해외 온라인뱅킹 인증현황 및 향후 전망

변정호*, 이채창*, 이동훈*
*고려대학교 정보보호대학원
e-mail:paradoxlab@korea.ac.kr

Survey of Overseas Internet Banking Authentication Mechnisms

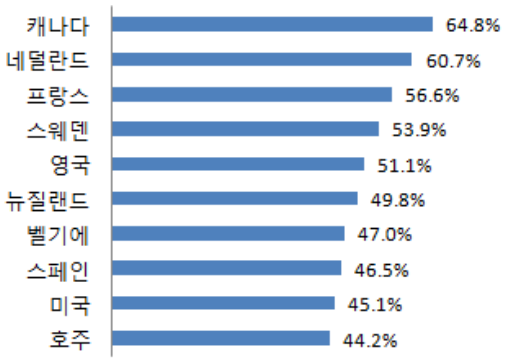
Jeung-Ho Byun*, Chae-Chang Lee*, Dong-Hoon Lee*
*Graduate School for Information Security, Korea University

요 약

1995년 세계 최초로 미국의 SFNB(Security First Network Bank)가 온라인뱅킹 서비스를 시작한 이래, 온라인뱅킹의 보급률은 전 세계적으로 급격한 성장세를 보이고 있으며, 이러한 성장세는 스마트폰, IPTV 등 새로운 전자금융 환경이 형성되면서 앞으로도 지속 될 것으로 판단된다. 온라인뱅킹이 이렇게 성장할 수 있었던 이면에는 보안성이 확보된 인증기술의 지속적인 개발이 큰 역할을 했다. 최근 우리나라는 인증기술의 보안성, 편의성, 다양성을 높이기 위한 다양한 노력들이 일어나고 있다. 특히 인터넷 익스플로러 기반의 공인인증서를 대체하기 위해 적극적인 연구가 진행 중에 있다. 본 논문에서는 금융 선진국이라고 할 수 있는 해외 주요 선진국들의 온라인뱅킹에서의 인증기술들을 살펴보고, 이러한 인증기술들의 비교, 분석을 통해 앞으로 등장 가능한 인증기술을 전망하며 향후 온라인뱅킹 인증기술과 관련된 연구에 기반이 되고자 한다.

1. 서론

인터넷 환경의 발달로 온라인뱅킹을 이용한 금융거래가 증가하고 있다. 한국은행에 따르면 2011년 전체 온라인뱅킹 서비스 등록 고객 수는 모바일뱅킹서비스 이용 증가로 전년대비 12.5% 늘어 7,482만 명을 기록하며 증가세를 이어갔다. 뿐만 아니라, 2010년 10대 온라인뱅킹 이용 국가 중 캐나다에서는 매달 온라인뱅킹에 접속하는 사용자가 약 65%로 인터넷을 통한 전자금융거래가 활발하게 이루어지고 있음을 볼 수 있다.



출처 : 컴스코어 미디어 메트릭스, 15세 이상, 2010년 8월

(그림 1) 2010년 온라인뱅킹 보급률 10대 국가

Finextra Research에 따르면 2010년, 미국의 45%의 온라인뱅킹 이용자 중 15%가 모바일뱅킹서비스를 이용하고, 2016년에는 모바일뱅킹서비스 이용자가 50%에 이를 것으로 예상하고 있다. 덧붙여 상대적으로 네트워크 기반 시설면에서 후발주자인 동남아시아 여러 나라에서도 온라인뱅킹 이용자는 지속적으로 증가하고 있는 추세이다.

<표 1> 2010년과 2011년 온라인뱅킹 방문자 수 비교
(단위 : 천 명)

구 분	2010년 1월	2011년 1월	변화율(%)
말레이시아	2,360	2,746	16%
홍콩	1,304	1,543	18%
베트남	701	949	35%
싱가포르	779	889	14%
인도네시아	435	749	72%
필리핀	377	525	39%

해외 각국의 금융회사들은 새롭게 등장하는 온라인뱅킹 환경에서의 보안위협에 대응하기 위하여 여러 가지 인증기술들을 지속적으로 개발하여 적용하여 왔다. PKI 기반의 공인인증서를 주요 인증기술로 이용해왔던 우리나라는 공인인증서가 모바일 환경을 비롯한 여러 가지 상황에서 적용성과 편의성을 만족시키지 못함에 따라 최근 공인인증서의 대체 가능한 새로운 인증기술을 모색하고 있는 중이다.

