情報保護學會論文誌
第18卷 第1號, 2008. 2

홈트레이딩 시스템 서비스의 보안 취약점 분석 및 평가기준 제안*

이 윤 영†, 최 해 랑, 한 정 훈, 홍 수 민, 이 성 진, 신 동 휘, 김 승 주‡, 원 동 호
성균관대학교 정보통신공학부 정보보호연구소

Security Analysis on the Home Trading System Service and Proposal of the Evaluation Criteria*

Yunyoung Lee†, Haelahng Choi, Jeonghoon Han, Sumin Hong, Sungjin Lee
Donghwi Shin, Seungjoo Kim‡, Dongho Won
Information Security Group, School of Information and Communication Engineering, Sungkyunkwan University

요 약

증권시장이 커짐에 따라 홈트레이딩시스템(Home Trading System)을 이용한 증권거래가 활발해지고 있다. HTS는 주식 시세 조회를 비롯한 매매상담 등의 많은 기능을 제공하고 있다. 그러나 사용자의 편의성과 효용성을 중심으로 한 기능은 개발되고 적용되고 있지만 개인정보 및 거래의 안전성에 대한 보안기능은 미흡한 실정이다. 본 논문은 키로깅과 스니핑을 통해 HTS의 보안서비스를 분석하여 많은 개인정보가 노출됨을 설명한다. 그리고 취약점을 파악하여 HTS가 가져야할 바람직한 평가기준을 제시한다.

ABSTRACT

As stock market gets bigger, use of HTS(Home Trading System) is getting increased in stock exchange. HTS provides lots of functions such as inquiry about stock quotations, investment counsel and so on. Thus, despite the fact that the functions for convenience and usefulness are developed and used, security functions for privacy and trade safety are insufficient. In this paper, we analyze the security system of HTS service through the key-logging and sniffing and suggest that many private information is unintentionally exposed. We also find out a vulnerable point of the system, and show the advisable criteria of secure HTS.

Keywords : HTS, Home Trading System, Security Analysis

Ⅰ. 서 론

국내의 증권거래는 거래를 하기 위해 증권사로 직접 찾아가야했던 과거와는 달리, 가정용 투자정보시스템에서 발전된 HTS(Home Trading System)가 널리 보급되면서 빠른 속도로 성장하고 있다. HTS는 인터넷이 연결된 곳이라면 공간적 제약 없이 거래할 수 있는 등의 장점을 지니면서 사용자와 거래금액이 증가하고 있다. 그러나 HTS를 이용한 온라인 증권거래가 발달하면서

접수일: 2007년 7월 5일; 채택일: 2007년 11월 7일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음. (IITA-2007-C1090-0701-0028)
† 주저자, yylee@security.re.kr
‡ 교신저자, skim@security.re.kr

사용자의 편리성 및 효용성을 위한 기능이 개발되어 적용되고 있지만 개인정보의 보호 및 거래의 안전성을 위한 보안기능은 미흡한 실정이다.

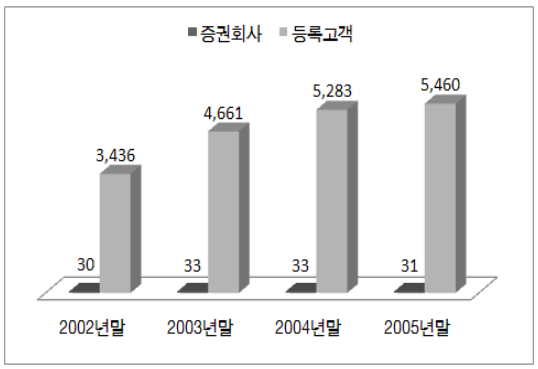
2005년 5월, 국내 첫 인터넷 뱅킹 해킹 사건 이후, 개인정보보호의 중요성이 높아지면서 금융기관은 보안솔루션을 도입하여 위협에 대응하고 있다. 그러나 HTS 접속을 위한 인증 및 서비스 이용과정에서, 보안솔루션이 설치가 되어 있어도 제대로 적용되지 않아 키로깅 및 스니핑을 통하여 아이디, 로그인 비밀번호, 공인인증서 암호 등의 개인정보가 노출되었다.

HTS에 적용된 보안서비스의 안전성을 조사하기 위해 28개 증권사의 보안서비스 취약점을 분석하였다. HTS 이용 시, 인증 및 서비스를 이용하는 과정에서 제공되는 보안서비스에 대해 보안솔루션의 제공 여부와 올바르게 적용되었는지에 초점을 맞추었으며, 키로깅은 2007년 7월 4일까지, 스니핑은 2007년 5월 2일까지 시도하여 개인정보노출에 대해 분석하였다. 그리고 HTS에서 제공되는 보안서비스의 문제점을 분석하여 HTS가 가져야할 바람직한 평가기준을 도출하였다.

본 논문의 2장에서는 HTS와 이용현황 및 문제점에 대해 살펴본다. 3장에서는 HTS에 적용된 보안 솔루션을 알아보고 인증과정과 서비스를 이용하는 동안 키로깅, 스니핑을 통해 노출된 개인정보를 알아본다. 4장에서는 HTS의 문제점을 분석하고 5장에서는 공통평가기준을 적용하여 HTS가 가져야할 평가기준을 도출한다. 그리고 6장에서 결론을 맺는다.

