한국산학기술학회논문지
Vol. 10, No. 8, pp. 1920-1925, 2009

전자금융거래의 안전성 강화를 위한 종단간 암호화

성재모[1], 이수미[2*], 안승호[3], 노봉남[3]
[1]전남대학교 정보보호협동과정, [2]금융보안연구원, [3]전남대학교 시스템보안연구센터

The End-to-End Encryption for Enhancing Safety of Electronic Financial Transactions

Jae-Mo Seung[1], Su-Mi Lee[2*], Seung-Ho Ahn[3] and Bong-Nam Noh[3]
[1]**Interdisciplinary Program of Information Security, Chonnam National University**
[2]**Financial Security Agency**
[3]**System Security Research Center, Chonnam National University**

요 약 '05. 6월 인터넷 뱅킹으로 인한 최초 사고는 전자금융거래 보호를 위한 보안프로그램 기능을 중지하고, 이용자가 입력한 주요 금융거래정보 즉 공인인증서 비밀번호, 계좌비밀번호, 보안카드 비밀번호 등을 수집하여 이를 전자금융거래에 사용하였다. 이처럼 백신 프로그램이나 개인 방화벽과 같은 보안프로그램의 기능을 우회하는 해킹 툴에 의해 금융정보를 갈취하는 행위는 계속해서 시도되고 있다. 따라서 전자금융거래에 있어 이용자 단말기에서부터 금융기관의 금융거래서버까지 이용자가 입력한 금융거래정보를 안전하게 보호하는 것을 목적으로 전자금융시스템을 구성해야 한다. 본 논문에서는 전자금융거래에서 발생된 위협에 대해 원인을 분석하고, 이를 기반으로 현 전자금융거래인 인터넷뱅킹, 금융자동화기기, 모바일뱅킹에서 보안성 향상을 위해 고려해야 할 보안사항에 대해 기술한다.

Abstract `05. June, the first Internet banking accident occurred by the malignant cord. It discontinued security programs for protecting important financial informations. A computer hacker had made a collation of password, OTP(One Time Password) values etc and illegally withdraw one´s savings from the bank using the financial information. The attackers are continuously attempted with the hacking tool under bypass security programs as the vaccine program or the personal fire-wall. Therefore, an electronic financial system should be composed with the goal which is to protect financial informations from user's terminal to a banking server. In this paper, we make an analysis of menaces in electronic financial transactions and explain considerable security issues to enhance safety in Internet banking, CD/ATM and mobile banking.

Key Words : Internet Banking, CD/ATM, Mobile Banking, Financial Information, End-to-End Encryption

1. 서론

최근에는 인터넷 뱅킹, 사이버 증권 거래 시스템, 모바일 뱅킹 등의 사용 증가로 인해 이용자의 주요 정보가 유출되어 피해를 입는 경우가 증가하고 있고, 고의적으로 타인의 정보를 알아내어 금융범죄에 이용하거나 사이버 상에 있는 타인의 자산을 훔치는 것과 같은 범죄가 갈수록 지능적이고 대담하게 이루어지고 있다. 이용자 단말기에는 중요한 정보를 각종 해킹의 위협으로부터 보호하기 위해 보안프로그램이 설치되고, 이를 통해 외부 침입을 감지하여 각종 개인정보의 무단 유출 및 데이터 손상의 위협을 사전에 차단하는 역할을 수행한다. 하지만 보안프로그램에 의해 보호받지 못한 구간에서 이용자의 금융거래정보 유출 사고가 발생하였다. 따라서 다양한 해킹기술을 방지하기 위한 여러 대응기술이 이용자의 금융거래정보를 보호하기 위해 개발되고 있다. 그 중 하나로 종단간 암호화(End-to-End Encryption)를 고려해 볼 수 있다. 종단간 암호화는 이용자 단말기에서 금융거래정보를 입력하는 이벤트가 발생하는 순간부터 암호화를 수행하고 금융거래서버까지 전 구간에서 금융거래정보를 암호화된