따라서 본 논문에서는 해외 온라인뱅킹에서 사용되는 다양한 인증기술들이 어떻게 보안성과 함께 적용성과 편의성을 제공하는지에 대해 살펴보고 비교하여, 향후 전망

*본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원사업"의 연구결과로 수행되었음

을 알아보고자 한다.

2. 인증기술의 이해 및 분류

온라인뱅킹에서의 인증기술은 원격지에 있는 사용자에 대한 인증기능뿐만 아니라, 사용자와 금융회사 간에 전송되는 거래내역의 무결성을 보장하는 기능을 포함한다. 최근 온라인 뱅킹에서 가장 위협이 되고 있는 MITB와 같은 공격은 거래내역에 대한 무결성을 위협하는 대표적인 공격기법이라 할 수 있다. 이러한 인증기술은 일반적으로 암호기술과 연동해서 제공되며, 거래당사자 이외에는 온라인 뱅킹에 접속하거나, 이체거래를 할 수 없도록 하는 기능을 한다.

인증에 쓰이는 정보를 인증요소(Authentication Factor)라고 하며, 인증요소 관점으로 <표 2>와 같이 세 가지로 분류 할 수 있다.

<표 2> 인증요소와 해당하는 대표 인증기술 예시

구분	인증요소	대표적인 인증기술 예시
1	지식기반의 알고 있는 것 (Something the user knows)	고정비밀번호, 등록정보질의응답
2	소지기반의 가지고 있는 것 (Something the user has)	보안카드, 스마트카드, H/W암호토큰, OTP발생기
3	특성기반의 고유한 것 (Something the user is)	바이오인증(지문, 정맥, 홍채 등)

이와 같은 인증요소 중에 하나를 이용하는 인증방식을 단일 요소 인증(single-factor authentication)라하며 보다 보안성을 높이기 위해서는 다수의 인증요소를 결합한 다중 요소 인증(multi-factor authentication)이 사용된다. 다중 요소 인증기술에는 전화인증과 같은 대역외(Out-of-Band) 인증과 위치기반 인증도 포함한다. 대역외 인증 방식은 인증요소를 복수로 사용하는데 있어서, 사용자와 온라인뱅킹 서버 사이에 2가지 이상의 채널을 사용하는 것을 말한다.

미국의 연방금융감독위원회(Federal Financial Institutions Examination Council)는 온라인뱅킹 환경의 인증 가이드라인을 통해 진화하는 온라인뱅킹 위협에 보다 적극적으로 대응하기 위해 이용자 인증을 단일 요소 인증에서 다중 요소 인증으로 갱신할 것을 권고 하고 있다. 실제로 우리나라를 비롯해 대부분의 나라에서는 사용자의 인증 및 거래내역의 무결성을 보증하기 위해 다중 요소 인증을 이용하고 있다.

3. 해외 주요국의 인증기술 현황 및 분석

본 장에서는 대표적인 금융 선진국들의 온라인뱅킹 인증기술 사례들을 살펴보고, 보안성과 이용편의성의 측면에서 장·단점을 알아본다.

3.1 CAP

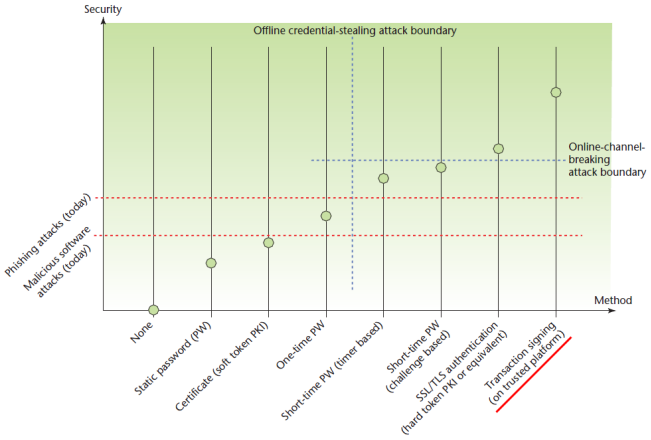
CAP(Chip Authentication Program)은 스마트카드 리더기 OTP로써, OTP단말기에 스마트카드를 장착하여 인식 한 후 OTP를 생성하는 형태이다. 거래정보를 반영하여 인증정보를 생성하고 거래정보가 위·변조되지 않음을 증명하는 거래연동 인증기술의 대표적인 기술로 꼽힌다. 영국을 포함하여 유럽에서 서비스를 시작하여 영국의 Barclays, Lloyds 등의 여러 은행에서 이용되고 있으며, 전 세계적으로 가입자 수가 8백만 명을 넘어섰다.