Ⅱ. 홈트레이딩 시스템

증권사를 찾아가 주식시세 조회, 매매 등을 할 수 있었던 예전과는 달리, HTS가 개발되어 인터넷이 연결된 곳이라면 어디서든지 증권거래를 할 수 있게 되었다. 주식시세 조회를 위해 제공되었던 가정용 투자정보시스템에서 발전된 HTS는 2000년대에 들어서서 주식시세 조회를 비롯하여 매매상담, 특정 조건에 대한 자동매매 등의 여러 기능이 추가되면서 온라인 증권 발전에 많은 영향을 끼치고 있다. HTS는 인터넷이 연결된 곳이라면 공간의 제약 없이 거래할 수 있다는 점과 매매수수료가 저렴하다는 등의 장점을 가지면서 널리 이용되고 있다. [그림 1]에서 보는 것과 같이 HTS 등록 고객 수는 2002년 말 343만여 명에서 2005년 말 546만여 명으로 꾸준히 증가하고 있고 [표 1]에서 보는 것과 같이 조회, 자금이체, 주식매매 등의 이용실적도 증가하고 있다.[1] 이렇게 HTS를 이용한 온라인 증권거래 및 인터넷 뱅킹 등의 인터넷 금융거래가 활발해지면서 이용자의 편의성이나 효용성을 위한 기능들은 많이 개발되어 적용되고 있지만 이용자의 개인정보보호를 위한 보안기능은 미흡한 실정이다. 그 예로 2005년 5월, 해킹 프로그램을 설치해 인터넷 뱅킹 비밀번호 등을 알아낸 뒤 은행계좌에서 거액을 인출해가는 첫 인터넷 뱅킹 해킹 사건이 발생하였고 2007년 2월, 간단한 개인정보(로그인 정보와 주민등록번호)의 노출을 통한 공인인증서 해킹으로 한 사용자가 5천만 원의 금전적 손해를 입은 피해가 일어나 사용자의 우려를 완전히 해소시키지 못하고 있다.[2][3] 나날이 증가하는 해킹 위협에 인터넷 뱅킹뿐만이 아니라 HTS 서비스의 경우도 예외일 수는 없다. HTS를 이용함에 있어서 이용자의 개인정보가 오가고 거래의 안전성이 중요하기 때문에 그에 대한 보안도 중



[그림 1]. HTS 등록 고객 수(단위 : 천명)

[표 1]. HTS 이용실적 (단위 : 건)

년도	이용실적				
	계	조회	자금 이체	주식매 매주문	기타
2002	5,073,756	4,701,039	3,898	339,502	4,266
2003	5,242,146	4,668,190	4,519	521,506	5,597
2004	5,278,736	5,035,674	2,001	239,501	1,599
2005	6,936,433	6,582,881	4,463	346,532	2,557

요시 되고 있지만 증권거래의 경우 1분, 1초의 지연으로 인한 피해가 막심하다는 특징을 갖고 있어 보안 솔루션의 도입에 많은 어려움이 발생하고 있다. 이용자의 뒤쳐진 보안 의식도 문제이지만, 모든 보안을 고려할 수 없고 효과에 비해 과다한 비용이 필요할 경우 구축을 꺼리는 증권사의 입장으로 인해 현재 이용되고 있는 HTS가 많은 위협에 노출되어 있는 것이 지금의 현실이다.

Ⅲ. 홈트레이딩 시스템 취약점 분석

2장에서 살펴본 바와 같이 HTS 서비스, 인터넷 뱅킹 등의 인터넷 금융거래의 규모가 꾸준히 증가함에 따라 그 위협이 증가하였고 금융기관에서는 개인정보의 보호를 위해 보안솔루션을 구축하여 보안서비스를 제공하고 있다.

본 장에서는 국내 온라인 증권거래에서 제공하고 있는 보안서비스와 HTS에 대한 개인정보노출을 분석하기 위해 스니핑은 2007년 5월 2일, 키보드해킹은 2007년 7월 4일 오후 8시까지 현재 국내의 28개 증권사를 조사하였다. 조사 증권사 선정기준은 HTS 이용자들에게 많이 알려진 증권사를 중심으로 네이버에 등록되어 있는 증권사 목록 검색을 통해 이루어졌다. 각 증권사 HTS의 사용자 인증과정과 증권 서비스를 이용하는 동안 보안솔루션을 적절히 제공하고 적용하는지에 초점을 맞추어 키보드해킹과 스니핑을 통한 개인정보노출에 대해 분석하였다. 낮은 공격수준을 가지고도 쉽게 공격할 수 있게 하기 위하여 인터넷 상에서 쉽게 구할 수 있는 Netbus, SKin2000, Ethereal, Commview 프로그램을 분석을 위한 툴로 선정하였다. 키보드해킹은 Netbus와 SKIn2000 프로그램을 사용하여 HTS를 이용 시, 이용자의 키보드 입력 정보가 노출되는지 조사하였고, 스니핑은 Ethereal과 Commview 프로그램을 사용하여 이용자가 HTS를 이용할 때 전송되는 정보가 노출되는지 조사하였다.

HTS에 적용된 보안 솔루션은 크게 키보드보안솔루션, 웹보안솔루션, 그리고 해킹차단솔루션으로 나눌 수 있다. 키보드보안솔루션은 개인정보 입력의 최초 수단인 키보드 단계에서부터 서비스 전 구간에 걸쳐 시행되는 보안솔루션으로 키보드를 통해 입력되는 개인의 중요 정보, 아이디, 패스워드, 계좌 번호, 카드 번호 등을 키보드 드라이버 레벨에서 암호화하여 키로거(Key Logger) 프로그램 등의 공격에 의해 중요 정보가 유출되는 것을 근본적으로 차단하는 기능을 제공한다.[4] 웹보안솔루션은 불안전한 데이터 채널 상에서 암호 체계를 이용하여 통신망 내의 두 지점 간에 안전하게 정보를 송수신하는 기능을 제공하고 해킹차단솔루션은 이용자 컴퓨터를 조사하여 알려진 해킹 툴을 검색하여 삭제하고 침입 탐지 및 차단 기능을 제공한다.[4]

HTS에 적용되는 보안솔루션은 증권사의 홈페이지에서 설치한 보안솔루션을 이용하거나 HTS 실행 시, 주식 정보 등을 업데이트하면서 보안솔루션을 같이 설치하기 때문에 트레이 아이콘이 생성되어 확인할 수 있는 것 이외에는 정확히 어떤 보안 솔루션을 제공하는지에 대한 정보가 없다. 따라서 키로깅과 스니핑을 통해 아이디, 패스워드 등의 개인정보노출 여부에 초점을 맞췄다.

