情報保護學會論文誌
第 23 卷 第 1 號, 2013. 2

홈트레이딩 시스템의 취약점 분석과 휴대전화 인증을 이용한 대응방안 제시*

최 민 근,† 조 관 태, 이 동 훈‡
고려대학교 정보보호대학원

Analysis of Security Vulnerability in Home Trading System, and its Countermeasure using Cell phone*

Min Keun Choi,† Kwan tae Cho, Dong Hoon Lee‡
Graduate School for Information Security, Korea University

요 약

사이버 주식거래가 증가함에 따라 홈트레이딩 시스템을 이용한 주식거래가 활발해지고 있다. 홈트레이딩 시스템은 개인투자자 대다수가 이용하는 방법으로 코스닥에서는 75%도 가장 큰 비중을 차지하고 있으며, 코스피에서도 40%의 점유율을 기록하고 있다. 하지만 홈트레이딩 시스템은 사용자의 속도와 사용자 편의성에 초점을 맞추고 있어 보안기능이 다소 미흡함을 발견하였다. 본 논문에서는 홈트레이딩 시스템 사용시 메모리에 인증정보가 평문으로 남는 취약점을 기반으로 메모리 덤프 툴을 이용하여 주식부정거래 가능성을 분석하고 휴대전화 SMS를 이용한 투채널 인증으로 주식부정거래에 대응할 수 있는 인증기법을 제시한다.

ABSTRACT

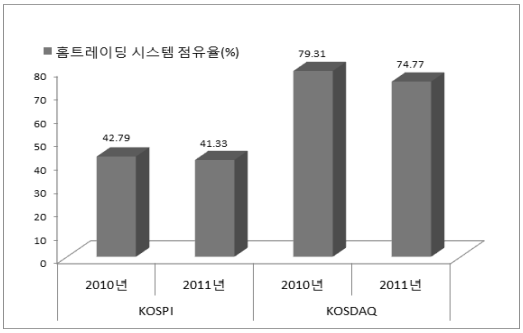
As cyber stock trading grows rapidly, stock trading using Home Trading System have been brisk recently. Home Trading System is a heavy-weight in the stock market, and the system has shown 75% and 40% market shares for KOSPI and KOSDAQ, respectively. However, since Home Trading System focuses on the convenience and the availability, it has some security problems. In this paper, we found that the authentication information in memory remains during the stock trading and we proposed its countermeasure through two-channel authentication using a mobile device such as a cell phone.

Keywords: Home Trading System, stock trading, two-channel authentication

I. 서 론

홈트레이딩 시스템은 PC와 인터넷만 있으면 어디서나 주식거래를 할 수 있는 사이버 주식거래 시스템이다. 2011년 기준으로 유가증권시장에서 홈트레이딩 시스템은 40% 이상의 점유율을 기록하고 있고, 코스닥에서는 약 75%의 점유율을 기록하고 있으며, 개인투자자의 경우 70% 이상이 홈트레이딩 시스템을 이용하여 주식거래를 하고 있다[1]. 이렇게 홈트레이딩 시스템을 이용한 주식거래가 늘고 보편화 되었지만, 홈트레이딩 시스템의 보안기능은 아직 미흡하다. 그 예로 2006년 투자상담사가 개인투자자의 홈트레이딩 시스템 계정을 해킹하여 주식거래 내역을 따라해 2009년까지 1억 5천만 원의 부당이익을 취했다가 2010년에 처벌받은 사례가 있으며[2], 2007년 인터

접수일(2012년 9월 6일), 수정일(2012년 11월 27일), 게재확정일(2012년 12월 27일)
* 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원사업"의 연구결과로 수행되었음.
† 주저자, icon6@korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr



〔그림 1〕 증권시장에서의 홈트레이딩 시스템 점유율

넷에서 쉽게 구할 수 있는 Keylogger와 Wire-Shark를 이용해 개인정보 노출 문제점도 지적되었다〔3〕.

이러한 문제를 바탕으로 본 논문에서는 메모리에 남아있는 정보를 분석하였다. 메모리 분석은 메모리 덤프 파일에서 평문으로 노출되는 정보에 초점을 맞추었다. 확인결과 아이디, 로그인 비밀번호, 계좌비밀번호와 같은 인증정보가 평문으로 노출되는 것을 확인할 수 있었으며, 노출된 인증정보를 이용하여 주식거래까지 가능한 것으로 확인되었다. 즉, 기존 기법은 공격자에 의한 부정거래 공격을 차단할 수 없다. 현재 메모리에 인증정보가 평문으로 남아있는 취약점에 대응하기 위해 확장 종단간 암호화 기술, 제로화 등이 개발되었다. 확장 종단간 암호화 기술은 메모리에 인증정보를 남기지 않는 장점이 있으나, 서버에서 가용성이 떨어지는 단점이 있고〔4〕, 제로화는 가용성을 보장하는 장점이 있지만 평문정보가 노출되는 구간의 존재와 사용자 편의성을 위해 인증번호를 저장할 경우 사용할 수 없는 단점이 존재하기 때문에 홈트레이딩 시스템에 적합하지 않다〔5〕.

본 논문에서는 기존 기법들의 가용성을 유지하면서 부정거래 공격을 차단할 수 있는 인증기법을 제안한다. 제안된 인증기법은 휴대전화를 이용한 투채널 인증기법으로, 작은 연산량을 요구하는 해쉬함수와 Exclusive OR(XOR)를 사용하여 인증코드를 생성함으로써 해쉬체인 형식으로 인증코드를 인증한다. 투채널 인증기법은 사용자 인증 및 부정거래 공격 차단을 보장하며, 해쉬함수와 XOR는 적절한 가용성을 보장한다. 이에 더하여, 본 논문에서는 구현을 통하여, 확장 종단간 암호화 기술과 현재 사용되는 기법의 가용성을 제안된 기법과 비교함으로써 제안된 기법의 우수성을 입증한다.

본 논문의 구성은 2장에서 관련연구와 주식거래 시스템에서 고려해야하는 요구사항에 대해 알아보고, 3장에서는 홈트레이딩 시스템과 메모리에 평문으로 남아있는 인증정보에 대해 알아본다. 4장에서는 휴대전화를 이용한 사용자 인증 및 안전한 주식거래 방법에 대해 제시하고, 5장에서는 제시한 인증방법을 분석한 후 6장에서 결론을 맺는다.

II. 관련연구 및 배경

본 장에서는 기존에 연구된 다양한 인증기법과 인증정보를 보호하기 위한 모듈에 대해 알아보고, 홈트레이딩 시스템에서 고려해야하는 요구사항에 대해 알아본다.

2.1 사용자 인증 관련 연구

2.1.1 아이디, 로그인 비밀번호

아이디와 로그인 비밀번호는 보편적으로 사용되는 사용자 인증방법이다. 홈트레이딩 시스템에도 적용되어 있으며, 아이디의 경우 5글자 이상, 로그인 비밀번호의 경우 영어+숫자 조합으로 6~8글자 이상을 권장하고 있다. 이러한 로그인 비밀번호를 통한 비밀번호가 노출되었을 때 매우 취약하므로 주기적으로 비밀번호를 바꿔줘야 한다. 금융회사나 포털 사이트의 경우 3개월에 한 번씩 사용자에게 비밀번호 변경을 권장하는 메시지를 보여주고 있으며, 무차별 공격에 대한 안전성을 높이기 위해 다양한 문자 조합(예를 들어, 영어+숫자+특수문자)과 같이 복잡도를 높이는 방법을 권장하고 있다.