*교신저자 : 이수미(smlee@fsa.or.kr)
접수일 09년 07월 01일 수정일 (1차 09년 07월 20일, 2차 09년 08월 18일) 게재확정일 09년 08월 19일

데이터 형태로 유지하여 전송되므로 해킹으로부터 보호할 수 있는 기법을 말한다. 결국 종단간 암호화를 통해 이용자의 금융거래정보는 네트워크 영역뿐만 아니라 단말기 내부에서도 어떠한 형태로든 평문으로 존재하지 않아 암호키를 공유한 금융거래서버만이 금융거래정보를 확인할 수 있다. 본 논문에서는 전자금융거래에서 발생된 보안사고 사례를 살펴보고, 사고 원인을 분석하여 전자금융거래의 보안성 향상을 위해 고려해야할 사항에 대해 살펴본다.

2. 전자금융거래 이용현황

2009년 4월 29일 한국은행에서 발표한 '2009년 1/4분기 국내 인터넷 뱅킹 서비스 이용현황'[5]에 따르면 2009년 3월말 현재 금융결제원의 인터넷 뱅킹용 공인인증서 발급수는 1,430만개로 전년말 대비 11.1% 증가했다. 19개 금융기관에 등록된 인터넷 뱅킹 고객수는 중복을 포함하여 합산했을 때, 5,496만명으로 전년말 대비 4.5% 증가하였으며, 이중 개인과 기업은 각각 2008년말 대비 4.5%와 3.7%가 증가하였다.

[표 1] 금융기관 인터넷 뱅킹 등록 고객수[1)]

(단위 : 천명, 천개社, %)

	2007 12월말	2008				2009. 3월말
		3월말	6월말	9월말	12월말	
개 인	42,396 (5.3)	44,564 (5.1)	46,239 (3.8)	48,113 (4.1)	49,912 (3.7)	52,181 (4.5)
기 업	2,302 (6.0)	2,378 (3.3)	2,482 (4.4)	2,584 (4.1)	2,683 (3.8)	2,781 (3.7)
합 계	44,698 (5.3)	46,942 (5.0)	48,721 (3.8)	50,697 (4.1)	52,595 (3.7)	54,962 (4.5)

주 : 1) ( ) 내는 전분기말 대비 증감률

2009년 3월 중 금융서비스의 전달채널별 업무처리비중(건수 기준)은 전체 입출금거래 기준으로 비대면 거래 비중이 85.3%이며 그 중 인터넷 뱅킹이 32.9%를 차지했고, 조회서비스 거래 기준으로는 비대면 거래 비중이 79.3%이며, 그 중 인터넷뱅킹이 60.5%로 가장 높은 비중을 나타내었다. 2009년 1/4분기의 전체 인터넷뱅킹 이용건수 (일평균 기준)은 2,641만건으로 전분기 대비 9.9% 증가한 것으로 나타났으며, 그 중 인터넷뱅킹 이체 건수는 421만건으로 전분기에 비해 건수는 18.9% 증가하였다.

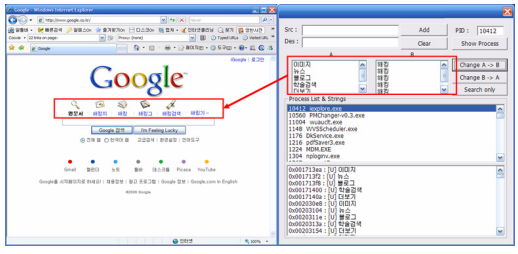
[표 2] 2009년 3월중 금융서비스의 전달채널별 업무처리 비중(건수 기준)

구 분	대면거래 (창구거래)	비 대 면 거 래				합 계
		CD/ATM	텔레뱅킹	인터넷뱅킹		
입출금거래 건수기준	14.7	39.2	13.2	32.9	85.3	100.0
조회건수	20.7	9.3	9.5	60.5	79.3	100.0