(그림 2) 스마트카드 리더기 OTP

CAP단말기는 확인(identify), 응답(respond), 서명(sign) 모드의 3가지 형태로 작동한다. 이 중 확인모드와 응답모드는 사용자 인증을 위해 사용되는 형태로, 확인모드는 일회용 비밀번호를 생성하고 응답모드는 거래화면에서 제시하는 질의(Challenge)값에 대한 응답(response)값을 생성하기 위해 이용한다. 서명모드는 거래금액, 수취인 계좌번호 등 거래정보를 입력하여 생성된 값을 거래화면에 다시 입력하는 방식으로 거래연동 인증을 위해 사용된다.

CAP 방식은 스마트카드와 CAP 단말기를 모두 소지하고 다녀야 하는 불편함이 있고, CAP을 이용한 인증 절차가 복잡하다는 단점이 있다. 하지만 스마트카드를 장착한 후 PIN값을 입력하여 이용하는 방식으로 지식기반, 소지기반의 다중 요소 인증을 지원함으로써 높은 보안성을 제공한다.

Secure Internet Banking Authentication(IEEE, 2006)에 따르면, CAP과 같이 신뢰된 플랫폼에서의 거래연동 인증기술이 모든 공격기법에 대응 가능한 인증기술로 평가되고 있다.



(그림 3) 공격에 대한 인증기술 안정성 분류

CAP 방식에서는 비밀정보 추측공격, Phishing공격에 의해 사용자의 비밀정보 유출이 불가능하고 공격에 의한 거래정보 위·변조에 대응 가능하므로 온/오프라인 공격

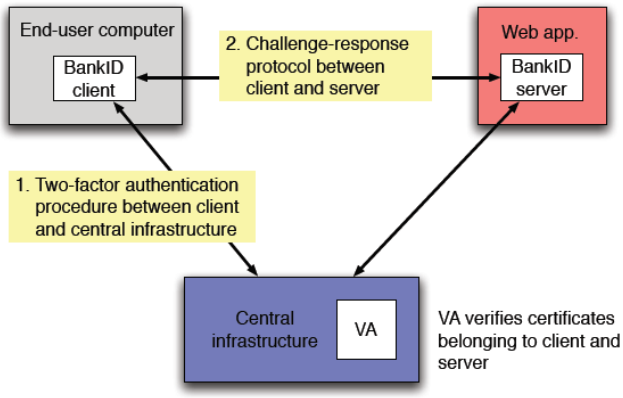
에 안전하다. 또한 MITB공격으로 부정거래가 발생하더라도 거래연동 인증으로 공격을 탐지하고 방어할 수 있다.

3.2 BankID

BankID는 노르웨이, 스위스, 덴마크 등 북유럽 국가 다수의 은행에서 사용하는 인증기술로 국내에서도 이용중인 PKI 기반 공인인증서의 변형된 형태의 인증기술이다. 2010년 말 기준으로 노르웨이에 약 270만 건이 발급되었으며 등록된 인구수도 240만 명에 달한다. 초창기에는 온라인뱅킹 이용자를 대상으로 인증기능을 제공하기 위해 개발되었으나, 현재는 은행업무 뿐만 아니라 의료, 공공기관 등 다양한 서비스 제공자를 대상으로 서비스하고 있다.

일반적인 PKI 기반의 인증서와 가장 큰 차이점은 인증서의 저장위치를 들 수 있는데, BankID의 경우 개인키를 중앙 기반시설에 저장하고 관리하는 것이 특징이다. 정상적으로 등록이 완료된 BankID 이용자는 BankID를 이용할 수 있는 사이트에 접속하여 자바 애플릿(Java applet) 형태로 내장되어 있는 BankID 클라이언트을 이용하게 되고, 이러한 클라이언트는 사용자 PC에 별도의 소프트웨어가 설치될 필요가 없으며 거래와 관련된 정보도 저장되지 않아 편의성과 보안성을 동시에 만족시킬 수 있다.