3.1. 분석 환경 및 방법

3.1.1. 분석 환경

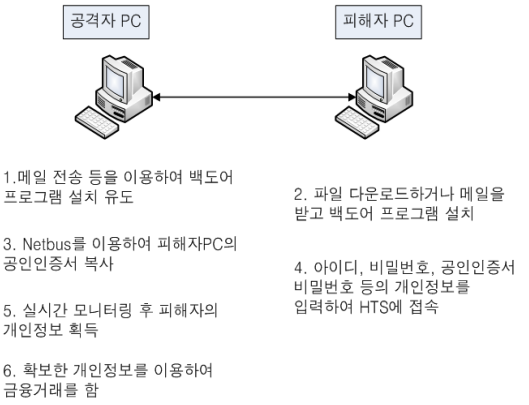
각 증권사가 제공하는 보안서비스의 취약점을 분석하기 위해 [표 2]와 같은 환경을 구축하였다. 제공하는 보안솔루션이 사용자 환경에 따라 영향을 받을 것을 감안하여 피해자 PC를 2대를 두고 운영체제를 다르게 하여 다양성을 주었다. 보안솔루션의 적용과 HTS 자체를 분석하기 위하여 모든 PC에는 백신 프로그램은 설치되어 있지 않다.

3.1.2. 분석 방법

[표 2]. 분석 환경

	CPU	Memory	OS
공격자 PC	Pentium4 3.2GHz	1.00GB	Windows XP Professional Version 2002 Service Pack 2
피해자 PC1 (데스크탑)	Intel Core(TM) 2 CPU 6400 2.13GHz	1.00GB	Windows XP Professional Version 2002 Service Pack 2
피해자 PC2 (노트북)	Intel Pentium M Processor 1.2GHz 600MHz	504MB	Windows XP HomeEdition Version 2002 Service Pack 2

본 절에서는 HTS의 취약점을 분석하기 위하여 실행한 공격 방법에 대해서 알아보도록 하겠다. 공격자는 Netbus에서 제공하는 백도어(Back Door)프로그램을 압축하여 그림 파일이나 멀티미디어 파일 등과 패킹(Packing)을 한다. 패킹한 백도어 프로그램 파일을 메일 전송이나 메신저를 이용한 파일 전송 등을 이용하여 피해자 PC에 설치하도록 유도한다. 패킹이 되어있기 때문에 피해자는 백도어 프로그램을 인식하지 못하고 자신의 PC에 백도어 프로그램을 설치한다. 대부분의 사용자가 공인인증서를 PC에 저장하고, NPKI 폴더 등에 공인인증서가 저장되어 있어 공격자는 Netbus를 이용하여 피해자 PC에서 공인인증서를 다운로드하고 피해자 PC를 감시한다. 그 후 피해자가 HTS를 실행하여 개인정보를 입력하면 공격자는 이 정보를 획득하여 확보한 개인정보를 이용하여 금융거래를 시도한다. 위의 내용을 도식화하면 [그림 2]와 같다



[그림 2]. 공격 시나리오

3.1.3. 사용 프로그램 분석

[표 3]은 알려진 키보드 해킹 프로그램들을 분석한 것이다. 각각의 키보드 해킹 프로그램에 대해 Hide/Stealth, Keylogging, Screen shot, Websites visited, Clipboard, Applications, Sending E-mail 기능을 조사하였다. Hide/Stealth는 키보드 해킹 프로그램이 실행됨을 알 수 없게 하는 기능을, Keylogging은 키보드를 입력했을 때, 마우스를 클릭한 것과 마우스를 클릭한 곳에 있는 내용, Text form edit contorol의 내용을 가로채는 기능을 나타낸다. Screen shot은 주기적으로 현재 화면을 캡처하는 기능을 나타내고 Websites visited는 방문한 웹사이트가 어디였는지를 알려주는 기능, Clipboard

[표 3]. 알려진 Keylogging 프로그램 분석 (△ : Hide 기능은 있으나, 항상 Tray Icon으로 표시됨)

기능 / 이름	Hide/ Stealth	Key logging (Keyboard)	Key logging (Mouse)	Key logging (Edit Control)	Screen shot	Websites Visited	Clip board	Applications (Run or Exit)	Sending E-mail
SKin2000 v6.0	○	○	○	○	×	×	×	○	×
SC-KeyLog PRO v3.2	○	○	○	×	×	×	○	○	○
Active Key Logger v3.7.3	○	○	×	×	×	○	×	×	×
Key spyware v1.855	○	○	○	×	○	×	×	×	○
PC Spy Keylogger v2.34	○	○	×	×	○	×	○	×	○
KGB Keylogger v4.04	△	○	○	×	○	○	○	○	○
Actual Keylogger v2.4	○	○	×	×	○	○	○	○	○
Keystroke Spy v1.10	○	○	×	×	×	×	×	×	○

는 클립보드에 저장된 내용을 가로채는 기능을 나타낸다. Applications은 실행한 프로그램이 무엇인지, 프로그램 경로가 어디인지 등을 알려주는 기능을 하고 Sending E-mail은 위에 나타난 기능들에 의해 수집한 데이터들을 E-mail로 보내주는 기능을 한다. 자세한 내용은 각 키보드 해킹 프로그램의 매뉴얼을 참조하였다. SKin2000의 경우, 추가적으로 Dialog Box 같은 윈도우를 사용하는 부분을 메모리에서 읽어와 접근하는 Edit Control 기능이 있어 키로깅 툴로 선정하였다.