3. 전자금융거래 보안사고 사례 및 원인 분석

3.1 인터넷 뱅킹

인터넷 뱅킹에서 최근 이슈가 되고 있는 위협은 메모리 해킹이다. 이는 주기억장치에 저장되는 데이터를 절취하거나 이를 조작하는 해킹 기법을 말한다. 기존에 메일이나 전화 등 외부수단을 이용해 사용자의 계좌번호와 계좌 비밀번호 등의 금융거래정보를 절취하는 것과 달리 PC 해킹을 통해 백도어 프로그램을 설치한 뒤 전용 툴을 통해 메모리 상의 데이터를 절취하고 변조한다는 점에서 그 차이가 있다. '07. 8월 공론화된 보안위협으로써 주로 온라인 게임 어플리케이션을 해킹하기 위해 주로 사용되었던 기법이다. 웹브라우저(IE) 내로 유입된 정보에 대한 위·변조를 감지하는 보안모듈 또는 절차가 존재하지 않음으로 이용자가 웹브라우저의 입력 필드에 데이터를 기록하는 순간 그림 1과 같이 웹브라우저 메모리의 해당 영역에 존재하는 금융거래정보를 절취 및 변조할 수 있는 위협이 존재하는 것이다.



[그림 1] 웹브라우저(IE) 메모리공간내의 문자열 검색 및 변경

이러한 메모리 해킹을 통한 인터넷 뱅킹의 실질적인 피해는 아직 보고된 바가 없지만 메모리 해킹은 실제 가능하며, 메모리 해킹 방식이 범죄에 악용될 경우 인터넷 뱅킹을 운영하고 있는 금융기관의 신뢰성과 안정성에 큰 위협이 된다는 점에서 최근 금융권과 정보보호업계에서

이슈로 떠오르고 있다. 해커들이 대규모 조직을 구성되어 메모리 해킹을 통해 인터넷 뱅킹을 수행하는 PC들을 집중 모니터링하여 미리 개설해 놓은 여러 대포통장의 계좌들로 이체 자금들을 빼돌리는 방식으로 범죄에 악용할 수는 있는 가능성을 갖고 있다.

3.2 금융자동화기기

국내의 금융자동화기기은 대부분 은행들이 직접 운영하고 있으나 부가가치통신망 사업자로 통신사업자(KT 등)로 부터 통신회선을 임대하여 다양한 정보처리 서비스를 제공하는 사업자인 VAN(Value Added Network)에 의해 전체 금융자동화기기의 약 16%는 운영되고, VAN 사업자들이 운영하는 수량의 약 13.8%는 VAN사업자가 금융자동화기기를 개인에게 판매하고 소유주인 개인(점주)이 현금충전, 장애관리 등의 업무를 수행하는 형태인 점주 운영방식으로 운영되고 있다. 은행들이 직접 설치하는 경우에는 자체 영업점이나 특별한 안전장치를 갖춘 365코너 등에 설치하고 있어 복제기를 설치하기가 어렵기 때문에 사고 위험성이 상대적으로 낮다. 그러나 VAN 사업자들이 설치하는 자동화기기는 지하철역이나 옥외의 장소 또는 개인 영업점에 설치하고 있어 누군가가 자동화기기에 접근하는 것을 통제하는데 어려움이 있다. 바로 이러한 자동화기기에서 카드 정보 유출 사고가 발생하는 것이다. 자동화기기를 이용한 사고 유형은 신용카드 소지자가 결제 시 직접 리더기에 읽히는 것을 확인하지 않는 주유소, 술집 등에서 개인 복제기를 이용하거나 택배 회사 직원이 개인 복제기를 이용하여 복제하는 수법이 있다. 이와 유사한 사례로 카드가 들어가는 슬롯 위에 스키밍 장치를 제작하여 설치한 후 이용자의 카드정보를 습득하는 사고가 발생했다. 동 방법은 미국의 Los Angeles에서 처음 등장하였고, 국내에서도 비밀번호를 알아내기 위해 몰래 카메라를 설치한 경우가 2003년 광주지역에서 발생했다. 또한 최근 2008년 3월 국내 5개 은행에서 도용된 신용카드에 의해 현금이 인출되는 사고가 발생했다. 원인분석 결과 5개의 카드가 모두 서울 모처에 설치된 자동화기기를 이용한 사실이 확인되었다. 이후 자동화기기를 해체한 결과 노트북이 설치되어 있었고, 천정에는 카메라가 설치되어 있었다. 또한 동 노트북에서는 560여명의 신용카드 정보가 저장되어 있어 감독당국은 해당 은행에 사실을 통보하여 거래를 정지하고 본인에게 통보하여 재발급을 받도록 조치하였다.

