情 報 保 護 學 會 誌
第 15 卷 第 4 號, 2005. 8

인터넷을 이용한 금융 거래 시 보안성 강화 수단에 관한 고찰

이 상 진*

요 약

최근 국내의 인터넷 뱅킹에 대한 해킹 사고를 계기로 시스템의 문제점을 진단하고 이에 따른 대응책을 기술한다. 이러한 시도는 특히 근간의 PKI 체계를 보완/강화하는 방향으로 진행하는 것이 바람직하다. 또한 인터넷 뱅킹의 궁극적은 안전성 보장을 위한 별도의 부가적인 보안장치의 특징과 장/단점을 소개함으로써 개인의 정보보호를 위한 대안을 제시한다.

Ⅰ. 도 입

지난 6월 3일, 외환은행 고객을 대상으로 한 해킹은 정부와 금융당국을 바짝 긴장시켰다. 왜냐하면 지난 1999년 공인인증기관이 설립된 후 대부분의 인터넷 뱅킹은 공인인증서 기반으로 진행함으로써 보안성이 충분히 담보되었다고 믿고 있었기 때문이다. 더욱이 고도화된 해킹 기법이 아니라 초보적인 수준의 키보드 모니터링을 통한 해킹이었기 때문에 놀라움은 더욱 클 수밖에 없었다.

금융당국은 이번 사건이 키보드 해킹으로부터 비롯되었으므로 모든 시중은행이 이에 대한 보안 소프트웨어를 설치할 것과, 휴대용 저장장치에 인증서 및 개인키를 저장할 것을 권고한 바 있다. 또한 인증서 재발급 시 재발급용 비밀번호나 SMS의 사용 등으로 본인인증을 강화하는 식으로, 직접적으로 문제가 발생한 부분에 대한 부분을 중심으로 처방을 내놓았다[1].

한편 정통부는 관계부처와 공동으로 Task Force를 구성, 인터넷 뱅킹 이외에 증권, 인터넷 쇼핑 등 전자거래 전반의 안전성 실태를 조사하고, 이 결과를 토대로 안전한 전자금융서비스 제공을 위한 정보보호 지침을 마련해 하반기부터 시행할 계획이다[2].

이번의 사고에서는 기존에 사용하던 인증서 및 개인키를 도용하지 않았으나 개연성이 충분히 존재하므로 보다 근본적인 대안을 마련하는 것이 사고의 재발을 막기 위해서도 절실히 필요하다. 특히 간과되지 말아야 하는 것은, 인터넷 뱅킹 자체를 위한 보안처방뿐만 아니라 일반적인 공인인증서 체계에 대한 정보보호라는 부분을 함께 해결해야 한다는 점이다. 즉, 효과적인 대안을 통하여 직접적으로 금융자산을 보호하는 것도 중요한 목적이지만, 개인의 프라이버시가 보호되고 있는지에 대하여 보다 포괄적인 해법이 필요하다.

Ⅱ. 현 황

온라인 금융거래량은 시간이 지나갈수록 증가세가 두드러진다. 한국은행의 발표에 의하면, 인터넷뱅킹은 전체 거래량의 30%에 달하며, 전체 금융거래 규모는 2005년 1/4분기 동안 2,200조원이 넘을 만큼 대단히 크다.

〔표 1〕 온라인 거래 유형별 규모[3]

온라인 거래 유형	2005년 1/4분기	2004년 4/4분기 비교
전자금융 거래대금	2292조 4190억원	3.2% 증가
자금이체	1296조원	3.7% 증가
전자자금이체 수수료 수익	1455억원	5.2% 감소
인터넷 보험계약	345억원	9.7% 증가
증권거래대금	919조원	3.1% 증가
증권거래 수수료	3277억원	58% 증가
신용카드 거래	17조원(4100만건)	5.2% 감소

본 논문은 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성지원사업의 연구 결과로 수행되었습니다.
* 고려대학교 정보보호대학원 부교수 (sangjin@korea.ac.kr)

〔표 2〕 인터넷 뱅킹의 규모[4]

범 주	내 용
등록 고객수	2290만명
공인인증서 발급건수(금융결제원)	740만개
하루 이용 건수(금액)	1042만건 (10조 831억원)
사용 장비	PC(97.5%), 모바일뱅킹(2.5%)
인터넷뱅킹 업무처리 비중(은행)	30.5%

한국은행에 따르면 인터넷뱅킹서비스를 이용하고 있는 고객 수는 20개 은행(8개 시중은행, 10개 지방 및 특수은행, 기타 2개 은행)에 대하여 2,290만 명에 달하며, 업무처리비중은 30.5%로서 이는 창구 직원을 통하여 거래되는 30.6%에 거의 육박한다. 특히 8개 시중은행의 경우에는 창구 직원을 통한 경우가 26.1%인데 반하여 인터넷뱅킹으로 34.0%가 금융거래를 한 것으로 밝혀짐에 따라 인터넷뱅킹은 단일방식으로 가장 많은 거래를 성사시키는 주요 수단이 되고 있다.