2.1.2 공인인증서

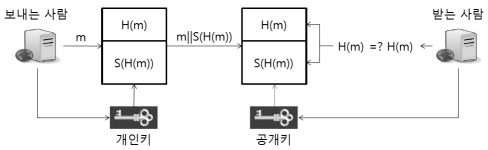
공인인증서를 통한 인증은 인터넷뱅킹과 홈트레이딩 시스템 같은 전자금융을 위해서 필수적으로 사용되는 인증수단이다. 국내에서 사용되는 공인인증서는 소프트웨어형태의 인증서로 공인인증서와 개인키 저장파일로 이루어져 있으며, X.509 v3의 기준에 따라서 작성되어있다. X.509 표준에 따른 공인인증서가 제공하는 기능은 〔표 1〕과 같으며 공인인증서를 이용한 서명과 금정과정은 〔그림 2〕와 같이 이루어진다〔6〕.

2.1.3 Multi-factor 인증

다중요소 인증은 서로 다른 두 가지 이상의 인증 요

〔표 1〕 공인인증서의 제공 기능

공인인증서 기능
가. 인터넷상에서 정보 교환 당사자의 신원확인
나. 전송되는 정보의 변형 방지
다. 계좌번호, 계좌비밀번호 및 금융거래 내역을 도청 및 해킹으로부터 방어
라. 자신이 수행한 거래에 대한 부인을 봉쇄
마. 한 개의 공인인증서로 은행, 증권, 기타 전자정부서비스 등을 이용가능
바. 전자거래기본법, 전자서명법 등의 법적 보호



〔그림 2〕 인증서를 이용한 서명 및 검증과정

소를 이용하여 사용자를 인증하는 것을 말하며, 이때 사용되는 인증요소는 다음과 같다.

1) 알고 있는 것 : 로그인 비밀번호, 공인인증서 암호 등
2) 가지고 있는 것 : 보안카드, OTP, 공인인증서 등
3) 인증 개체 그 자체 : 지문, 홍채 등

미국 연방 금융 기관 검사위원회(FFIEC)에 따르면 다중요소는 서로 다른 두 가지 이상의 인증요소를 사용할 때 다중요소라 할 수 있으며, 한 가지 종류의 인증요소를 여러 개 사용할 경우 다중요소 인증이라 할 수 없다〔7〕. 현재 홈트레이딩 시스템은 아이디와 로그인 비밀번호, 공인인증서를 함께 사용하는 다중요소 인증방식을 사용하고 있다. NIST 800-63-1 (NIST)에서는 이러한 다중요소 인증방식에 대해 각각 사용되는 경우보다 높은 3레벨의 보증수준을 정의하고 있으며, 이것은 SSL을 이용한 인증방식을 제외하고는 가장 높은 보증수준을 나타낸다〔8〕.

2.1.4 보안카드

금융회사는 계좌이체와 같은 전자금융거래를 신청할 경우 보안카드를 발급해준다. 이러한 보안카드는 금융회사별로 발급해주며 금융거래시 공인인증서와 함께 다중인증요소로써 사용된다.

보안카드를 이용한 인증은 2개의 비밀번호를 2자리씩 입력하는 방식으로 인증이 이루어진다. 따라서 보안카드의 안전성은 보안카드를 이루고 있는 비밀번호의 개수에 의존한다. 현재의 보안카드는 30~35개의 비밀번호로 구성되어 있으며, 이러한 비밀번호를 이용한 조합은 870~1190개를 이룬다〔9〕.

2.1.5 OTP(One Time Password)

OTP는 일회용 비밀번호로서 매번 다른 번호를 발생시켜 이를 이용하여 사용자 인증을 한다. 또한 현재의 패스워드로부터 다음에 사용될 패스워드를 유추하는 것이 수학적으로 불가능하다.

현재 사용되는 OTP의 생성방식은 인증 서버가 전달한 Challenge값과 공유된 비밀키의 조합을 이용하여 OTP값을 발생시키는 Challenge Response방식과 OTP토큰과 인증 서버가 동일한 시간 값이나 이벤트 카운터 값을 동기화하여 가지고 있으면서 공유하고 있는 비밀키와 조합하여 OTP값을 생성해내는 시간동기화-이벤트 동기화-조합 방식(동기화 방식)등이 존재한다〔10〕.

2.1.6 투채널 인증

다중채널 인증은 인증요소를 각기 독립적인 통신채널을 통해 전달하는 것을 의미한다. 인터넷뱅킹 상에서 다중채널 인증은 PC에서 금융거래를 시도한 후 ARS 전화로 재확인하는 방식으로 제공되었지만, 스마트폰의 보급으로 스마트폰을 이용하여 QRcode를 읽음으로써 거래내역을 스마트폰에서 전자서명 후 금융회사로 전송하는 방식의 기술과 PC와 스마트폰 양쪽의 전자서명을 비교하는 방식 등 다양한 다중채널 인증방식이 연구되고 있다〔11〕,〔12〕.

2.1.7 주민등록증 발급일자를 통한 사용자 인증

행정안전부에서는 주민등록증 발급일자를 이용한 주민등록증 진위확인 서비스를 제공하고 있으며, 넷마블, 아이템매니아와 같은 사이트에서 주민등록번호 도용 방지 목적으로 사용하고 있다. 주민등록증 발급일자는 노출되었을 시 재발급을 통해 수정 가능하고 사용자 인증으로 무분별하게 사용되지 않았기 때문에 노출이 덜 되어있다는 장점이 있다. 하지만 노출되었을 경우 갱신을 위해 주민등록증 재발급 받아야 하며, 재발급에 2주정도의 시간이 소요되기 때문에 그 시간동안 사용할 수 없는 단점이 있다.

2.2 인증정보 보호를 위한 관련연구

2.2.1 키보드 보안 모듈

키보드 보안 모듈은 키로거와 같은 키보드 해킹 프로그램에 대응하기 위해 만들어진 모듈이다. 키보드 해킹 프로그램은 타인 PC의 키보드 입력내용을 볼 수 있도록 해주는 프로그램으로 사용자가 인터넷 이용 시 키보드 입력 내용을 해킹한다. 따라서 키보드 보안 모듈은 키보드 해킹 프로그램이 키 입력 값을 빼내가지 못하게 하기 위해 키보드 드라이버를 제어한다. 키보드 드라이버 제어를 통해 키보드 보안 모듈은 키보드 포트 해킹, 키보드 드라이버 후킹과 같은 키보드 해킹 프로그램으로부터 키 입력 값을 보호할 수 있다[4].

2.2.2 메모리 보호 모듈

메모리 보호 모듈은 홈트레이딩 시스템이 참조하고 있는 메모리에 타 프로세스의 접근을 차단하는 보안모듈이다. 타 프로세스의 메모리 접근을 차단함으로서 온라인으로 송수신되는 인증정보와 거래정보 등이 유출 및 조작되는 것을 방지하고 온라인 거래의 신뢰성을 높여주는 역할을 한다.

2.2.3 제로화

제로화는 메모리에 평문으로 저장된 인증정보를 '0'또는 '1'로 덮어쓰는 방법이다. FIPS PUB 140-2에 정의되어있으며, 본 목적은 암호화키 보호이지만 메모리에 저장된 정보를 삭제할 경우에도 사용된다[5].

제로화가 필요한 데이터로는 암호화에 필요한 비밀키, 평문 등의 정보가 속해지며, 비정상적인 종료와 Reset 공격 등에 대해서도 대응할 수 있어야 한다.

2.2.4 종단간 암호화

종단간 암호화 기술은 키보드 보안 모듈과 PKI 암호화 모듈을 연동함으로써 이용자 PC 전 구간에서 금융거래 정보를 안전하게 전송하므로 외부 침입으로부터 보호할 수 있는 기술을 말한다. 보안모듈 사이의 세션키 공유 방식에 따라 초기 종단간 암호화 기술과 확장 종단간 암호화 기술로 나누어진다.

1) 초기 종단간 암호화 기술

초기의 종단간 암호화 방식은 키보드 보안 모듈이 키보드 입력 값을 암호화하여 메모리에 적재한 후 전송 이벤트 발생 시 복호화하여 PKI 암호화 모듈로 전송한다. PKI 암호화 모듈은 금융회사 서버간에 공유된 세션키로 암호화하여 금융회사 서버로 전송한다. 초기 종단간 암호화 기술은 키보드 보안 모듈에서 PKI 암호화 모듈로 키보드 입력 값을 전송하는 과정에서 복호 모듈에 의해 평문으로 존재하는 구간이 전재하게 되어 키보드 입력 값이 노출될 가능성을 내포하고 있다.