3.3 모바일 뱅킹

VM(Virtual Machine) 모바일 뱅킹은 별도의 금융IC칩을 내장하지 않은 휴대폰으로도 모바일 뱅킹을 할 수 있는 서비스이다. 전용 폰이 아니더라도 대부분 기종의 휴대폰으로 은행거래를 이용할 수 있는 것이다. 그동안 모바일 뱅킹은 특정 금융IC칩을 장착한 휴대폰에서만 사용이 가능했기 때문에 은행마다 별도로 발급하는 금융칩을 휴대폰에 삽입해야 했다. 만일 이동통신가입자가 고객사를 바꿀 경우 모바일뱅킹을 위해서는 금융칩을 새로 발급받아야 하는 불편함이었으나 VM모바일 뱅킹은 휴대폰으로 해당 프로그램을 내려 받기만 하면 대부분 기종의 휴대폰으로 은행거래를 할 수 있게 되었다. 이러한 이유로 VM모바일 뱅킹 서비스는 이용자의 편의성을 인정받아 이용자 가입 건이 증가하고 있는 추세이다. 하지만 VM모바일 뱅킹의 보안 취약점을 조사한 결과, VM모바일 뱅킹 거래 시 유효기간이 만료된 서버인증서를 사용하더라도 VM모바일 뱅킹 거래가 정상적으로 동작한 것으로 VM뱅킹 프로그램이 서버에 대한 인증을 하지 않거나 오작동되는 것으로 확인됐다. 또한 휴대폰을 이용하여 결제서비스를 이행한 후 인터넷 상에서 쉽게 구할 수 있는 암호 해독 프로그램에 연결시켜 1분 내에 비밀번호 6자리가 드러나는 사건도 있었다. 이 방법은 휴대폰에 남겨진 로그를 분석하여 똑같은 숫자들 사이에 나타나는 상이한 숫자들을 모으면 PIN(Personal Identification Number)이 되는 것으로 나타났다. 그 결과 금융권에서는 PIN을 비롯한 금융거래정보에 대한 검증절차를 수정하고 보강한 것으로 알려졌다.

3.4 전자금융사고 원인분석

전자금융거래에 대한 보안사고 영역은 단말기로부터 금융기관 서버까지 주요 금융거래정보가 입력되고, 전송되는 전 구간이 그 대상이 됨을 살펴볼 수 있다. 전자금융거래에서 발생한 보안사고의 주요 원인으로는 발생 구간에서 주요 금융거래정보에 대해 암호화를 제공하지 않거나 금융거래서버에 대한 정상적인 인증을 수행하지 않아 발생됨을 살펴볼 수 있다. 즉 인터넷 뱅킹에서는 키보드 입력으로부터 암호화 모듈까지 금융거래정보가 평문으로 존재함으로써 키로깅, IE후킹, 메모리 변조 등에 의해 주요 금융거래정보가 유출되거나 변조되고, 모바일뱅킹 사고 역시 PIN 및 금융거래정보가 단말기 내에 평문으로 존재하여 발생된 사고임을 볼 수 있다. 금융자동화기기 경우는 카드 리더기로부터 본체 구간까지 금융거래정보가 평문으로 전송되어, 이 구간에서 탭핑 도구로 주요 금융거래정보를 유출하고, 이로부터 현금카드를 만드는 카드 복제사고가 발생한 것이다. 살펴본 바와 같이 금융정보에 대한 유출 사고는 정해진 구간에서 발생되는 것은 아니다. 금융거래정보가 전송되는 전 구간은 해커의