2.1 인터넷 뱅킹 시스템의 인증

일반적으로 사용되는 인증 메커니즘은 다음의 세 가지로 구분할 수 있다.

- □ 유형 1: 사용자가 알고 있는 정보(what you know) : 패스워드나 개인정보 등의 지식 정보
- □ 유형 2: 사용자가 갖고 있는 매체(what you have) : 열쇠, 토큰, 카드 등의 물리적 매체
- □ 유형 3: 사용자의 본질(what you are) : 지문, 홍채, 성문, 정맥 등의 사용자 신체상의 특성

한편, 현재 국내의 인터넷 뱅킹 시스템은 이중 유형 1의 반복적인 적용에 의존한다. 즉, 다양한 인증 메커니즘을 혼용하여 사용하기 보다는, 동일방식의 체계를 반복함으로써 소극적으로 인증을 강화하는 정도에 그친 것이다.

그림 1의 동작 과정 중 은행 입장에서 자금의 이체를 승인하는 결정적인 정보로 생각하는 것은 보안카드가 있으며, 은행별 통상 30여 개의 4자리수로 구성된 난수표를 사용하고 있다.

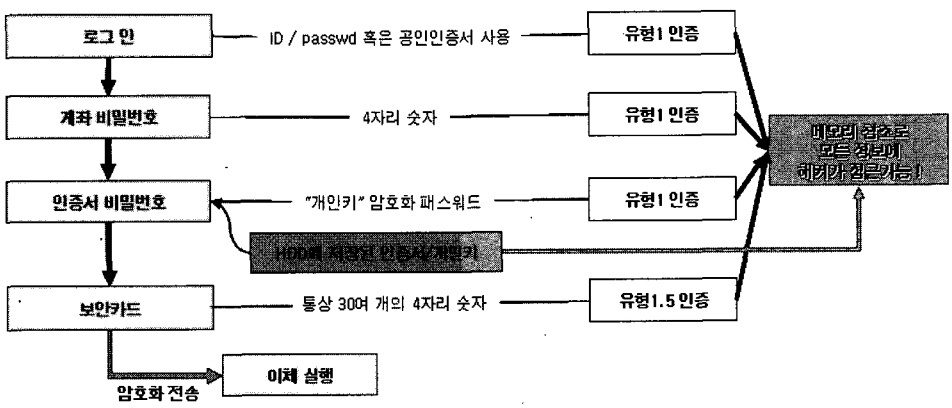
2.2 해킹 기법

해커는 전지전능하지 않다. 특별히 고도화되지 않은 대부분의 해커는 단순히 사용자의 컴퓨터 자원 정보를 모니터링하여 정보수집하고, 이를 분석하여 응용하는 방식을 따른다. 이는, 일반 유닉스나 리눅스의 경우와 달리, 윈도우 기반의 개인용 PC에는 telnet과 같은 원격접속을 통한 제어 기능이 보통 제공되지 않기 때문에 더욱 그렇다.

해커의 정보 모니터링 수단은 보통의 바이러스나 트로이 목마, 혹은 악성 프로그램을 위장하여 설치, 실행하게 한 후 각종 컴퓨터 자원 상에 출력되는 정보를 가로채는 방식으로 진행된다.

- □ 키보드 입력 정보 : NetDevil 등
- □ 통신망 전송 정보 : Sniffer 등
- □ 모니터 출력 정보 : BackOrifice, NetBus, SchoolBus, Serv7 등
- □ 메모리 내용 참조 : ArtMoney, TMK, T-Search, WPE, Cheat OMatic 등

이러한 해킹에 대비한 인터넷 뱅킹은 현재 대부분



〔그림 1〕 현행 인터넷 뱅킹의 인증체계

의 은행이 키보드 입력 정보를 보호하는 툴을 사용 중이다. 그러나 최근의 조사[5]에 따르면 단순 키보드 입력 모니터링 방지 솔루션만으로는 내부 메모리를 참조하는 경우 속수무책인 것이 밝혀졌다.