스니핑은 이더넷의 특징을 이용한다. 이더넷은 CSMA/CD 프로토콜을 사용하며, 로컬 네트워크에 연결되어 있는 모든 호스트들이 회선을 공유한다.[5] 그러므로 같은 네트워크에 속해있는 호스트들은 회선을 통해 전송되는 트래픽을 전부 볼 수 있다. 하지만 전송되는 트래픽들을 전부 본다면 CPU에 인터럽트가 많이 발생하여 부하가 많이 걸려 비효율적이다. 이를 해결하기 위하여 NIC(Network Interface Card)는 자신의 고유한 MAC(Media Access Control) 주소를 갖고 있어 프레임에 명시된 MAC 주소와 자신의 MAC 주소를 비교하여 다르면 프레임을 버리고, 같다면 CPU에 인터럽트를 발생시키는 것이다. 하지만 로컬 네트워크 내의 모든 트래픽을 볼 수 있도록 설정을 바꿔서 자신의 PC에 모든 트래픽을 받아드리게 할 수 있다.[6] 이렇게 받아들인 트래픽을 패킷 캡처 프로그램을 이용하여 전송되는 패킷을 붙잡아 악의적인 의도로 그 안의 데이터를 훔쳐보는 것이 스니핑이다. 키보드 해킹 프로그램과는 달리, Ethreal, Commview 등 알려진 많은 패킷 캡처 프로그램은 거의 동일한 수준의 기능을 제공하므로 세분화하여 분석하지 않았다.

3.2. HTS 서비스 개인정보노출

[표 4]. 증권사 리스트

증권사
교보증권, 굿모닝신한증권, 대신증권, 대우증권, 대한투자증권, 동양종합금융증권, 리딩투자증권, 메리츠증권, 미래에셋증권, 부국증권, 비엔지증권, 삼성증권, 서울증권, 신영증권, 우리투자증권, 유화증권, 이트레이드증권, 코리아RB증권, 키움닷컴증권, 푸르덴셜투자증권, 한국투자증권, 한양증권, 한화증권, 현대증권, BRIDGE증권, CJ투자증권, NH투자증권, SK증권

[표 5]. 각 증권사의 HTS 버전

증권사	버전
굿모닝신한증권	12.0.0.49974
대우증권	5.0.62
동양종합금융증권	5.0
리딩투자증권	2.11.15.0
서울증권	1.0
신영증권	2.1.13.0
한양증권	1.0
CJ투자증권	1.10
SK증권	7.3.0.3

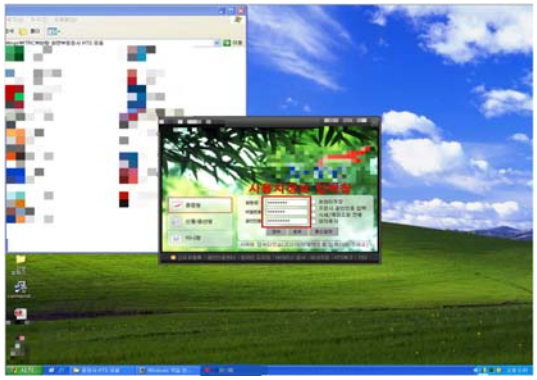
HTS의 보안서비스를 분석하기 위해 위에서 설명한 공격 시나리오를 가지고 국내 28개 증권사의 HTS를 조사하였다. 조사한 증권사 리스트는 [표 4]와 같고 HTS의 버전은 [표 5]와 같으며 명시되지 않은 경우 생략을 하였다.

3.2.1. 키로깅을 통한 개인정보노출

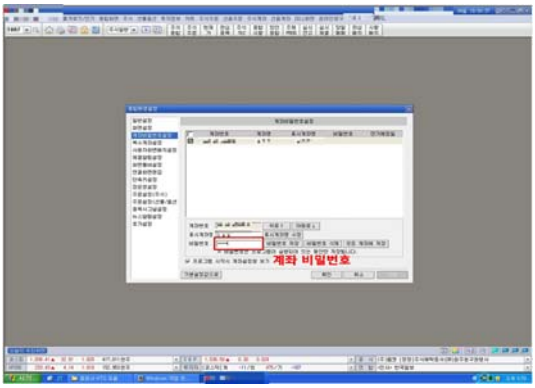
HTS의 키보드보안솔루션의 경우 키보드보안솔루션이 설치가 되어도 제대로 적용되지 않거나 설치가 되어 실행이 되고 있어도 키로깅이 가능한 경우가 있었고 키보드보안솔루션을제공하지 않는 경우도 있었다. 노출되는 개인정보의 유형에 따라 분류하면 다음과 같다.

◉ 아이디, 로그인 비밀번호, 공인인증서 암호, 계좌비밀번호가 노출되는 경우

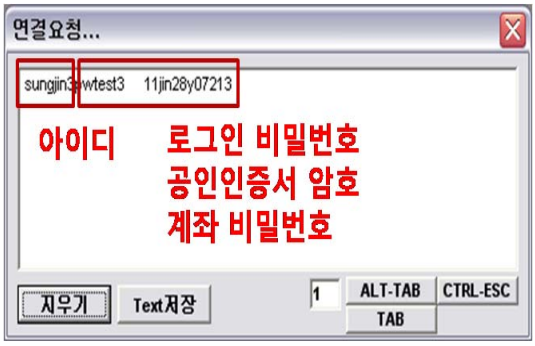
J증권, K증권, M증권의 경우 아이디, 로그인 비밀번호, 공인인증서 암호, 계좌비밀번호가 노출되었다. 이 증권들은 노출된 개인정보를 가지고 로그인이 가능했으며 Netbus로 복사한 공인인증서를 이용하여 증권거래까지 가능하다. J증권과 K증권은 HTS 실행 시 [그림 3]과 같이 트레이 아이콘으로 동작하는 보안솔루션은 없었으며 이용자의 개인정보를 입력하는 과정에서 개인정보가 [그림 5]와 같이 노출되었다. [그림 4]에서 이용자가 서비스를 이용하는 과정 중 입력한 계좌비밀번호도 [그림 5]와 같이 그대로 노출되었다.