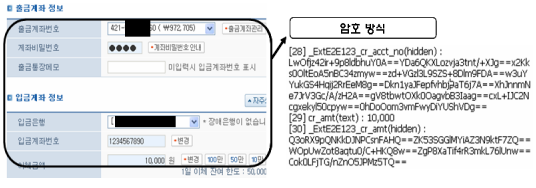
표적이 될 수 있고, 이에 따라 적절한 암호화를 통해 기본적으로 주요 금융정보에 대해 보호가 이루어져야 할 것이다. 전자금융거래에 있어 이용자 단말기에서부터 금융기관 전자금융거래시스템까지 입력된 금융거래정보를 안전하게 보호하는 것을 목적으로 전자금융시스템을 구성해야 한다.

4. 전자금융 거래정보 보호를 위한 종단간 암호화

본 4장에서는 3장에서 분석된 사고원인을 기반으로 안전한 전자금융거래를 위해 적용 가능한 종단간 암호화 방식에 대해 살펴본다.

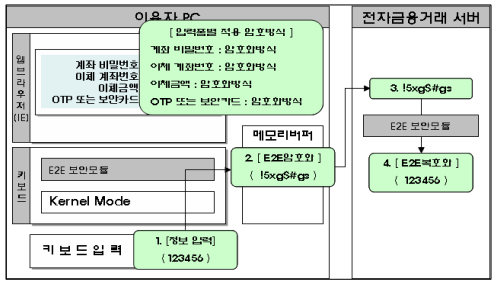
4.1 인터넷 뱅킹

인터넷 뱅킹에서 주요 금융거래정보에 대한 암호화를 적용하는 방식에는 주요 금융거래정보를 치환테이블에 의해 치환하는 방식과 암호화 키로 인한 암호화 방식으로 나눌 수 있다. 각 금융기관에 적용된 방식은 두 가지 방식이 혼용되어 계좌비밀번호, OTP, 보안카드 등에 치환방식이 적용되고, 이외 이체계좌번호, 이체금액에는 암호화방식이 적용된 혼합형태와 단지 암호화만을 적용한 단일형태로 존재한다. 인터넷 뱅킹에서 이용자 PC에서 설치된 키보드보안프로그램과 암호화프로그램의 연동[1]에 의해 키 이벤트가 발생될 때 마다 키 값을 암호화하는 형태다. 하지만 “종단간(E2E) 암호화 적용 가이드”[3]에서 기술된 것과 같이 암호화된 계좌 비밀번호를 PKI 보안프로그램에 적용되기 전에 복호화하는 방식으로 이용자 PC내에서 평문으로 존재하는 구간이 발생되어 문제점으로 지적되고 있다. 키보드보안프로그램과 금융거래서버로 설정되지 않아 발생된 문제이다. 이와 같이 종단간 암호화를 수행하지 않았을 때 취약한 구간이 존재하게 된다. 따라서 기본적으로 종단간 암호화를 수행하면서 메모리 해킹에 의한 변조까지 방지할 수 있는 기술에 대해 살펴본다. 본 논문에서는 암호화만을 적용한 단일방식에 대해서 기술한다.