이 가운데 메모리를 참조하는 해킹은 매우 강력하므로 소프트웨어로 막을 수 없는 지경이다. 즉, 아무리 안전한 소프트웨어를 동작시켜 컨텐츠를 보호한다고 하더라도 어느 순간에는 평문(plaintext) 그대로가 메모리에 노출될 수 밖에 없기 때문에 이러한 공격을 제대로 방어하려면 소프트웨어가 아닌 별도의 장치를 사용하는 것이 효과적일 수 밖에 없다.

Ⅲ. 대 안

3.1 이중인증

이중인증이란 대표적으로 3가지 인증 메커니즘 중 어느 두 가지를 선택적으로 적용한 경우의 시스템을 말한다. 즉 사용자 암호와 물리적 매체를 결부시켜 인증체계를 강화할 수도 있고, 또 생체정보와도 결합할 수 있다. 이중인증 방식이 안전한 이유는 전혀 이질적인 방식이 사용됨으로써 어느 한 가지 유형에 대한 공격보다 훨씬 어렵게 되기 때문이다.

시중에는 이중인증을 지원하는 다양한 매체가 출시되어 있고, 대부분 유형 1과 유형 2의 인증기법을 결합한 것이다. 이런 장치를 도입하기 위해서는 보안성, 구현의 편의성, 사용자 편의성, 이동성 및 호환성 등의 다양한 기준에 따라 용도에 맞게 선택적으로 적용하는 것이 바람직하다.

〔표 3〕 다양한 인증 지원 방식 및 장치

제품군	내 용
ID / password	대표적인 현행 인증방식
스마트카드	단순 저장형과 프로세서형으로 구분됨
USB 인증토큰	
지문인식기	단순 센서형이 일반적이다.
OTP	일회용 난수 생성기능 제공

3.2 개인용 보안장치

정통부는 최근의 인터넷뱅킹 사고를 계기로 한국정보보호진흥원(KISA) 및 유관기관과 전담팀을 구성하여 효과적인 대응방안을 모색하고 있다. 특히 정통부의 시각은 이번의 사고가 현존하는 사용자의 개인키 정보를 해킹하여 범죄가 발생하지는 않았으나, 사고의 개연성을 놓고 볼 때 충분히 그런 방식으로 확장될 수 있음을 고려하여, 근본적인 대책을 수립하고자 노력하고 있다.[6]

따라서 이중인증 체계를 도입할 것과 기존의 PKI 체계를 유지/강화하는 방안으로 개인용 보안장치(HSM, HardWare Security Module) 사용을 검토하고 있다. 특히 주목해야 할 점은 기존의 단순 정보 저장 장치나 다른 방식의 인증장치와는 달리 보다 근본적인 보안성을 담보할 수 있는 매개체 사용을 권고하는 것이다. 이러한 개인용 보안장치의 필요조건은 다음과 같다.

□ 자체적으로 안전한 메모리 영역을 확보할 것
- 내부에 저장되어 있는 키나 기타 중요정보를 열람할 수 없는 안전한 구조이어야 한다.

□ PKI 암호 처리(특히 개인키를 이용한 전자서명)는 토큰 내부에서 실행할 것
- 토큰 자체적으로 공개키를 처리할 수 있는 프로세서가 탑재되어 있어야 하며, 따라서 데스크톱 컴퓨터와는 별도로 자체적인 암호처리가 가능하여야 한다.

□ 표준 인터페이스를 준용할 것
- 보안장비의 표준 인터페이스인 PKCS#11은 기본적으로 만족시켜야 하며, 부가적으로 Microsoft Crypto-API를 지원하여야 한다.

이러한 요구조건을 만족하는 보안장치는 사실상 (프로세서형) 스마트카드나 (프로세서형) USB 토큰 밖에 없다. 따라서 한국정보보호진흥원은 현재 국내에서 시판중인 몇 가지 제품을 리뷰하여 그 결과를 정리하였다.