[그림 3]. K증권 사용자정보(아이디, 로그인 비밀번호, 공인인증서 암호) 입력창



[그림 4]. K증권 계좌 비밀번호 입력창



[그림 5]. K증권 아이디, 로그인 비밀번호, 공인인증서 암호, 계좌 비밀번호 노출

M증권은 HTS 실행 시 [그림 6]과 같이 키보드 보안 프로그램 구동 중이라는 메시지가 출력되면서 Ahnlab Smart Update를 실시한 후, 잠깐 MyKeydefense가 트레이 아이콘으로 표시되었다가 사라졌다. 다시 수동 설

[그림 6]. M증권 HTS 구동시 첫 화면

[그림 7]. M증권 사용자정보(아이디, 로그인 비밀번호, 공인인증서 암호) 입력창

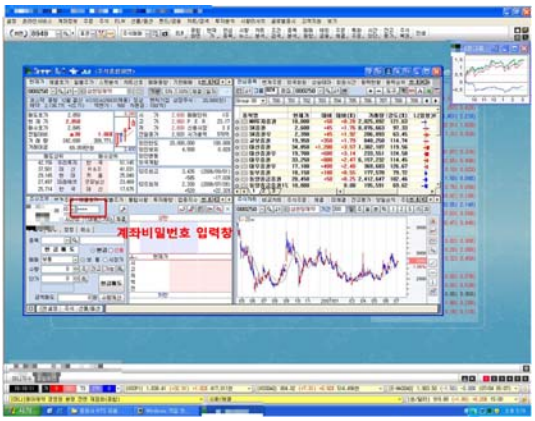
치를 하여도 똑같은 상태로 머물러 제대로 설치가 되지 않았고 이 상태에서 [그림 7]과 같이 서비스를 이용 시 이용자의 개인정보를 입력하는 과정에서 개인정보가 [그림 9]와 같이 노출되었다. [그림 8]에서 이용자가 서비스를 이용하는 과정 중 입력한 계좌비밀번호도 [그림 9]와 같이 그대로 노출되었다.

◉ 아이디, 계좌비밀번호가 노출되는 경우

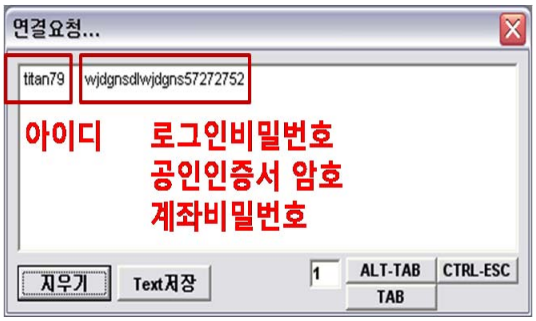
R증권의 경우 [그림 10]에서 이용자의 개인정보를 입력하는 과정에서 아이디와 [그림 11]에서 HTS 서비스를 이용하는 중 입력한 계좌비밀보호가 [그림 12]에서처럼 노출되었다.

◉ 아이디, 공인인증서 암호가 노출되는 경우

S증권의 경우 [그림 13]과 같이 이용자의 개인정보를



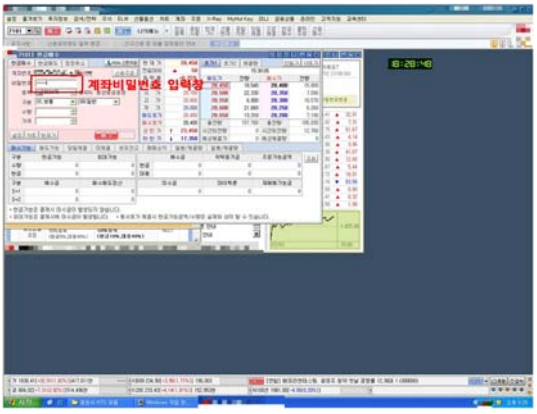
[그림 8]. M증권 계좌비밀번호 입력창



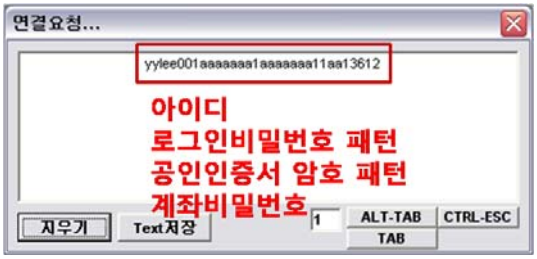
[그림 9]. M증권 아이디, 로그인 비밀번호, 공인인증서 암호, 계좌 비밀번호 노출

[그림 10]. R증권 사용자정보(아이디, 로그인 패스워드, 공인인증서 암호) 입력창

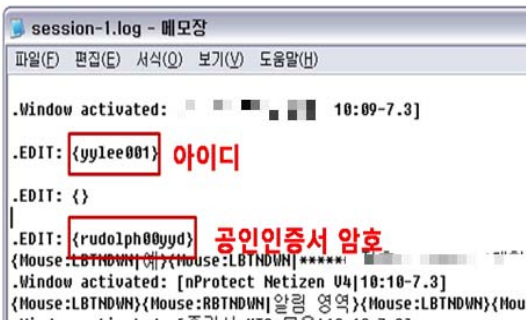
입력하는 과정에서 아이디와 공인인증서 암호가 노출되었다.



