0]	100% [0]
Inquiry (2)	2-48×10-19	2-48×10-19	100%
Transfer (3)	0	10-10×30-2	10-10×30-2
Loans (4)	0	0	0

2) 괄호 안은 현금카드 등 전달 시 직원에 의한 본인확인 등 추가 대책을 적용한 이후의 공격 성공율

(Type C 단말제어 공격) 1등급 신분증 사본을 통한 인증은 Type A와 동일하다. 2등급 휴대폰 인증은 휴대폰 번호 취득이 가능하고 단말을 직접 제어하므로 가입자식별모듈(USIM)을 소지하지 않아도 원격 제어를 통해 공격에 성공한다. 3등급 계좌이체는 타행 계좌이체에 필요한 인증매체를 해킹을 통해 소유하지 못하여 추가공격이 필요하다. 4등급은 Type B와 동일하다.

위를 정리하면, 서비스 등록단계 실명확인에 대한 안전성 분석결과 가장 강력한 공격모델인 Type C 단말제어에서 1, 2단계는 취약하고, 3단계는 기존 인터넷뱅킹 본인확인과 안전성이 등등하며, 4단계는 기존 인터넷뱅킹보다 높은 수준의 안전성을 제공한다. 따라서, 1단계 계좌개설(서비스등록) 후 직원 방문을 통한 현금카드 전달 시 실명확인하는 보안대책을 적용하고, 보다 안전한 인터넷은행 실명확인을 위해서는 3단계 또는 4단계를 선택할 필요가 있다.

4.1.4 서비스 이용(본인확인) 단계의 안전성

최대한의 안전성 분석을 위해, 공격자가 악성코드를 주입하여 메모리공격 및 원격 단말제어가 가능한 상태에서 아래과 같다. 1등급은 최초 계좌개설 단계로 실제 본인인증이 발생하지 않으므로 분석대상에서 제외한다.

(Type A 가로채기) 2등급 단말 Mac값은 취득 가능하나, 공격자가 이용자 단말을 소유하지 않아서 Mac 인증 추가공격이 필요하다. 3등급 a의 보안카드 지시번호와 SMS 지시번호 취득은 가능하나, 휴대폰을 소유하지 않아서 추가 공격이 필요하다. 3등급 b의 OTP 지시번호와 SMS 취득은 가능하나, 휴대폰을 소유하지 않아서 추가 공격이 필요하다. 3등급 c의 공인인증서 비밀번호는 가로채기가 가능하나 공인인증서 자체를 소유하지 않았으므로 공격에 안전하다. 4등급 중 거래연동형 OTP지시번호는 취득은 가능하나 서버에서 이용금액과 계좌번호 변조 여부를 확인할 수 있으므로 안전하고, 지문정보는 취득 가능하나 은행 창구에서 대면 등록한 지문과 일치 여부 및 타임스탬프를 서버에서 확인 가능하므로 안전하다.

(Type B 메모리해킹) 2등급 단말 Mac값은 취득 및 변조 가능하여 피해자 단말을 미소유한 상태에서도 공격자가 Mac 인증에 성공한다. 3등급 a 보안카드 지시번호는 메모리해킹을 통해 취득 가능하다. 3등급 b OTP[3]는 지시번호 취득 후 일정한 허용시간 동안 공격이 가능하고, 3등급 c의 공인인증서 비밀번호는 가로채기가 가능하나 공인인증서 자체를 소유하지 않았으므로 추가공격이 필요하다. 4등급 거래연동형 OTP 지시번호는 취득 가능하나, 서버에서 이용금액과 계좌번호 변조를 서버에서 확인할 수 있으므로 추가 공격이 필요하다. 4등급 지문정보는 지문패턴 취득은 가능하나, 은행 창구에서 대면 등록한 지문과 대조 및 타임스탬프를 통해 변조 여부를 서버에서 확인 가능하므로 안전하다.

Table 11. Property of mandatory authentication

Service level	Attack success rate		
	Credential theft	Memory hacking	Device control
Inquiry (2)	2^{-48}	100%	100%
Transfer (3a)	$30^{-2}\times10^{-6}$	100%	100%
Transfer (3b)	10^{-12}	100% [in allowed time]	100% [in allowed time]
Transfer (3c)	0	$57^{-8}\times10^{-12}$	100% [in allowed time]
Loans (4)	0	0	0

(Type C 단말제어) 2등급, 3등급 a, 3등급 c는 Type B와 동일하다, 3등급 c는 공인인증서와 공인인증서 비빌번호, OTP지시번호 획득이 가능하므로 허용시간내에서 공격에 성공 가능하다. 4등급은 Type B와 동일하다.