BankID의 인증과정은 2단계로 나누어지게 되는데, 1단계는 사용자의 개인키를 보관하고 전자서명을 수행하는 중앙서버 인증이며, 2단계는 실질적으로 서비스를 제공하는 웹 애플리케이션의 BankID서버와 사용자간의 인증으로 구분되어 진다. 1단계의 경우 사용자는 사회보장번호를 입력하고 하드웨어 OTP로 생성한 토큰을 이용하는 다중요소 인증방식을 취하고 있으며, 2단계의 경우 질의-응답 방식으로 본인을 확인하게 된다.((그림 4) 참조)



(그림 4) BankID의 인증절차

그러나 BankID는 다음과 같은 몇가지 문제점들이 제기되어 왔다. 첫 번째로 전자서명을 생성하는 주체가 사용자가 아닌 중앙서버이므로 전자서명의 당사자가 본인임을 증명할 수 있는 TTP(Trusted Third Party)가 존재해야 하지만 현재까지 따로 존재하지 않는 것과 두 번째로 BankID의 기술 및 운영 형태에 관한 정보가 비공개 상태로 운영된다는 점이다. 하지만 이러한 단점에도 불구하고 서명을 위한 개인키를 위탁 관리함에 따라 비교적 편의성이 뛰어나 사용자들이 선호하게 되었다. 최근에는 모바일에서도 이용 가능한 서비스가 제공됨에 따라 사용자의 편의성은 보다 증대될 것이다.

3.3 SMS OTP

SMS OTP는 온라인뱅킹을 위한 인증정보에 해당하는 비밀번호를 모바일기기에 SMS로 전송받으며, 해당 SMS에서 확인한 비밀번호를 온라인뱅킹 이용 시 입력하여 인증하는 방법이다. 스마트카드 리더기 OTP와는 다르게 단말기를 직접 조작할 필요 없이 수신한 SMS의 비밀번호를 거래화면에 입력하면 되므로 훨씬 간편하다.

소지기반의 SMS OTP인증기술은 지식기반의 ID/비밀번호와 함께 다중 요소 인증으로 많이 이용되고 있으며, 미국 Bank of America, 독일 Deutsche Bank, Postbank, 싱가포르 OCBC Bank, United Overseas Bank 등에서 많이 사용되고 있다.

(그림 5) 서비스 접속을 위한 SMS OTP

3.4 패드형 OTP

패드형 OTP는 토큰을 확인할 수 있는 디스플레이와 숫자를 입력할 수 있는 키패드로 구성된 OTP 장치를 말한다. 호주의 BOQ(Bank Of Queensland)를 비롯하여 다수의 국가에서 사용 중인 인증기술로서 키패드를 이용한 거래연동 인증이 가능한 것이 특징이다. 호주의 BOQ의 경우 (그림 6)과 같은 모양의 패드형 OTP를 이용한다.

(그림 6) 호주의 패드형 OTP

이러한 패드형 OTP는 토큰을 생성하기 위해서 사용자식별번호(PIN)를 입력해야하므로 다중 요소 인증방식으로 분류 된다. 사용자는 사용자식별번호 입력 후 두 가지 모드를 이용할 수 있다. 첫 번째 모드를 이용하게 되면 8비트의 일반적인 OTP 토큰이 생성되며, 두 번째 모드를 이용했을 경우에는 송/수신자 계좌번호, 거래금을 입력하여 해당 거래내역과 연계된 OTP 토큰을 생성함으로써 보다 향상된 보안성을 유지할 수 있다. 따라서 호주의 BOQ의 경우 25,000달러 이상의 금액을 거래이체 할 경우 두 번째 모드를 이용해야지만 거래가 가능하다.

3.5 주요 인증기술들에 대한 비교분석

본 절에서는 이상 살펴본 주요 인증기술들에 대한 적용성, 편의성, 보안성을 기준으로 <표 4>와 같이 비교분석하였다.