2) 확장 종단간 암호화 기술

확장 종단간 암호화 기술은 이용자 PC에 키보드 보안 모듈의 종단간 암호화 모듈만이 존재하고, 종단간 복호모듈은 전자금융거래 서버에만 위치되도록 설계함되었다. 초기 종단간 암호화 방식의 문제점은 키보드 입력 값이 PC내 평문으로 존재하는 구간이 발생한다는 점이다. 따라서 키보드 보안 모듈과 금융회사의 서버간에 세션키를 공유하여 종단간에 암호화를 제공하는 방식으로 개선하였다. 개선된 확장 종단간 암호화 기술은 키보드 보안 모듈과 금융회사 서버가 종단간 암호키를 공유하는 단계와 암호화된 키보드 입력 값을 금융회사 서버에 전송하는 단계로 이루어진다. 확장 종단간 암호화 기술은 키보드 입력값을 복호화 과정 없이 금융회사로 전송함으로써 기밀성을 보장하게 된다. 이로 인해 PC에서 복호 모듈을 제거하고 종단간 암호키를 세션 및 페이지마다 갱신함으로써 평문 노출 위협을 방지할 수 있다.확장 종단간 암호화는 키보드 보안 모듈과 PKI 암호화 모듈을 연동하여 키보드 입력 값을 서버에서 복호화 하는 방식이다. 확장 종단간 암호화는 사용자PC에서 키 입력 값을 복호화

〔표 2〕 분석환경

PC 구분	CPU	Memory	OS
Host PC	Intel Core(TM) i7-2620M 2.70GHz	8.00GB	Windows 7 Home Premium K (64bit)
가상머신 (VMware)	Intel Core(TM) i7-2620M 2.70GHz	1.00GB	Windows XP Professional Version 2002 Service Pack 3 (32bit)

하지 않으므로 메모리에 평문 인증정보를 남기지 않는다[4].

2.3 홈트레이딩 시스템에서 고려해야하는 요구사항

2.3.1 사용자 인증

홈트레이딩 시스템은 비대면 거래이므로 사용자 인증을 통해 정당한 사용자를 구별할 수 있어야 한다. 현재 홈트레이딩 시스템은 공인인증서와 인증정보가 들어있는 메모리 덤프 파일이 노출되었을 경우 공격자는 사용자 계정으로 로그인과 부정거래를 할 수 있다. 따라서 정당한 사용자만 접근을 허용하는 인증수단이 필요하다.

2.3.2 가용성

홈트레이딩 시스템은 짧은 시간 내에 실시간으로 주식거래가 처리되어야 한다. 따라서 사용자PC에서 서버로 보내지는 주식주문데이터의 생성 및 처리시간은 현재 홈트레이딩 시스템과 비교하여 그 차이가 미비해야 한다.

2.3.3 부정거래 방지

인증정보가 노출되었을 경우에도 공격자에 의한 부정거래를 막을 수 있어야 한다. 공격자는 메모리에 남아있는 인증정보 탈취와 전송구간에서의 스니핑을 통해 인증정보를 획득할 수 있지만, 이러한 인증정보를 통해 타인의 명의로 주식거래를 실행하는 등 이와 같은 부정거래를 할 수 없어야 한다.

III. 홈트레이딩 시스템 취약점 분석

본 장에서는 홈트레이딩 시스템을 이용할 때 인증정보가 평문으로 남는 취약점과 노출된 인증정보를 이용하여 계정탈취가 가능한지를 분석한다. 분석대상은 금융투자협회에 등록되어있는 증권회사 중에서 홈트레이딩 시스템 서비스를 제공하는 증권사를 대상으로 하였으며[13], 총 40개 국내증권사 중 랜덤하게 16개 증권사를 지정하였다. 증권사가 운영하는 홈트레이딩 시스템이 2개 이상일 경우 개인정보 노출이 많은 홈트레이딩 시스템을 기준으로 결과를 작성하였다.

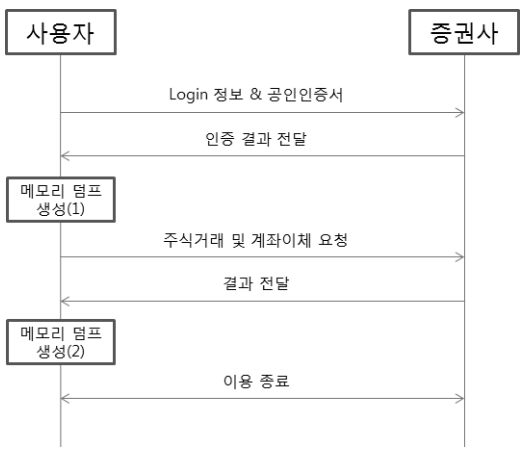
3.1 분석환경

16개 증권사의 홈트레이딩 시스템을 확인하기 위해 가상머신을 사용하였으며, 가상머신의 환경은 [표 2]과 같다. 증권사에서 제공하는 보안모듈과 각 증권사별로 메모리에 남아있는 정보를 수집하기 위해 홈트레이딩 시스템 별로 하나의 가상머신을 부여하였으며, 가상머신에는 홈트레이딩 시스템과 메모리 덤프 파일 생성 프로그램을 설치하였다. 또한 증권사에서 제공하는 키보드 보안 모듈, PKI 암호화 모듈, 개인 방화벽 등과 같은 보안 모듈은 모두 설치하였다.

3.2 분석방법 및 사용도구

3.2.1 분석방법

본 절에서는 메모리에 인증정보가 평문으로 남는 취약점을 분석하기 위하여 실행한 방법에 대해서 알아보도록 한다. 홈트레이딩 시스템 프로그램을 실행 후 로그인과 계좌이체 혹은 주식거래를 시도한다. 이 후 메모리에 인증정보가 남아있는지 확인을 위해 메모리 덤프 파일을 생성한 후 Hex editor로 분석한다. 메모리 덤프 파일은 [그림 3]와 같이 2번 생성하며, (1)번째 생성된 메모리 덤프에서는 아이디, 로그인 비밀번호, 공인인증서 암호를 평문검색하였고 (2)번째 생성된 메모리 덤프에서는 계좌비밀번호를 평문검색하였다. 그리고 2개의 메모리 덤프 파일을 통해 얻은 인증정보를 사용하여 공격자의 부정거래 가능성을 파악한다.



[그림 3] 메모리 덤프 생성 순간

3.2.2 사용도구 분석

메모리에 남겨진 인증정보 분석에 사용된 도구는 전체 메모리를 덤프파일로 생성해주는 도구와 메모리 덤프파일분석에 필요한 HEX editor이다. 본 논문에서는 메모리 덤프프로그램에 windd를 사용하였으며, HEX editor는 HxD editor를 사용하였다. 두 개의 프로그램은 모두 프리웨어로써 누구나 쉽게 접할 수 있는 프로그램이다. windd의 경우 전체 메모리를 파일로 생성해주며, 실행시 RAM 크기와 동일한 파일사이즈로 메모리 덤프파일을 생성한다. 분석에 windd를 사용한 이유는 전체 메모리 덤프의 경우 메모리 보호 모듈을 우회하여 메모리 덤프파일 생성이 가능하기 때문이며, 홈트레이딩 시스템에서 사용하는 메모리에 대해 접근할 경우 메모리 보호 모듈에 의해 접근이 차단되는 것을 알 수 있다. HxD editor의 경우 프리웨어로써 사용에 제약이 없기 때문에 사용한 프로그램으로 다른 010editor과 같은 다른 HEX editor을 사용해도 무방하다.