[그림 11]. R증권 계좌비밀번호 입력창



[그림 12]. R증권 아이디, 로그인 비밀번호 패턴, 공인인증서 암호 패턴, 계좌비밀번호 노출



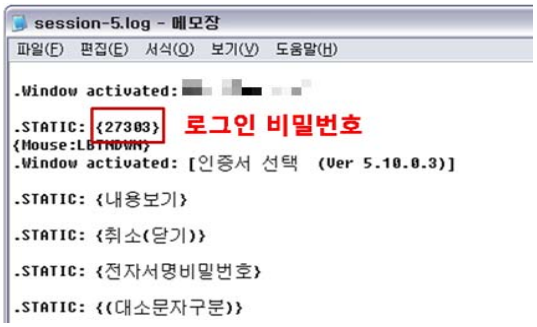
[그림 13]. S증권 아이디, 공인인증서 암호 노출

◉ 로그인 비밀번호가 노출되는 경우

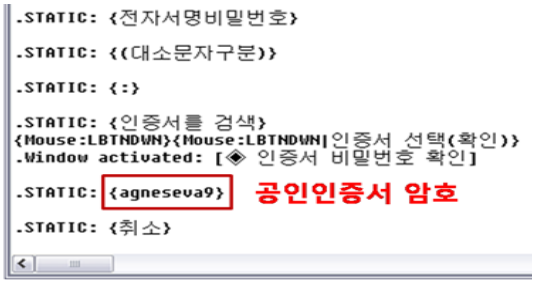
G증권의 경우 [그림 14]와 같이 이용자의 개인정보를 입력하는 과정에서 로그인 비밀번호가 노출되었다.

◉ 공인인증서 암호가 노출되는 경우

L증권의 경우 [그림 15]와 같이 공인인증서 암호가 노출되었다.



[그림 14]. G증권 로그인 비밀번호 노출



[그림 15]. L증권 공인인증서 암호 노출

[그림 16]. P증권 사용자정보(아이디, 로그인 비밀번호, 공인인증서 암호) 입력창

[그림 17]. P증권 아이디 노출

◉ 아이디가 노출되는 경우

D증권, P증권, AA증권, BB증권의 경우 [그림 17]과 같이 아이디가 노출되었다.

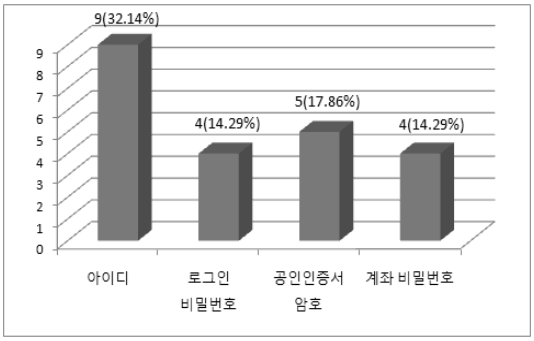
◉ 기타

I증권은 로그인이 성공하면 개인정보가 노출되지 않지만 잘못된 로그인 정보를 입력하거나, 장기간 거래를 하지 않아 사용정지가 되어 오류 메시지를 출력하는 경우 아이디, 로그인 비밀번호, 공인인증서 암호가 노출되었다.

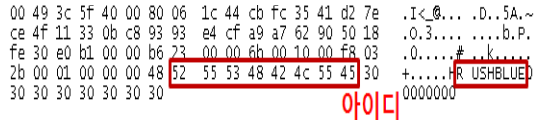
키로깅을 통해 노출된 개인정보별 증권사의 통계는 [그림 18]과 같다. 로그인 비밀번호, 공인인증서 암호, 계좌 비밀번호 등은 노출되어서는 안 되는 개인정보임에도 불구하고 각각 14.29%, 17.86%, 14.29%가 노출이 되었다. [표 6]은 키보드해킹을 통한 증권사별 노출정보를 나타낸다.

[표 6]. 증권사별 키보드해킹을 통한 노출정보(△:기타 참조)

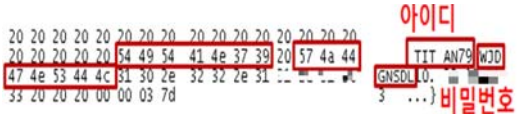
증권사	키보드해킹			
	아이디	로그인 비밀 번호	공인 인증서 암호	계좌 비밀 번호
A증권	×	×	×	×
B증권	×	×	×	×
C증권	×	×	×	×
D증권	○	×	×	×
E증권	×	×	×	×
F증권	×	×	×	×
G증권	×	○	×	×
H증권	×	×	×	×
I증권	△	△	△	×
J증권	○	○	○	○
K증권	○	○	○	○
L증권	×	×	○	×
M증권	○	○	○	○
N증권	×	×	×	×
O증권	×	×	×	×
P증권	○	×	×	×
Q증권	×	×	×	×
R증권	○	×	×	○
S증권	○	×	○	×
T증권	×	×	×	×
U증권	×	×	×	×
V증권	×	×	×	×
W증권	×	×	×	×
X증권	×	×	×	×
Y증권	×	×	×	×
Z증권	×	×	×	×
AA증권	○	×	×	×
BB증권	○	×	×	×
계	9	4	5	4