위를 정리하면, 공격자가 Type B 및 Type C의 강력한 공격모델에서 2~3단계는 취약하여 기존 은행의 인터넷뱅킹(Table 13.)과 유사한 정도의 보안성을 제공한다, 4단계의 경우 모든 공격모델에서 공격에 성공하지 못하는 강력한 안전성을 제공한다. 따라서, 비대면으로 운영되는 인터넷은행의 특징을 감안할 때, 기존 인터넷뱅킹과 비슷한 보안수준을 제공하는 3단계 또는 더 안정적인 보안수준을 제공하는 4단계를 선택할 필요가 있다.

3) 피싱사이트 접속을 유도하여 OTP 발생번호를 입력하게 하여 불법 계좌이체하는 사고사례[20,24,25]가 보고됨

Table 12. Safety of internet banking mandatory authentication[23]

Classification	Attack success rate	
	Guessing attack	Memory hacking
Certificate +Security cards	10^{-4}	100%
Certificate + OTP	10^{-6}	100%
HSM +Security cards	$2^{-2048}\times N$	100%

4.2 유용성 분석

국내 지급수단 이용형태 분석결과에 따르면, 인터넷뱅킹 서비스는 계좌조회가 90.9%, 계좌이체가 9.1%, 대출이 0.0%를 각각 점유하고 있다. 또한 일인당 결재성예금 보유율은 99.6%로 대다수 국민이 대면 실명확인을 완료한 예금을 보유하고 있으며, 예금잔액은 100만원~300만원이 40.5%, 100만원 미만이 32.0%로, 대다수 예금이 300만원 이하 잔액을 유지하는 것으로 나타난다[9].

제안하는 인터넷은행 본인확인 구조는 낮은 등급 서비스에 대해 낮은 본인확인 등급을 요구한다. 계좌개설, 조회 등 이용률이 가장 높은 서비스에 대해 낮은 등급의 간편한 실명확인 방법을 요구하는데, 이러한 구조는 이용자에게 편의성을 제공하여, 이용자에게 가입을 유도하고 인터넷은행의 초기 가입자 기반 확보에 효과가 있을 것으로 기대된다.

또한, 높은 등급 서비스를 이용하기 위해서는 실명확인을 통하여 추가적으로 서비스 등록을 하고, 높은 안전성을 원하는 이용자는 높은 등급의 인증매체를 신청하여 발급받을 수 있다. 이처럼, 제안하는 인터넷은행 본인인증 구조는 이용자가 자신에게 적합한 서비스 및 보안수준을 선택하게 함으로써, 기존의 공급자 중심의 서비스를 이용자 중심의 서비스로 전환하는 효과도 있을 것으로 기대된다.

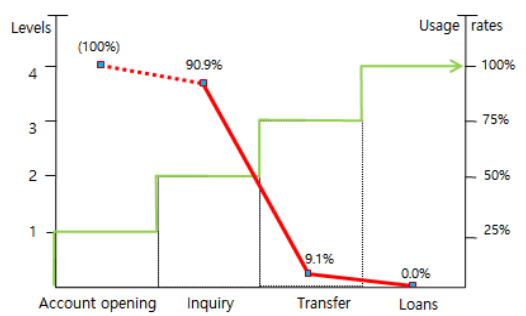

Fig. 6. Expected usage rates

V. 결 론

인터넷은행 안전성을 위한 본인확인 방법으로서 서비스 등급에 기반한 본인확인 구조는 낮은 서비스 등급에 대해 낮은 등급의 본인확인 방법을 적용하더라도 기존 인터넷뱅킹 본인확인에 비해 가로채기공격, 메모리해킹, 단말제어 공격으로부터 등급에 따라 기존 인터넷뱅킹 본인확인 구조와 비슷하거나 더 높은 안전성을 제공함을 확인하였다. 또한, 이용자의 가입 유도를 통해 인터넷은행 고객기반 확보에 유용함을 확인하였다. 다만 아직 인터넷은행이 설립 전이고, 운영 데이터가 존재하지 않은 관계로 본인인증 구조와 이용자의 가입실적과의 관계를 정량적으로 규명하는데는 한계가 있었다.

향후 인터넷은행이 설립되어 운영단계에 들어서면, 본인확인 구조의 안전성과 유용성에 대한 상관관계를 정량적인 데이터를 기반으로 연구할 필요가 있다.