3.3 메모리 덤프 파일 분석

16개 증권사의 메모리 덤프 파일을 분석한 결과 평문으로 인증정보가 노출되는 것을 확인하였고, 이를 〔표 3〕로 정리하였다. 노출된 인증정보를 통해 계정탈취 가능성이 있는 12개 증권사에 대해서 다음과 같이 분류하였다.

〔표 3〕 증권사별 평문 노출된 인증정보와 부정거래가능여부

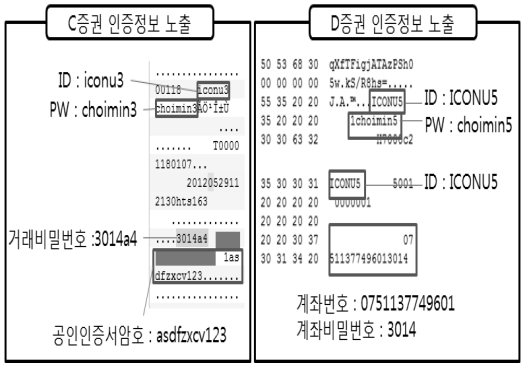
증권사	아이디	로그인 비밀번호	공인 인증서 암호	계좌 비밀 번호	부정 거래 가능
A증권	○	×	○	×	×
B증권	○	○	○	○	○
C증권	○	○	○	○	○
D증권	○	○	×	○	△
E증권	○	○	○	○	○
F증권	○	○	○	○	○
G증권	○	○	○	○	○
H증권	○	○	○	○	○
I증권	○	×	○	○	×
J증권	○	×	×	×	×
K증권	○	○	○	○	○
L증권	○	○	○	○	○
M증권	○	×	○	×	×
N증권	○	○	○	○	○
O증권	○	○	○	○	○
P증권	○	○	×	○	△
계	16	12	13	13	10 (2)

아이디, 로그인 비밀번호, 공인인증서 암호, 계좌비밀번호가 노출된 경우

B증권, E증권, F증권, G증권, H증권, K증권, L증권, N증권, O증권은 아이디, 로그인 비밀번호, 공인인증서 개인키 비밀번호, 계좌비밀번호가 노출되었다. 그리고 C증권은 계좌비밀번호가 아닌 거래비밀번호를 사용한다. 하지만 거래비밀번호도 메모리에 평문으로 노출되어있음을 알 수 있다. 이 증권사들은 공격자가 메모리 덤프파일을 생성해서 공인인증서와 공인인증서 개인키 파일을 함께 복사해간다면 계정탈취가 가능하고, 부정거래까지 가능하다.

3.3.1 아이디, 로그인 비밀번호, 계좌비밀번호가 노출된 경우

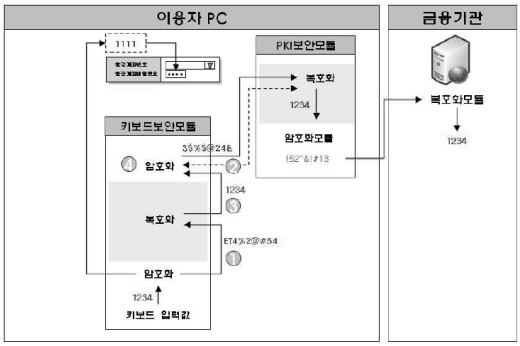
D증권, P증권은 아이디, 로그인 비밀번호, 계좌비밀번호가 노출되었다. 이 증권사들은 공인인증서 암호가 노출되지 않는다. 하지만 공인인증서 암호의 경우 PKES#1에 의해 올바른 암호인지를 검증하기 때문에 암호 복잡도가 낮을 경우 무차별 공격으로 암호를 알아 낼 수 있다. 따라서 공격자가 메모리 덤프 파일과 공인인증서, 공인인증서 개인키 파일을 함께 복사해갈 경우 2.3.1과 마찬가지로 부정거래는 가능하다〔14〕,〔15〕.



〔그림 4〕 메모리에 평문으로 노출된 인증정보

3.1 메모리에 인증정보 평문 노출 원인

홈트레이딩 시스템에서 메모리에 인증정보가 평문으로 남는 취약점은 증권사에서 초기형 종단간 암호화 기술을 사용하기 때문에 발생한다. 초기형 종단간 암



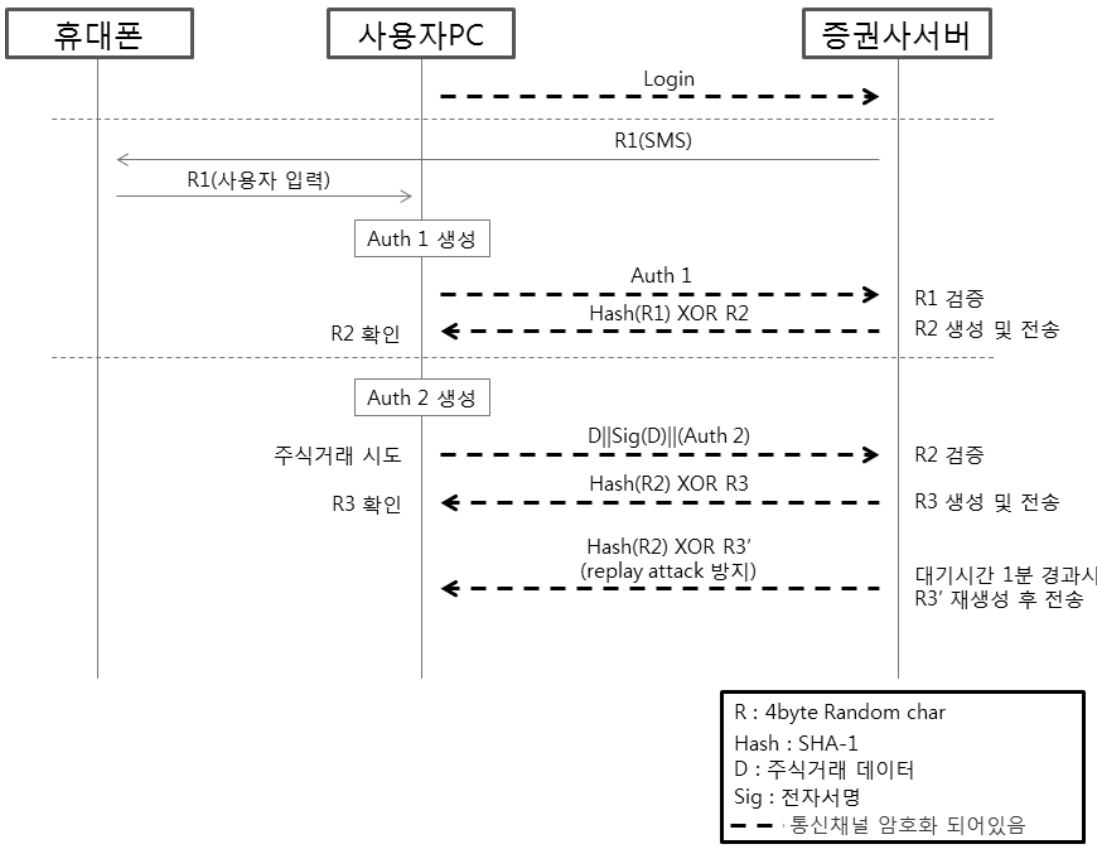
〔그림 5〕 초기형 종단간 암호화에서 평문 노출 구간

호화 기술은 〔그림 5〕와 같이 키보드 보안 모듈에서 PKI 암호화 모듈로 데이터를 전송할 때 복호화 후 재암호화가 이루어지며[4], 이 과정에서 메모리에 평문 데이터가 기록된다. 이러한 취약점을 막기 위해 은행권의 인터넷뱅킹에서는 확장 종단간 암호화 기술이 도입되고 있으나, 홈트레이딩 시스템에서는 가용성의 문제로 도입하지 못하고 있다.