[그림 2] 입력필드별 적용된 종단간 암호화

우선 종단간 암호화는 키보드 입력에 의해 이벤트가 발생된 필드에 적용이 된다. 이와 같은 필드 중 주요 금융거래정보인 계좌비밀번호, OTP 또는 보안카드에 종단간 암호화가 적용되어 계좌비밀번호 등에 대해 기밀성[4]이 제공되었고, 그 이후 메모리 해킹과 같이 입금계좌번호, 이체금액에 대한 변조에 의해 발생될 수 있는 위협을 방지하고자 암호화를 통해 데이터에 대한 무결성을 제공한다. 종단간 암호화를 적용하기 위해 PKI 보안프로그램 이외의 별도 암호모듈(E2E암호모듈)이 필요하다. 이때 암호화 키 공유 대상은 키보드보안프로그램과 금융거래서버가 되므로 E2E암호모듈은 이용자 PC에 설치되며, E2E복호모듈은 금융거래서버에 설치되어 종단간 암호화를 수행해야 한다. 다음은 종단간 암호화에 대한 개략적인 절차이다.



[그림 3] 종단간(E2E)암호화 절차

① 사전에 전자금융거래에 필요한 일련의 절차가 모두 완료 가정 하에 이용자는 키보드 장치를 통해 계좌비밀번호 및 계좌번호 등 금융거래정보를 입력

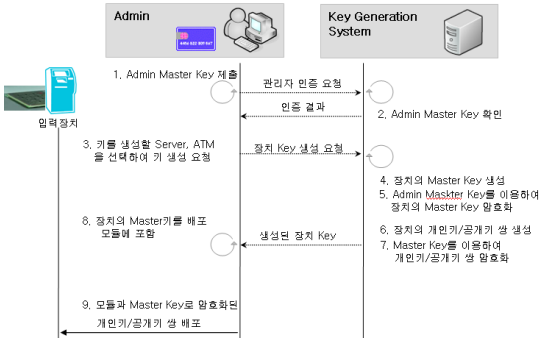
②③ 키보드 장치로부터 유입된 금융거래정보를 E2E 암호모듈에서 암호화하며, 암호화된 값은 웹브라우저(IE)의 html가 아닌 별도 메모리버퍼에 저장한 후 입력이 완료되면 이를 PKI암호프로그램에 의해 이중암호화가 수행되고 전자금융거래 서버로 전송

④ 전자금융거래 서버로 유입된 암호 데이터는PKI복호프로그램에의 복호화되며, 이를 E2E복호모듈에 의해 재복호화 수행

4.2 금융자동화기기

현재까지 금융자동화기기에서 네트워크로 전송되는 정보는 암호화를 통해 기밀성이 제공되고 있었으나, 금융자동화기기 내부에서 전송되는 정보에 대해서 보안이 미흡하다. 즉 카드 리더기와 본체사이에서 평문으로 전송되는 금융거래정보를 유출시킨 사고로부터 살펴볼 수 있다. 이와 같은 사고의 원인 또한 금융자동화기기 내부 통신

에 대해 기밀성을 제공하지 않았기 때문이다. 현재 본체와 금융거래서버 또는 VAN사 간에 암호화 키 교환과정 이후 공유된 암호화 키로 금융거래정보를 암호화하고 있다. 이에 추가적으로 카드 리더기 내부에도 암호모듈을 탑재하여 카드 데이터 읽힘 현상이 발생할 때 마다 카드 리더기에서 암호화하는 과정을 수행해야 한다. 그 결과 카드 리더기와 본체사이에 전문장비로 인한 탭핑이 발생해도 암호화된 데이터를 수집하게 될 것이다. 보안수준을 강화하기 위해서 카드 리더기와 금융거래서버 또는 VAN사 간에 암호화 키 교환 과정을 세션이 발생할 때 마다 수행되어야 하나, 현재 금융자동화기기 서비스 형태를 유지하면서 금융자동화기기 내부에서의 금융거래정보에 대한 기밀성을 제공하는 방식을 우선적으로 제공해야 할 것이다. 따라서 암호화 과정을 수행하기 위해 카드 리더기와 본체 간에는 암호화 키 교환과정이 수행되어야 한다. 암호화 키 공유과정은 다양한 방식이 존재할 수 있다. 그 예로 그림 4에 대해 주요설명은 다음과 같다.