프로세서형 보안토큰은 스마트카드나 USB 인증토큰 모두 동일한 수준의 보안성이 있다. 왜냐하면 USB 인증토큰의 코어 알고리즘 모듈은 대체로 스마트카드를 그대로 사용하기 때문이다. 스마트카드는 매우 얇으

〔표 4〕 다양한 인증 지원 방식 및 장치(KISA)

타입	업체	알고리즘
스마트카드	LG 히다찌	RSA, SHA-1, (3)DES, MD5
	삼성 SDS	
	SCT	
USB 인증토큰	SCT	
	Rainbow	
	XiLogics	

면서 휴대하기 편하지만, 리더기를 갖고 다녀야 하는 문제로 인해 사용자 편의성이나 이동성에 심각한 제한이 있다. 또한 카드 자체의 안전성은 좋으나 리더기의 가격이 비싸고 유지보수 사례가 잦은 단점이 있다.

반면 USB 인증토큰은 스마트카드의 장점을 수용하면서 어디에나 존재하는 USB 인터페이스를 사용하므로 추가적인 비용이나 번거로움을 해소한 특징이 있다.

3.3 해외 사례

미연방 예금보험위원회(FDIC, Federal Deposit Insurance Corporation)에서는 금융기관 계정에 대한 불법적인 해킹시도에 대한 위험을 감소시키는 방안을 찾기 위하여 보고서를 발표하였다.[7] 미연방 통상위원회(FTC, Federal Trade Commission)에 따르면 2003년도에 미국에서의 계정절취(identity theft) 사고는 1천만 건, 이로 인한 비즈니스 및 소비자의 피해액은 500억 달러에 이른다고 보고하였다. 이런 종류의 사고는 매우 빠른 속도로 증가하는 추세에 있으며 특히 피싱(phishing)이나 기타 해킹 기법으로부터 비롯된다.

이에 따라 온라인상의 계정절취 문제를 해소하기 위하여 다음과 같은 대안을 제시하였다.

1. 기존의 고객에 대한 단일인증 체계를 이중인증 방식으로 업그레이드 할 것
2. 취약점 탐지 소프트웨어를 사용하여 위협 요소를 점검할 것
3. 피싱과 같은 온라인 사기 피해를 당하지 않도록 사용자 교육 프로그램을 강화할 것
4. 금융 서비스회사, 정부 및 관련업체와의 정보공유를 지속적으로 유지할 것

그 결과 금융기관과 거래하는 각 사용자에게 안전한 이중인증 토큰 사용을 권고하기 위하여 몇 가지 항목으로 다양한 제품군을 평가하였다. 표 5에서 금융기관은 구현 편의성과 보안성이 주관심사인데 반해, 사용자/소비자는 이동성, 보안성 및 사용자 편의성이 주관심사이다.

3.4 개인 정보보호

본 논의의 연장선상에서 중요하게 고려해야 할 대목은 개인의 정보를 어느 정도까지 보호할 것인가 하는 점이다. 즉, 현재의 사건은 개인의 금융, 그 중에서도 직접적으로 현금을 이체할 수 없는 부분에만 초점이 맞춰져 있다. 그러나 최근의 사고에서 볼 수 있었던 바와 같이 일반적인 해킹 기술을 통하여 개인키 및 이를 암호화한 패스워드 역시 손쉽게 해킹당할 수 있다. 즉, 2000년 이후의 공인인증서 기반 체계는 윈도우 환경의 경우 일괄적으로 c:\program files\npki 폴더 밑에 인증서와 개인키 정보를 파일로 저장하고 있다. 이때 개인의 인감과 법적으로 동일한 효력을 갖는 개인키가 노출될 경우의 파장이란 대단할 수밖에 없을 것이다.

또한, 인터넷 뱅킹을 다른 각도에서 본다면 메모리 해킹을 통하여 아이디/패스워드나 혹은 공인인증서 로그인 정보를 모두 가로챌 수 있다. 이런 정보를 토대로 해커는 개인의 주민번호, 계좌번호, 잔액 등을 매우 손쉽게 조회할 수 있음은 물론, 여기서 그치지 않고 제3의 범죄를 촉발할 수 있는 매우 취약한 환경에 처한 것이다.

따라서 스마트카드나 혹은 안전도가 이와 동등한 USB 토큰과 같은 강력한 개인정보 보호 매체를 적극 사용하여야 하며, 이러한 매체 내부에서만 개인키를 저장하고 모든 암호 인증 과정을 수행하게 하는 것이 현재의 해킹 사고를 방지하는 대책이라 할 수 있다. 주의해야 할 점은 로그인이나 기타 중요한 사용자 인증/보안 처리 프로세싱을 데스크톱과는 독립적으로 수행해야 한다는 것이다.