IV. 홈트레이딩 시스템의 계정탈취를 막기 위해 제안된 기법

4.1 시스템 모델

제안된 기법은 홈트레이딩 시스템에서 휴대전화의 SMS를 이용하여 인증번호를 전송함으로써 투채널 인증을 만족시키면서 인증과정의 보안성을 높이는 방법이다. 투채널 인증은 다른 채널을 통해 사용자 인증에 필요한 정보가 전송되는 방식을 말하며, 본 논문에서는 휴대전화를 통해 SMS를 전송받음으로써 투채널 인증을 만족하다. 하지만 현재의 홈트레이딩 시스템에서는 공격자에 의해 사용자의 개인정보 수정이 가능하기 때문에 투채널 인증의 안전성을 보장하지 못하므로 개인정보를 수정하지 못하게 하기위한 추가적 인증이 필요하다. 현재 행정안전부에서는 주민등록번호 발급



〔그림 6〕 휴대전화를 이용한 주식거래 scheme

일자를 통한 사용자 인증 서비스를 제공하고 있다. 주민등록번호와 달리 주민등록증발급일자는 노출되었을 경우 바꿀 수 있고, 주민등록증을 가지고 있는 사람이라면 누구든지 사용할 수 있다는 장점이 있다. 따라서 개인정보 수정시 주민등록증 발급일자를 이용한 인증수단을 도입한다면 개인정보의 무결성을 보장하고, 이를 통해 투채널 인증의 안전성도 보장할 수 있다.

4.2 제안된 인증 기법 상세

제안된 인증방법은 홈트레이딩 시스템에서 주식거래 이전에 휴대전화로 전송된 인증번호를 입력함으로써 공격자의 계정탈취를 차단하고, 주식거래시 사용자의 불편함을 없애는데 초점을 두었다. 제안된 주식거래 방법은 사용자인증과 주식거래식별로 나누어진다.

사용자인증은 아이디, 로그인 비밀번호, 공인인증서 암호, 휴대전화로 전송된 인증번호가 사용되며, 휴대전화로 전송된 인증번호를 이용하여 인증코드를 생성하고 서버가 인증코드를 검증하는 순서로 이루어진다. 인증번호는 재사용 방지를 위해 유효시간을 두었으며 유효시간은 1분이다. 1분이 경과하였을 경우 새로운 인증번호를 재생성하여 다시 전송한다. 그리고 사용자 편의성을 고려하여 로그인 이후 주식거래 창으로 이동시 1회에 한해서 사용자인증을 시도한다.

주식거래 무결성은 사용자인증을 받은 세션을 식별하는 방법으로 정당한 사용자의 거래임을 보장한다. 주식거래 무결성도 인증번호를 이용하여 이루어진다. 하지만 가용성을 높이기 위해 휴대전화를 이용한 인증번호전송이 아닌 서버에서 사용자PC로 전송된다. 주식거래 무결성을 보장하기 위해 사용자PC는 인증번호를 이용하여 인증코드를 만들고 거래정보 뒤에 붙이는 방식으로 이루어진다. 전송구간에서 인증번호를 보호하기 위해 해쉬함수를 이용함으로써 가용성에 미치는 영향을 최소화 하였다.

제안된 주식거래 방법은 크게 5단계로, 휴대전화로 보내진 인증번호를 이용한 사용자 인증코드 생성 및 전송, 사용자 검증, 주식거래식별을 위한 난수 생성 및 전송, 주식거래 인증코드 생성, 주식거래 인증코드 검증으로 구성된다.

4.2.1 용어 표기

R_n : 서버에서 생성된 인증번호.숫자 8자리이다.

$Timestamp$: 인증코드가 생성된 시간을 기록된 값. 숫자6자리이다(6byte).

UC_n : 사용자PC에서 생성된 $Timestamp$와 R_n로 구성된 메시지

SC_n : 서버에서 생성된 인증번호를 안전하게 전송하기 위한 메시지

$Hash$: Hash function으로 SHA-1이 사용됨.

XOR : Exclusive OR를 나타내며 연산기호 ⊕로 표기된다.

D : 주식거래 데이터

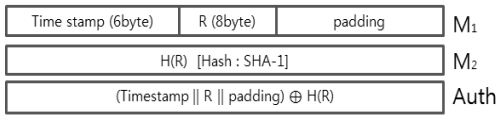
S_m : 서버로 전송되는 주식주문데이터

$Auth_n$: 사용자 인증과 주식거래 무결성을 위한 인증코드

4.2.2 휴대전화 SMS로 보내진 인증번호를 이용한 사용자 인증코드 생성

휴대전화의 SMS로 보내진 인증번호 R_1을 홈트레이딩 시스템을 통해 입력함으로써 사용자 인증코드 $Auth_1$이 생성하고, 이를 통신채널 암호화를 거쳐 서버로 전송한다. $Auth_1$의 구조는 〔그림 7〕과 같다. $Auth_1$은 R_1의 재사용 방지를 위한 $Timestamp$와 사용자인증을 위한 R_1을 붙여 생성한 M_1에 R_1을 $Hash$하여 생성한 M_2를 XOR하여 생성한다. 서버는 휴대전화로 보낸 인증번호가 1분 이내로 도착하지 않으면 재사용방지를 위해 새로운 인증번호를 재생성하여 다시 전송한다.

$$Auth_1 = (Timestamp \| R_1) \oplus Hash(R_1)$$



〔그림 7〕 사용자PC에서 서버로 보내는 인증코드 구조

4.2.3 사용자 검증

서버는 사용자PC에서 보내온 사용자 인증코드 $Auth_1$에서 인증코드가 만들어진 시간이 기록되어있는 $Timestamp$와 휴대전화를 통해 전송된 인증번호 R_1을 확인함으로써 사용자 인증을 한다.

$$Verify : Auth_1 \oplus Hash(R_1)$$
$$= Timestamp \| R_1 \oplus Hash(R_1) \oplus Hash(R_1)$$
$$= Timestamp \| R_1 \ (\because Auth_1 = Timestamp \| R_1)$$

4.2.4 주식거래 식별을 위한 인증번호 생성 및 전송

인증 된 사용자로부터 오는 주식거래를 식별하기 위해 서버는 인증번호 R_n를 생성하여 사용자PC로 전송한다. 이는 사용자 검증을 마친 세션에 한해서 보내지며, 전송구간에서 인증번호 R_n의 평문 노출을 막기 위해 R_{n-1}을 $Hash$하여 얻은 메시지와 XOR하여 전송한다.

$SC_n = R_n \oplus Hash(R_{n-1})$

1분 동안 R_n을 이용한 주식거래가 없을 시 서버는 새로운 인증번호 R_n'을 재생성하여 SC_n'을 만들고 이를 사용자PC로 다시 전송한다.

$SC_n' = R_n' \oplus Hash(R_{n-1})$

4.2.5 주식거래 인증코드 생성

사용자PC는 서버로부터 받은 SC_n에 R_{n-1}을 $Hash$한 값으로 XOR하여 R_n을 추출한다. R_n과 $Timestamp$를 합친 후 R_n을 $Hash$한 값으로 XOR하여 $Auth_n$을 생성한다. 생성된 $Auth_n$는 사용자의 주식거래시 전자서명된 주식거래데이터 뒤에 붙인 뒤 서버로 전송한다. 1분간 사용자의 주식거래가 없을시 $Auth_n$은 폐기되고 서버로부터 재전송 받은 SC_n'을 이용하여 $Auth_n'$을 새롭게 생성한다.

$SC_n \oplus Hash(R_{n-1})$

$= R \oplus Hash(R_{n-1}) \oplus Hash(R_{n-1}) = R_n$

$(\because SC_n = R_n \oplus Hash(R_{n-1}))$

$Auth_n = Time\,stamp \| R_n \oplus Hash(R_n)$

$S_m = D \| Sig(D) \| Auth_n$

4.2.6 주식거래 인증코드 검증

서버는 사용자PC에서 보내온 S_m에서 인증된 사용자를 식별하는 $Auth_n$를 분리한 후 확인한다. $Auth_n$에서 R_n을 $Hash$한 값으로 XOR한 후 R_n과 $Timestamp$를 검증한다. 검증 후 인증된 사용자일 경우 주식거래 데이터를 처리한다. 주식거래데이터를 처리한 후 다음 주식거래를 위해 새로운 인증번호를 생성한 후 전송되며 이후 거래는 5.2.4부터 5.2.6까지 반복함으로써 이루어진다.