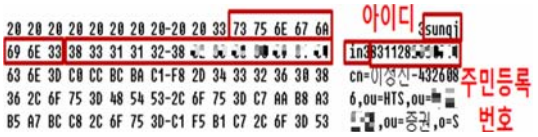
[그림 18]. 온라인 증권거래의 키보드해킹 정보별 노출



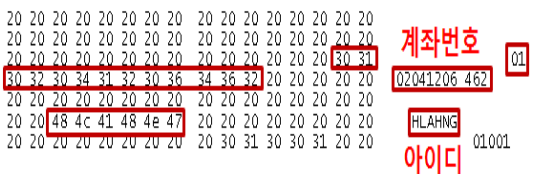
[그림 19]. B증권 아이디 노출



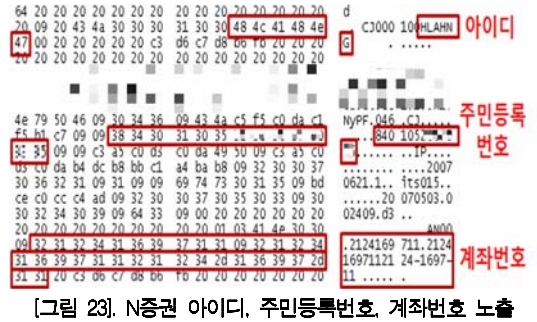
[그림 20]. A증권 아이디, 로그인 비밀번호 노출



[그림 21]. K증권 아이디, 주민등록번호 노출



[그림 22]. L증권 아이디, 계좌번호 노출



[그림 23]. N증권 아이디, 주민등록번호, 계좌번호 노출

3.2.2. 스니핑을 통한 개인정보노출

스니핑의 경우 키로깅보다 개인정보노출이 적었지만 웹보안솔루션이 제대로 적용되지 않거나 제공되지 않는 경우도 있었다. 노출되는 개인정보의 유형에 따라 분류하면 다음과 같다.

◉ 아이디가 노출되는 경우

B증권, G증권, I증권, M증권, P증권, Q증권, S증권, T증권, U증권, W증권, X증권, Y증권, AA증권, BB증권의 경우 [그림 19]와 같이 피해자의 아이디가 노출되었다.

◉ 아이디, 로그인 비밀번호가 노출되는 경우

A증권, D증권, E증권, F증권, H증권의 경우 [그림 20]과 같이 피해자의 아이디와 로그인 비밀번호가 노출되었다.

◉ 아이디, 주민등록번호가 노출되는 경우

K증권, R증권의 경우 [그림 21]과 같이 피해자의 아이디와 주민등록번호가 노출되었다.

◉ 아이디, 계좌번호가 노출되는 경우

L증권의 경우 [그림 22]와 같이 피해자의 아이디와 계좌번호가 노출되었다.

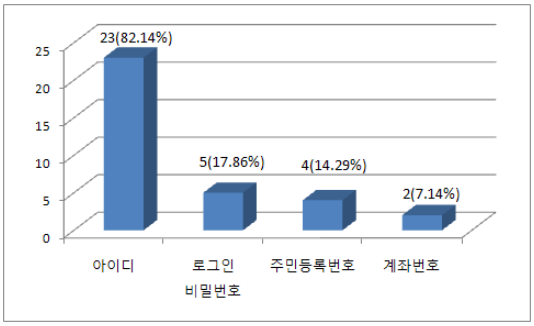
◉ 아이디, 계좌번호, 주민등록번호가 노출되는 경우

N증권의 경우 [그림 23]과 같이 피해자의 아이디, 주민등록번호, 계좌번호가 노출되었다.

스니핑을 통해 노출된 개인정보별 증권사의 통계는 [그림 24]와 같다. 로그인 비밀번호, 주민등록번호 등은 노출되어서는 안 되는 개인정보임에도 불구하고 각각 17.86%, 14.29%의 HTS에서 노출이 되었다. [표 7]은 스니핑을 통한 증권사별 노출정보를 나타낸다.

Ⅳ. 홈트레이딩 시스템의 취약점에 대한 원인 분석

위에서 살펴본 바와 같이 국내 HTS 이용 시, 개인정보보호를 위한 보안서비스가 제대로 이루어지지 않아 여러 정보가 노출되었다. 키보드보안프로그램의 경우



[그림 24]. HTS의 스니핑 정보별 노출

[표 7]. 증권사별 스니핑을 통한 노출정보

증권사	스니핑			
	아이디	로그인 비밀 번호	주민 등록 번호	계좌 번호
A증권	○	○	×	×
B증권	○	×	×	×
C증권	×	×	×	×
D증권	○	○	×	×
E증권	○	○	×	×
F증권	○	○	×	×
G증권	○	×	×	×
H증권	○	○	×	×
I증권	○	×	×	×
J증권*	×	×	×	×
K증권*	○	×	○	×
L증권	○	×	×	○
M증권*	○	×	×	×
N증권	○	×	○	○
O증권	×	×	×	×
P증권	○	×	×	×
Q증권	○	×	×	×
R증권	○	×	○	×
S증권	○	×	×	×
T증권	○	×	×	×
U증권	○	×	×	×
V증권	×	×	×	×
W증권	○	×	×	×
X증권	○	×	○	×
Y증권	○	×	×	×
Z증권	×	×	×	×
AA증권	○	×	×	×
BB증권	○	×	×	×
계	23	5	4	2

개인정보가 노출되지 않아도 [그림 25]와 같이 개인정보의 패턴을 노출시키는 경우가 많았다. 암호화된 정보를 보면 문자는 'a', 숫자는 '1'로 변환된다. 이렇게 패턴이 노출될 경우 패스워드 검출 프로그램을 이용한 Dictionary Attack과 Mask Attack 등에 취약하다. 이 장에서는 HTS 이용 시 개인정보가 노출되었던 원인을 살펴본다. 이 장에서는 그림과 표의 형식에 대하여 설명하겠습니다.