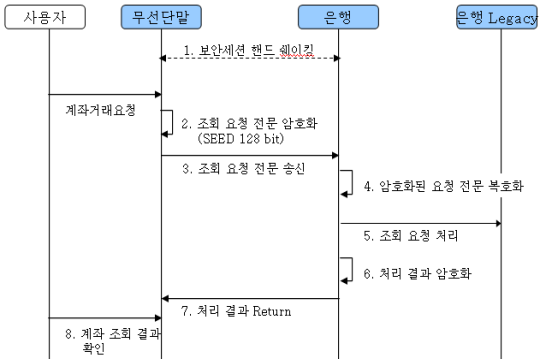
[그림 4] 금융자동화 거래에서의 종단간 암호화

① 입력장치에 RSA 및 SEED연산을 수행할 수 있는 암호모듈 탑재
② 금융기관에 마스터키 배포 및 입력장치에 삽입
③ 서버는 마스터키를 이용하여 RSA키 쌍을 암호화 후 입력장치에 전송

암호화를 위해 중요한 사항은 세션키 공유를 위한 키(공개키 또는 마스터키)는 금융자동화기기 내 또는 금융거래서버에서 저장하여 관리할 때 장기간 사용을 금해야 하며, 저장 시 암호화로 인해 유출 사고에 대비를 해야 할 것이다. 이와 같은 일련의 키 교환 과정을 수행한 후 금융거래정보는 카드 리더기로부터 금융거래서버까지 암호화하여 전송될 수 있다. 또한 그 외 위협을 방지하기 위해 금융IC카드 사용을 권장하거나 금융자동화기기의 접근제어를 강화하는 방식으로 해결해야 할 것이다.

4.3 모바일 뱅킹

최근 이용자의 편이성으로 인해 VM모바일 뱅킹 거래가 빈번하게 이루어지고 있으며, 이로 인해 VM 모바일 뱅킹에 대한 보안 위협들이 드러나고 있다. 그 예로 VM 모바일 뱅킹 거래에서 주요 비밀정보인 PIN에 대한 유출 사고가 있었다. 주요 원인으로는 암호화의 미적용으로 인해 발생된 문제이다. 따라서 모바일 뱅킹 또한 인터넷 뱅킹과 같이 종단간 암호화가 적용되어야 모바일 뱅킹 시 존재할 수 있는 위협을 방지할 수 있을 것이다. 다음은 주요금융거래 중 이용자 PIN에 대해 종단간 암호화가 적용되어 검증되는 절차를 설명한 것이다.



[그림 5] 모바일 뱅킹 거래에서의 종단간 암호화

① 모바일 단말기와 전자금융거래 서버 간에 암호화 키 교환 과정(보안세션 핸드쉐이킹)이 수행
② 교환된 암호화 키를 이용하여 금융거래정보에 대해 모바일 단말기 내에서 암호화 과정 수행

이용자는 VM 모바일 뱅킹을 시도하기 위해 PIN을 입력하게 된다. 이때 PIN은 휴대폰 내에서 검증과정이 이루어지지 않고, 암호화되어 금융거래서버로 전송한 후, 그 유효성을 검증하게 된다.

또한 Windows CE기반 스마트폰의 경우, 이용자 PC 환경이 Windows 운영체제를 감안할 때 기존 내재된 PC 보안 위협 기술이 스마트폰으로 전이될 가능성이 높으며, 소프트웨어 개발 환경이 기존 Windows 환경과 흡사하기 때문에 Windows 응용프로그램 개발자를 통해 다양한 해킹 도구 개발 및 악성코드 제작·배포가 상대적으로 용이할 것으로 판단된다. 이러한 위협으로부터 안전한 모바일 뱅킹 거래를 이행하기 위해 보안토큰과 같이 같이 정보는 USIM내에 저장하고, 암호연산을 USIM에서 수행하여 연산의 결과만을 스마트폰의 애플리케이션으로 전달하는 종단간 암호화 방식을 적용할 수 있다. 이와 같이 모바일

폰의 종단을 USIM으로 간주하고 금융거래서버와 암호화 키를 공유하는 절차를 설계한다면, 하드웨어적으로 안전한 저장영역을 사용하고 외부로 주요 금융정보가 노출되지 않은 형태를 유지할 수 있어 이용자의 금융정보를 보호할 수 있을 것으로 예상된다.