References

[1] Financial Services Commition, http://www.fsc.go.kr/know/wrd_list.jsp?menu=7420000&dn_no=490, Financial Glossary

[2] Financial Services Commission, "Internet Primary Bank will be Introduced," Press Release, Jun. 2015

[3] Financial Services Commission, "Internet Primary Bank Preliminary Approval Examination Will Review Centered on Innovation," Press Release, Sep. 2015

[4] Ministrary of Government Legislation, http://www.law.go.kr/lsInfoP.do?lsiSeq=154291&efYd=20141129#0000 "Law of Real Name Financial Transaction System", Nov. 2014

[5] Financial Services Commission, "A Comprehensive Handbook of The Real

Name Financial Transaction System," pp. 3-6, 2008
〔6〕 Korea Federation of Banks, "A Commentary of The Real Name Financial Transaction System," Dec. 2010
〔7〕 Financial Services Commission, "A Rationalization of Real Name Verification on the Account Opening," May. 2015
〔8〕 Byeong-Ho Seo, "Non-face-to-face real name verification introducing notes on," Financial Weekly Briefing, Korea Institute of Finance, 25(3), May. 2015
〔9〕 The Bank of Korea, "2014 The Result of The Usage Patterns of Means of Payment and Implications," Survey Materials 2005-1, Jan. 2015
〔10〕 Bon-Seong Gu, "An Introduction of Internet Bank," Korea Institute of Finance, Finance Policy Research Report, Mar. 2008
〔11〕 Tae-Ho Kim, "A study on Preparation for The Electronic Finance Risk of Domestic Internet Only Bank," Korea Institute of Information Security and Cyptology, 8(5), Oct. 2008
〔12〕 Yong-Jae Kim, "Need for Elimination of The Regulatory Arbitrage on The Real Name Financial Transaction System and The Advancement of The Regulation of The Real Name Verification Procedures," The Korean Journal of Securities Law, 14(2), 2013
〔13〕 Jae-Hoon Lee "Improvement of The Electronic Finantial Service and Developement of The Real Name Financial Transaction System," IT and Law Research 7, Feb. 2013
〔14〕 Geol-Won Bang, "Implementation of The Fingerprint Identification Algorithm Fingerprint Registration," Korea Multimedia Society, pp. 585-589, 2002
〔15〕 William E. Burr, Donna F. Dodson and Elaine M. Newton "Electronic Authentication Guideline", NIST Special Publication 800-63-2, Aug. 2013
〔16〕 Chan-Ju Jeong "Research for Online Identity Verification Using Financial Security OTP," Information Security Journal, 18(5), Oct. 2008
〔17〕 Peotta, Laerte, et al. "A formal classification of internet banking attacks and vulnerabilities," International Journal of Computer Science & Information Technology vol. 3, no. 1, pp. 186-197. Feb. 2011
〔18〕 Han-Na You "A Study on the Two-channel Authentication Method which Provides Two-way Authentication using Mobile Certificate in the Internet Banking Environment," The Journal of The Korean Institute of Communication Sciences 36(8), pp. 939-946, Aug. 2011
〔19〕 Jae-Sik Lee, "A Design of Service Provider Model and Authentication Seheme for Secure Internet Banking," Ph.D. Thesis, Soongsil University Graduate School, Jun. 2013
〔20〕 Han-Wook Lee and Hu-Gen Shin "A Review of User Authentication Strong to The Memory Hacking Attack," Korea Institute of Information Security and Cyptology 23(6) Dec. 2013
〔21〕 National Police Agency, http://www.police.go.kr/portal/main/contents.do?menuNo=200286, New Financial Crime(Memory Hacking)
〔22〕 Byung-Chul Cho and Jong-Man Park "Technology Review on Multimodal Biometric Authentication," The Journal of Korean Institute of Communications and Information Sciences 40(1) Feb, 2015
〔23〕 Chang-Hyun Cho, "Research on mobile communication dual channel authentication mechanism for Internet banking environment, security," Soongsil University Graduate School, Jun. 2010
〔24〕 Ditital Times, http://www.dt.co.kr/ cont

ents.html?article_no=201508130210055
8739001 13. Aug, 2015
〔25〕 Dititat Times, http://www.dt.co.kr/ cont
ents.html?article_no=201501280210035
1800001 28. Jan, 2015

〈저자소개〉

홍 기 석 (Ki-Seok Hong) 정회원
1998년 2월: 아주대학교 산업공학과 졸업
2014년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호정책, 전자금융보안, 개인정보보호

이 경 호 (Kyung-Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
1994년 2월~현재: 삼성그룹, 네이버(주), 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책