Ⅳ. 맺음말

현재 금융당국은 물론 정부에서도 문제의 본질을

〔표 5〕 다양한 인증 지원 방식 및 장치 (FDIC)

인증방식	구현 편의성	이동성	보안성	사용자 편의성	기타
ID/password	쉬움	좋음	중간	좋음	Man-in-the-middle-attack 가능
USB 인증토큰	쉬움	좋음	높음	좋음	피싱 및 해킹 취약성 없음
스마트 카드	중간	나쁨	높음	좋음	카드 리더 설치/보유의 어려움
OTP	나쁨	좋음	높음	좋음	OTP 인증서버 설치
지문인식	중간	나쁨	높음	좋음	가격이 비쌈

파악한 후, 대안을 찾기 위하여 노력하고 있다. 대체로 정통부는 최근 사안의 직접적인 문제뿐만 아니라 유사한 사고의 재발을 막기 위하여 개인별 보안장치를 도입할 것을 검토하고 있다. 이러한 대안은 근본적으로 PKI 체계를 유지/강화하는 방식으로 진행되고 있으며 이러한 흐름은 문제를 근본적으로 해결하는데 매우 큰 의미가 있다 하겠다.

반면 금융당국에서는 사고가 난 바로 그 지점에 대한 임기응변식의 대응에 치중하고 있으므로 향후 예산의 중복투자 뿐만 아니라 예상되는 해킹에 대한 적절한 대안으로는 다소 부족하다는 느낌을 지울 수 없다. 즉, 최근의 사고 자체를 효과적으로 막기 위해서는 One Time Password(OTP)의 도입만으로 충분한 것으로 판단하는 것 같다.

그러나 OTP 제품군의 특성상 표준이 없으므로 다수의 은행, 증권사, 보험사 및 신용카드사를 이용하는 소비자 입장에서는 1인당 여러 개의 다양한 OTP를 보유하는 번거로움을 감수해야 한다. 더구나 무엇보다 이런 대안의 문제점으로 지적되는 것은 OTP 시스템이 그 고유의 장점에도 불구하고 현행 공인인증체계를 유지/강화하는 것과는 거리가 멀다는 점이다.

최근의 인터넷 뱅킹 사고가 촉발시킨 개인인증수단의 효율적인 업그레이드라는 과제는 국내정보보호 체계를 한단계 진일보시킬 것은 분명하다. 더욱이 포괄적인 개인 정보보호를 달성하기 위하여 개인키를 안전한 토큰 내부에서만 관리하게 하는 방안은 이제 세계적으로 모범이 된 인터넷 강국, 그 중에서도 강력한 PKI 인증체계를 지원하는 대한민국의 또 다른 정보보호의 모범사례로 제시될 수 있을 것이다.

참 고 문 헌

[1] 임윤규, "공인인증서 재발급 까다로와진다", *디지털타임즈*,, 6월29일자, 2005

[2] 이구순, "정부, 전자금융거래 안전성 전면 실태조사 나서기로", *아이뉴스24*, 6월10일자, 2005

[3] "인터넷뱅킹 해킹방지 대책 추진", *시민일보*, 6월27일자, 2005

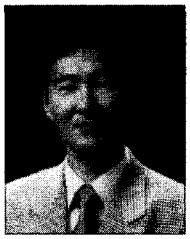
[4] "2005.6월말 현재 국내 인터넷뱅킹서비스 이용현황", *한국은행*, 7월28일자, 2005

[5] "뻥뻥 뚫린 인터넷뱅킹", *시사매거진 2580*, 문화방송, 6월19일, 2005

[6] "HSM 장비 도입 시 문제점 및 고려사항", *한국정보보호진흥원*, 6월29일, 2005

[7] "Putting an End to Account-Hijacking Identity Theft", *FDIC*, Dec. 14, 2004

〈著 者 紹 介〉



이 상 진 (Samgjin Lee)
종신회원

1987년 2월 : 고려대학교 수학과 학사
1989년 2월 : 고려대학교 수학과 석사
1994년 2월 : 고려대학교 수학과 박사
1989년 2월~1999년 2월 : 한국전자통신연구원 선임연구원,
1999년 2월~현재 : 고려대학교 정보보호대학원 부교수
〈관심분야〉 대칭키 암호, 정보은닉, 컴퓨터 포렌식