5. 결론

전자금융거래에서 발생되는 위협은 여러 가지 원인이 존재하지만 그 중 종단간 암호화에 의해 해결될 수 있는 위협들이 존재함을 살펴보았다. 따라서 금융관련 관계자는 전자금융거래 이용자 단말기로부터 금융기관의 금융거래서버까지 입력된 금융거래정보를 안전하게 보호하는 것을 목적으로 종단간 암호화가 적용 가능한 전자금융시스템을 구성해야 하며, 향후 인터넷 뱅킹, 모바일 뱅킹, 금융자동화기기 뿐만 아니라 TV뱅킹 등 전자금융거래별로 종단간 암호화에 대한 구체적인 적용 방안 및 적용 시기에 대한 대책이 간구되어야 할 것이다.

참고문헌

[1] 금융감독원, 전자금융거래 보안 종합대책, 9월, 2005.
[2] 금융감독위원회, 전자금융감독규정시행세칙, 12월, 2006.
[3] 금융보안연구원, “종단간 암호화 적용 가이드” 7월, 2007.
[4] 김인석, “전자금융 사고유형 분석을 통한 정보보호정책에 관한 연구, 2월, 2008.
[5] 한국은행, “2009 1/4분기 국내 인터넷 뱅킹 서비스 이용현황”, http://www.bok.or.kr/, 5월, 2009.

성 재 모(Jae-Mo Seung) **[정회원]**

- 1993년 2월 : 스트븐스공과 대학원 전산학과 (이학석사)
- 2006년 2월 : 전남대학교 정보보호협동과정 박사수료
- 1993년 8월 ~ 2003년 8월 : 데이콤 정보보호기술팀 팀장
- 2003년 8월 ~ 2006년 10월 : KISA 인터넷침해사고대응지원센터 해킹대응팀 팀장
- 2006년 10월 ~ 현재 : 금융보안연구원 보안기술팀 팀장

<관심분야>
시스템&네트워크 보안, 디지털 포렌식, MIS, 암호기술

이 수 미(Su-Mi Lee) **[정회원]**

- 2003년 2월 : 고려대학교 정보경영공학전문대학원 (공학석사)
- 2004년 3월 ~ 2006년 8월 : 나사렛대학교 정보과학부 겸임교수
- 2007년 2월 : 고려대학교 정보경영공학전문대학원 (공학박사)
- 2006년 12월 ~ 현재 : 금융보안연구원 보안기술팀 주임연구원

<관심분야>
암호프로토콜, RFID인증시스템, 디지털 포렌식

안 승 호(Seung-Ho Ahn) **[정회원]**

- 1981년 8월 : 전남대학교 대학원 수학과(이학석사)
- 1985년 2월 : 전북대학교 대학원 수학과(이학박사)
- 1987년 12월 ~ 1989년 12월 : 미국 미시간 대학 수학과 방문교수
- 1983년 5월 ~ 현재 : 전남대학교 수학과 교수

<관심분야>
암호학 분야

노 봉 남(Bong-Nam Noh) **[정회원]**

- 1982년 2월 : KAIST 대학원 전산학과 (이학석사)
- 1994년 2월 : 전북대학교 대학원 전산과 (이학박사)
- 1983년 9월 ~ 현재 : 전남대학교 전자컴퓨터정보통신공학부 교수
- 2000년 9월 ~ 현재 : 리눅스 보안 연구센터 소장

<관심분야>
컴퓨터와 네트워크 보안, 정보보호시스템, 전자상거래 보안