<표 4> 해외 인증기술들의 적용성, 편의성, 보안성 비교

구 분		CAP	BankID	SMS OTP	패드형 OTP	USIM OTP
적용성	가능	**상**	하	**상**	**상**	중
	적용비용	하	하	**상**	중	**상**
편의성	소지	하	**상**/하*	**상**	중	**상**
	사용	하	중	**상**	중	**상**
보안성	오프라인	**상**	**상**	**상**	**상**	**상**
	온라인	**상**	중	하	하	중
	거래조작	**상**	중	하	**상****/하	**상****/하

* BankID 사용 접근을 위해 부가적인 인증매체를 사용해야 하므로 소지의 불편함이 발생할 수 있음
** 거래연동 기술 도입시 거래조작 공격에 대응 가능

비교분석결과 적용성에서는 SMS OTP, 편의성에서는 SMS OTP 및 USIM OTP가 비교적 우수했으며, 보안성에 있어서는 CAP 방식이 가장 우수한 것으로 분석되었다.

4. 향후 전망 및 결론

스마트폰의 보급과 함께 앞으로 모바일뱅킹 서비스 이용률이 급격히 증가할 것이고, 이에 따라 모바일뱅킹 환경에서의 인증기술에 대한 연구가 보다 활발해 질 것이다. 뿐만 아니라 스마트폰 자체의 안전성이 보다 확보 된다면 스마트폰을 이용한 인증기술에 보다 관심이 집중 될 것이다. 최근 금융보안연구원에서 제안한 USIM 기반 모바일 OTP는 이러한 추세에 적합한 인증기술로서 추가적인 하드웨어 장치 없이 스마트폰의 USIM을 이용하여 사용자 편의성을 확보하면서 멀티채널 방식 및 거래연동 인증을 통해 보다 높은 보안성을 만족 시켜주고 있다. 또한 최근 국내에서도 도입된 사용자 편의성에 중점을 둔 그래픽 인증기술과 정맥 등의 바이오 정보를 이용한 인증기술도 향후 전망이 밝은 인증기술에 포함될 것이다.

대중화, 보편화되고 있는 지금의 전자금융환경에서는 보안성만을 강조하기 힘들게 되었다. 앞으로의 온라인뱅킹 인증에서는 모바일서비스의 확산을 대비하여 다양한 환경에 적용이 가능하고, 쉽고 편리하게 이용될 수 있는지에 대한 복합적인 검토가 필요하다. 본 논문에서 선진 인증기술을 검토해 본 결과, 적용성, 편의성, 보안성을 완벽하게 만족하는 인증기술은 찾을 수 없었으며, 각각의 장·단점을 활용하여 2가지 이상의 인증기술을 조합하여 사용하는 것이 효과적인 것으로 분석되어진다. 덧붙여 인증기술의 표준화를 통하여 인증기술의 개방성과 호환성이 확보된다면, 비용절감 효과와 보안성, 편의성이 증대될 것으로 전망된다. 이러한 변화를 바탕으로 편리하고 안전한 인증기술을 통해 전자금융거래 및 각종 온라인 서비스가 활성화되고 발전하기를 기대해본다.

참고문헌

[1] 2011년중 국내 온라인뱅킹서비스 이용현황, 한국은행 공보 2012-2-5호

[2] 전자금융 新인증기술 연구보고서, 금융보안연구원 2011.3

[3] 해외 온라인뱅킹 보안현황 조사 보고서, 금융보안연구원, 2010.2

[4] 이상민, 인증기술의 현황과 향후 전망, 금융결제원, 2011.10

[5] 유정각 외 1명, 인증기술의 현황과 향후 전망, 금융결제원, 2010.7

[6] Alain Hiltgen 외 2명, “Secure Internet Banking Authentication”, IEEE Security & Privacy, 2005.3

[7] Authentication in an Internet Banking Environment, FFIEC, 2005.10

[8] T.Weigold 외 1명, Secure Confirmation of Sensitive Transaction Data in Modern Internet Banking Services, IEEEInternet Security (WorldCIS), 2011

[9] Supplement to Authentication in an Internet Banking Environment, FFIEC 2011

[10] Hole, K.J 외 5명, Next generation internet banking in Norway, IEEE Security & Privacy, 2007

[11] Kristian Gjosteen, Weaknesses in BankID, a PKI-substitute Deployed by Norwegian Banks, 2008.6

[12] incsso.income.com.sg

[13] www.comscore.com

[14] www.comscoredatamine.com