$S_m = D \| Sig(D) \| Auth_n$

$Verify \ : \ Auth_n \oplus Hash(R_n)$

$= Timestamp \| R_n \oplus Hash(R_n) \oplus Hash(R_n)$

$= Timestamp \| R_n$

V. 제안된 인증기법의 분석

5.1 제안된 인증기법에서의 요구사항 분석

5.1.1 사용자 인증

홈트레이딩 시스템은 전자기기를 사용한 비대면 거래이므로 사용자 인증을 통해 정당한 사용자를 구별할 수 있어야 한다. 이러한 요구사항을 만족하기 위해 제안된 인증기법은 투채널 인증을 사용하여 정당한 사용자를 구별하고 공격자의 주식거래 접근을 차단한다.

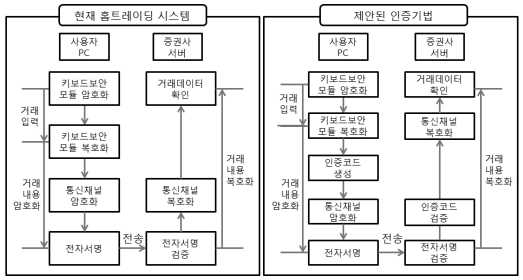
1) 투채널 인증의 안전성 분석

제안된 인증기법은 아이디, 로그인 비밀번호, 공인인증서를 사용하는 인증과 휴대전화를 통해 인증번호를 통해 투채널 인증을 만족한다. 이러한 투채널 인증의 안전성은 증권사에 저장되어있는 개인정보의 무결성에 의존한다. 따라서 공격자가 사용자의 개인정보를 수정할 수 없다면 휴대전화를 이용한 투채널 인증은 안전하다.

5.1.2 가용성

홈트레이딩 시스템을 이용한 주식거래는 실시간으로 이루어지기 때문에 보안모듈로 인해 발생되는 처리지연시간을 최소화 해야한다. 이러한 요구사항이 만족하는지를 확인하기 위해 현재 홈트레이딩 시스템과 확장 종단간 암호화, 그리고 제안된 인증기법에서 주식거래 데이터를 처리하는데 소비되는 시간을 측정하여 가용성을 비교하였다. 본 논문에서는 실제 증권사를 통한 주식거래에서의 가용성 비교를 할 수 없기 때문에 시뮬레이션 환경을 구축하여 테스트 하였다.

시뮬레이션 환경은 i7-2620M CPU와 8GB RAM이 설치된 노트북에서 이루어졌으며 주식거래 데이터를 생성과 처리하는데 사용되는 알고리즘을 프로그래밍으로 구현하여 암호화 복호화 과정을 반복하여 소비되는 평균 시간을 측정하였다. 가용성 테스트는 사용자가 주식거래를 하였을 때 발생하는 주식거래 데이터의 생성과 처리과정에서 발생하는 소비시간과 서버에서 다량의 데이터가 처리될 때 발생하는 지연시간을 각 과정별로 비교하였다. 사용자의 주식거래 데이터는 사용자PC에서 증권사 서버로 보내지는 데이



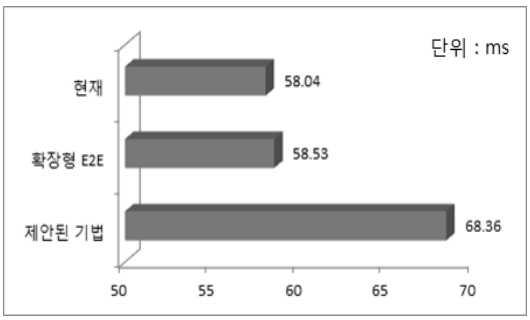
〔그림 8〕 현재 홈트레이딩 시스템과 제안된 인증기법에서의 주식거래 흐름도

〔표 4〕 구간 별 암호 알고리즘

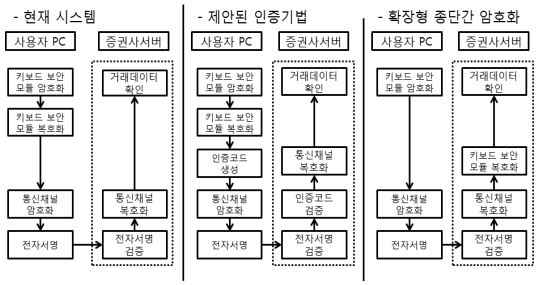
구 간	알고리즘
키보드 보안 모듈	SEED 128bit
인증코드 생성, 검증	SHA-1
통신채널 암호화	SEED-CBC 128bit
PKI 암호화 모듈	RSA 2048bit

터로써 키보드 보안 모듈과 통신채널 암호화, 전자서명과 같은 다양한 암호화 기법이 사용된다. 사용되는 암호화 기법은 〔표 4〕에 명시하였으며 테스트에서는 Java언어를 이용하여 프로그래밍 하였다. 주식거래 데이터의 생성과 처리 과정은 금융암호화 기술 적용 가이드를 참조하여 〔그림 8〕과 같은 과정으로 진행하였다〔16〕.

사용자 주식거래 데이터에 대한 테스트에서 현재 시스템과 확장 종단간 암호화 기법은 별 차이를 보이지 않았지만 제안된 기법은 약 17% 느린 것으로 나타났다. 이는 Hash 함수와 XOR 연산이 추가됨으로써 발생하는 시간으로 해석할 수 있다. 하지만 시간적으로 환산하였을 때 0.1초의 지연시간이 발생한 것으로 이것은 실제 사용자가 느끼기에 미미한 시간으로 큰 차이라 볼 수 없다.



〔그림 9〕 제안된 기법과 현재 주식거래의 속도비교 결과

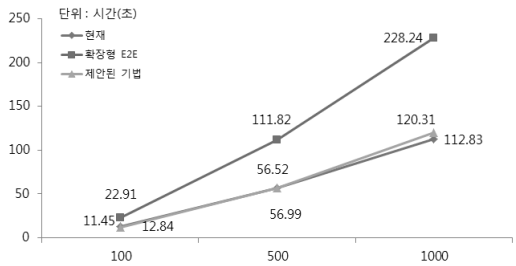


〔그림 10〕 시스템 별 복호화 시뮬레이션 과정

서버에서 다량의 데이터 처리로 발생하는 지연시간 비교는 시뮬레이션 환경에서 서버에서 발생하는 연산을 반복하여 소비되는 시간을 측정하는 방식으로 진행하였으며, 구체적 과정은 〔그림 10〕에 명시하였다.

진행과정은 전자서명된 주식거래 데이터의 검증과 통신채널 복호화 순서로 진행된다. 확장 종단간 암호화의 경우 키보드 보안 모듈의 복호화 과정이 추가되었고, 제안된 인증기법의 경우 Hash함수와 XOR로 이루어진 인증코드 검증과정이 추가되었다.

서버에서 발생하는 지연시간에 대한 시뮬레이션 결과는 〔그림 11〕과 같다. 현재 사용되는 인증기법과 제안된 인증기법은 별 차이가 없는 반면, 확장 종단간 암호화 과정은 많은 지연시간이 소비되는걸 알 수 있다. 이는 키보드 보안 모듈에서 암호화된 키보드 입력값을 서버에서 복호화하는 과정이 추가되기 때문이다.



〔그림 11〕 서버에서의 인증기법 별 다중 데이터 처리 속도 비교

제안된 인증기법은 전체 데이터 처리 과정에서는 현재 시스템과 확장 종단간 암호화 기술과 비교하여 미미한 시간 손실이 발생하지만 서버에서의 데이터 처리 지연시간은 확장 종단간 암호화 기술보다 좋은 결과를 보였다. 따라서 제안된 인증기법은 증권회사에서 중시하는 가용성을 만족한다.

5.1.3 부정거래 방지

제시된 인증기법은 주식거래시 인증코드를 이용하여 부정거래를 구별한다. 하지만 인증코드 자체를 공격자가 수집하는 것은 막을 수 없으므로 인증코드가 노출되더라도 공격자가 주식거래를 할 수 없게끔 대응책을 마련해야한다. 제시된 인증기법에서는 메모리 덤프 파일을 통해 인증번호와 인증코드를 수집하였을 경우에 대해 공격자가 주식거래를 할 수 없음을 증명한다.

1) 메모리에 노출되는 인증번호와 인증코드가 수집되었을 경우의 안전성

메모리에 노출되는 인증번호에 대한 안전성은 전송속도에 의존한다. 일반적으로 100Mbps 인터넷 망을 이용할 경우 1GB RAM에서 생성한 메모리 덤프 파일을 가져가기 위해 필요한 시간은 약 80초가 소비된다. 따라서 메모리 덤프 파일을 전송받기 이전에 새로운 인증번호가 사용자PC로 전송되며, 메모리 덤프 파일에 남아있는 인증번호는 폐기되어 사용할 수 없다.

2) 메모리 덤프 파일 전송에 소비되는 시간

RAM : 1GB
전송속도 : 100Mbps
전송에 걸리는 시간
= 1024Mbyte / (100Mbps)
= 8192Mbit / (100Mbps)
≒ 82초 = 1분 22초

5.2 홈트레이딩 시스템에서 관련연구 적합성 분석

이 절에서는 현재 전자금융에 사용되는 인증기법과 보안 모듈을 홈트레이딩 시스템 요구사항에 맞추어 비교하고, 사용 가능성에 대해 알아본다.

5.2.1 아이디, 로그인 비밀번호

NIST 800-63-1(NIST)에서는 아이디와 로그인 비밀번호를 이용한 사용자 인증에 대해 Keylogger, 피싱, 소셜엔지니어링 공격에 취약하다 정의하고 있다[8]. 이는 비밀번호가 노출되었을 때 안전성을 보장할 수 없기 때문이다. 현재 실험에 이용된 16개 증권사 중 12개 증권사에서 메모리에 아이디와 로그인 비밀번호가 평문으로 노출되기 때문에 아이디와 로그인 비밀번호를 사용하는 인증방식은 부정거래에 안전하지 못하다.

5.2.2 공인인증서

NIST에서는 Software로 이루어진 인증서는 복

〔표 5〕 인증기법 비교

사용자 인증 기법	사용자 인증	가용성	부정 거래 방지	비 고
아이디, 비밀번호	×	-	×	아이디와 비밀번호가 노출될 경우 도용가능
공인인증서	×	-	×	개인키 파일이 노출될 경우 도용가능
보안카드, OTP	○	-	○	시도-응답 방식으로 부정거래를 막을 수 있음 은행제휴계좌 사용자의 경우 보안카드와 OTP 미소유자가 있음.
다중요소 인증	×	-	×	이미 사용되는 인증기법으로 인증정보가 노출될 경우 도용 가능
투채널 인증 (기존에 제안된 기법)	○	×	○	투채널을 이용함으로써 사용자 인증과 부정거래 방지가 가능 기존의 투채널 인증은 거래데이터를 모바일 기기에서 금융회사로 전송하기 때문에 유선망에 비해 가용성이 떨어짐
주민등록증 발급일자를 통한 사용자 인증	×	×	×	고정된 값으로 노출되었을 경우 도용이 가능하며, 발급일자 변경을 위해선 주민등록증을 재발급 받아야 됨
키보드 보안 모듈	-	-	×	키보드 입력값을 암호화 하지만 PKI 암호화 모듈로 전송시 복호화 과정을 거침으로 평문이 노출됨
메모리 보호 모듈	-	×	×	전체 메모리 덤프 생성의 경우 막을 수 없음
제로화	-	×	△	인증정보가 사용된 후 지우는 방식으로 가용성엔 영향을 주지 않음 사용자 편의성에 의해 보관된 인증정보는 지울 수 없음
확장 종단간 암호화 기술	-	×	○	암호화를 통해 인증정보를 보호할 수 있음 서버에서의 지연시간이 발생함
제안된 인증기법	○	△	○	투채널을 이용함으로써 사용자 인증과 부정거래 방지가 가능. 랜덤한 값으로 인증코드를 생성하므로 인증정보가 노출되도 안전함. XOR와 Hash를 이용하기 때문에 속도저하가 미미함

사와 Offline Crack에 취약하다 정의하고 있다[8]. 이는 파일형태로 이루어진 인증서와 개인키를 복사하였을 때 제약 없이 사용이 가능하고, PBES#1 padding으로 비밀번호를 체크하기 때문에 무차별 공격이 가능하다. 또한 실험에 이용된 16개 증권사의 홈트레이딩 시스템 중 13개에서 메모리에 공인인증서 암호가 평문으로 노출되어있기 때문에 공인인증서를 통한 사용자 인증은 안전하지 못하다.

5.2.3 다중요소 인증

현재 홈트레이딩 시스템에서는 아이디와 로그인 비밀번호, 공인인증서를 함께 사용하는 다중요소 인증방식을 사용하고 있다. NIST에서는 이러한 다중요소 인증방식에 대해 각각 사용되는 경우보다 높은 3레벨의 보증수준을 정의하고 있다. 하지만 공인인증서와 개인키 파일이 복사되었을 경우 사용되는 비밀번호가 메모리에 모두 노출되기 때문에 다중요소 인증은 안전성을 보장할 수 없다.

5.2.4 보안카드 or OTP

보안카드와 OTP는 일회용 인증번호가 사용되므로 메모리에 노출되더라도 홈트레이딩 시스템의 안전성에 문제가 되지 않지만 은행을 통한 제휴계좌로 주식거래통장을 만들 경우 보안카드나 OTP를 제공하지 않기 때문에 보안수단으로 사용할 수 없다.

5.2.5 다중채널 인증

기존에 인터넷 뱅킹에서의 다중채널 인증은 다른 채널을 사용함으로써 보안을 강화할 수 있지만, 거래 데이터마다 휴대폰에서 전자서명을 해야 하기 때문에 휴대폰으로 데이터 전송과 전자서명에 소비되는 시간으로 인해 실시간 주식거래에서는 가용성이 떨어지는 문제가 있다.

5.2.6 키보드 보안 모듈

현재 홈트레이딩 시스템에서 키보드 보안 모듈은 키보드 입력 값을 암호화함으로써 키로거와 같은 키보드 해킹 프로그램으로부터 키보드 입력 값을 보호한다. PKI 암호화 모듈로 데이터를 전송할 때 복호화 모듈을 거쳐가기 때문에 키보드 입력값이 노출되는 문제가 발생한다. 이는 키보드 입력값을 암호화하면서도 인증정보가 메모리에 평문으로 노출되는 문제를 발생시킨다.

5.2.7 메모리 보호 모듈

메모리 보호 모듈은 홈트레이딩 시스템이 참조하고 있는 메모리에 타 프로세스의 접근을 차단하지만, 전체 메모리덤프를 생성하는 프로그램은 차단하지 않는다. 따라서 windd와 같은 전체 메모리덤프를 생성하는 프로그램으로 덤프파일을 생성하였을 때, 사용자 인증정보가 평문으로 노출되는 것을 막을 수는 없다.

5.2.8 제로화

제로화는 인증정보 사용 후 삭제하는 방식으로 주식거래 속도에 영향을 주지 않는 장점이 있다. 하지만 사용자 편의성에 의해 지속적으로 사용하는 인증정보

〔표 6〕 인증기법 별 정량적 비교표

사용자PC /서버	알고리즘	현재 시스템	투채널인증	확장 E2E	제안된 인증기법
사용자 PC	Seed	2	1	1	2
	Seed-CBC	1	1	1	1
	RSA	1	-	1	1
	Hash	-	-	-	1
스마트폰	RSA	-	1	-	-
서버	Seed	-	1	1	-
	Seed-CBC	1	1	1	1
	RSA	1	1	1	1
	Hash	-	-	-	1
비교	전체 사용 알고리즘	-	-	-	(+)Hash * 2
	서버	-	(+) Seed	(+) Seed	(+)Hash

에 대해서는 제로화를 실행할 수 없으며, 사용 중 오류로 인해 제로화 이전에 프로그램이 종료될 경우 인증정보가 메모리에 남아있는 문제가 있다.

5.2.9 확장 종단간 암호화 기술

확장 종단간 암호화는 사용자PC에서 키 입력 값을 복호화하지 않으므로 메모리에 평문 인증정보를 남기지 않는다[4]. 하지만 서버에서 키보드 입력 값을 복호화하기 때문에 동시에 여럿사용자가 주식거래요청을 할 경우 처리시간이 늘어나므로 가용이 떨어진다. 따라서 실시간 주식거래가 중요한 홈트레이딩 시스템에서 가용성이 떨어지는 확장 종단간 암호화는 적합하지 않다.

5.3 보안 모듈 지연시간의 정량적 비교 분석

이 절에서는 부정거래 가능성에 대해 막을 수 있는 투채널인증, 확장 종단간 암호화, 제안된 인증기법들에 대해 정량적 비교를 통해 효용성을 비교분석한다. 효용성 비교는 사용되는 전체 알고리즘에 대한 비교와 서버에서 사용되는 알고리즘에 대해 비교하였다. 사용된 알고리즘은 금융 암호기술 적용 가이드를 참고하여 작성하였으며 각 알고리즘 별 처리속도는 통상적으로 해쉬함수, 대칭키 암호화, 비대칭키 암호화 방식 순서로 빠르기를 가정하였으며, XOR연산은 포함하지 않는다.

비교결과 사용된 전체 알고리즘에서 현재 시스템과 확장 종단간 암호화 기술은 사용된 알고리즘이 같다. 반면 제안된 인증기법은 Hash함수가 2회 추가됨에 따라 시간손실이 발생하고 투채널 인증은 연산속도가 PC에 비해 떨어지는 스마트폰에서 전자서명이 이루어지기 때문에 시간 손실이 발생한다.

서버에서의 알고리즘 비교는 전체와 비교해서 차이가 많다. 이는 확장 종단간 암호화 기술이 키보드 보안 모듈에 의한 키보드 입력 값의 암호화를 서버에서 복호화하기 때문이다. 현재 시스템과 비교하였을 때 제안된 인증기법은 빠른 처리속도를 보이는 해쉬함수 1회가 사용된 반면 확장 종단간 암호화 기술과 기존에 제안된 투채널 인증의 경우 해쉬함수보다 느린 대칭키 암호화를 1회 사용된다. 따라서 서버에서 처리속도는 빠른 순서로 정렬하면 현재 시스템, 제안된 인증기법, 확장 종단간 암호화 순서로 나열할 수 있다.

VI. 결론

본 논문에서는 홈트레이딩 시스템 이용 시 메모리에 인증정보가 남는 취약점에 대해서 분석하였다. 그리고 분석 결과로부터 아이디, 로그인 비밀번호, 공인인증서 암호, 계좌비밀번호가 노출되는 것을 알 수 있었고, 휴대전화를 이용한 인증방법을 제시하였다. 온라인 주식거래에서 홈트레이딩 시스템이 자치하는 비중은 코스피의 경우 40%, 코스닥의 경우 70%에 달하지만 가용성 때문에 보안 솔루션 도입이 쉽지 않은 문제가 있다. 본 논문에서 제시된 주식거래 방법은 주식거래시 가용성을 최대한 보장하면서 인증정보가 노출되더라도 공격자의 부정거래를 막는데 초점을 두고 있다. 인증번호 보호를 위해 휴대전화를 이용한 투채널 인증을 사용하였고, 가용성을 보장하기 위해 인증코드 생성과 검증시 XOR과 해쉬함수를 이용하였다.

향후 연구로는 인증정보를 삭제하는 방식이 아닌 휴대전화를 통해 인증번호를 전송받고 인증코드를 생성하여 사용자 인증 그리고 메모리에 남아있는 인증정보를 이용한 주식거래 내용을 변조하는 공격에 대한 분석과 대응책 연구가 필요하며, 제안한 기법에서 사용된 SMS 인증 기법에 대한 안전성 분석이 필요하다.

참고문헌

[1] 양종곤, "주식거래, HTS'줄고' MTS'늘고," 서울파이낸스 2012. 3 뉴스, 2012.

[2] 이경원, "증권사 해킹, 알고 보니 '투자상담사'," etnews, 2010. 3 뉴스, 2010.

[3] 이윤영, "홈트레이딩 시스템 서비스의 보안 취약점 분석 및 평가기준 제안," 정보보호학회논문지, 18(1), pp 115-137, February. 2008.

[4] 금융보안연구원, "종단간(End-to-End) 암호화 적용 가이드," 금융보안연구원, October, 2007.

[5] Federal Information Processing Standards Publication 140-2, "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES," NIST, May, 2001.

[6] 김상균, "공개키인증 기반구조로서의 X.509에 대한 연구." 정보보호학회학회지, 8(3), pp 33-46, September. 1998.

[7] FFIEC,, "Authentication in an Internet Banking Environment," FFIEC. Decem-

ber. 2010,
〔8〕 NIST Special Publication 800-63-1, "Electronic Authentication Guideline, INFORMATION SECURITY," NIST, 2011, 12.
〔9〕 이원철, "전자금융거래시스템 취약점 분석 및 안전성 강화방안 연구," 정보보호학회학회지, 15(4), pp 43-48, August. 2005,
〔10〕 서승현, "OTP 기술현황 및 국내 금융권 OTP 도입 사례," 정보보호학회학회지, 17(3), pp 18-25, August. 2007,
〔11〕 정상각 "전자금융거래에서의 QR Code 기반 투-채널 인증기법의 제안," 석사학위논문, 고려대학교, December, 2010.
〔12〕 이용재 "이중채널을 이용한 안전한 사용자 인증 및 전자금융거래시스템에 관한 연구," 박사학위논문, 숭실대학교, December, 2011.
〔13〕 금융투자협회 증권 정회원 회원사 리스트 (http://www.kofia.or.kr/)
〔14〕 최윤성, "삭제된 공인인증서의 복구 및 개인키 암호화 패스워드의 검출," 정보보호학회논문지, 17(1), pp 41-55, February, 2007,
〔15〕 김종회, "GPU에서의 SEED암호 알고리즘 수행을 통한 공인인증서 패스워드 공격 위협과 대응," 정보보호학회논문지, 20(6), pp 43-50, December, 2010,
〔16〕 금융보안연구원, "금융부분 암호기술 관리 가이드," 금융보안연구원, January, 2010.

〈著者紹介〉

최 민 근 (Min Keun Choi) 학생회원
2009년 8월: 서원대학교 컴퓨터공학과 졸업
2011년 2월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 정보보호, 금융보안, 홈트레이딩 시스템, 소프트웨어 공학

조 관 태 (Cho, Kwantae) 학생회원
2005년 2월: 고려대학교 컴퓨터학과(학사)
2005년 3월~2008년 2월: 고려대학교 정보보호대학원(공학석사)
2008년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 WSN 보안, 기기간 보안 통신, 차량간 보안 통신, 키 교환

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학과(학사)
1987년 12월: Oklahoma University 전산학 대학원(공학석사)
1992년 5월: Oklahoma University 전산학 대학원(공학박사)
1992년 8월: 단국대학교 전자계산학과 전임강사
1993년 3월~1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월~2001년 2월 : 고려대학교 전산학과 부교수
2001년 2월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술