4.1. 개인정보노출의 원인

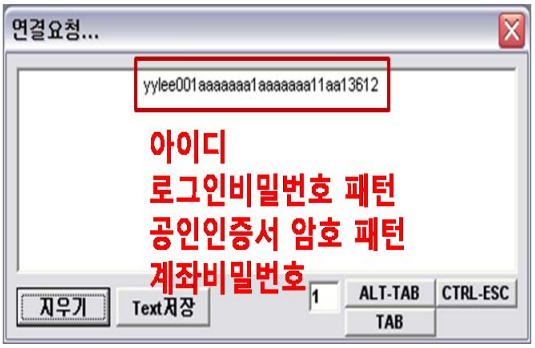
HTS 이용 시, 키로깅, 스니핑에 의해 개인정보가 노출되는 원인은 보안솔루션을 제공하지 않거나, 보안솔루션을 제공하여도 제대로 적용되지 않아 그 기능이 작동하지 않는 경우, 사용자 인증 후 보안솔루션을 적용하는 경우, 공인인증서의 저장위치 노출 이렇게 네 가지로 나눌 수 있다.

• 보안솔루션을 제공하지 않는 경우

증권사는 HTS를 제공함에 있어서 이용자의 개인정보 노출을 막기 위해 보안솔루션을 제공해야 한다. 대부분의 HTS가 어떤 보안솔루션을 제공하는지 명시하지 않았으며 이용자에게 주는 경고메시지도 존재하지 않았다.

• 보안솔루션을 제공하여도 제대로 적용되지 않아 그 기능이 작동하지 않는 경우

보안솔루션을 적용함에 있어서 적용되는 범위가 달라 개인정보가 노출되었다. 즉, 서비스 전체에 보안솔루션을 적용하지 않고 특정 메시지 창이나, 필드에 부분 적용하여 Security Hole이 생겼다.



[그림 25]. 개인정보에 대한 패턴 노출

• 사용자 인증 후 보안 솔루션을 적용하는 경우

HTS 접속 이전에, 필요한 모든 보안솔루션이 적용되어 실행이 되어야한다. 즉 보안솔루션이 적용되는 시점이 잘못되고 HTS 접속 시, 모든 동작이전에 HTS가 제공하는 보안솔루션이 제대로 작동하는지 확인하지 않아 개인정보가 노출되었다. 보안솔루션이 제대로 동작하지 않는다면 서비스를 제공해서는 안 된다.

• 공인인증서의 저장위치 노출

대부분의 HTS 이용자는 공인인증서를 PC에 저장하고 있다. 그러나 PC에 저장된 공인인증서는 저장되는 위치가 NPKI 폴더 등으로 노출되어 여전히 취약하다.[7]

Ⅴ. 안전한 홈트레이딩시스템을 위한 CC기반 평가기준

위에서 살펴본 바와 같이 보안 솔루션이 설치됨에도 불구하고 HTS에서 개인정보의 노출이 발생하고 있다. 이러한 문제의 원인은 HTS의 설계 및 개발 과정에서 보안기능에 대한 고려가 부족하였기 때문이다.

본 장에서는 이러한 문제의 원인을 해결하기 위해 HTS의 평가기준을 제시하여 설계 및 개발과정에서부터 보안기능을 적용할 수 있도록 한다. HTS의 평가기준을 도출하기 위해 ISO/IEC 15408 표준에 따른 공통평가기준 v3.1과 공통평가방법론 v3.1을 이용하며, 평가기준 도출 방법은 보호프로파일 및 보안목표명세서 작성 가이드를 참조한다.[9]

따라서 본 장에서는 HTS의 운영환경 및 보안기능을 정의하고, 앞에서 분석한 취약성을 통해 위협을 추출한다. 또한, HTS의 모든 보안기능에 대한 안전한 구현을 위해 본 논문의 취약점에서 도출된 위협 외에 HTS의 보안기능에 위협이 될 수 있는 사항들을 도출한다. 그리고 추출한 위협을 해결하기 위한 보안목적을 제안하고, 제안한 보안목적을 명세화 함으로써 평가기준을 제시한다.

5.1. HTS 설명

5.1.1. HTS 운영환경

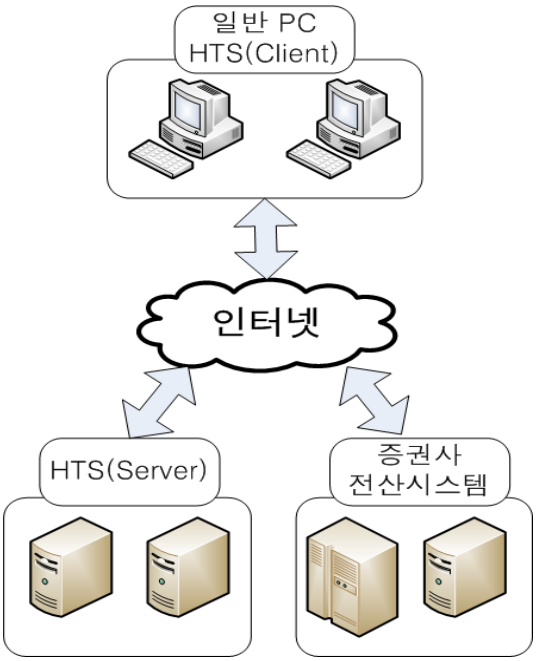
HTS는 클라이언트 프로그램과 서버 프로그램으로 구성된다. HTS 클라이언트는 HTS 서버에 식별 및 인증을 통해 접속하여 증권 거래 서비스를 제공받는다. HTS 서버는 HTS 클라이언트의 서비스 요청에 대한 응답을 제공하고, 관련 정보에 대한 관리 및 감시, 제어 기능을 수행한다. 증권사 전산 시스템은 실제 증권 거래를 담당한다. 따라서, HTS 클라이언트가 실제 증권 거래 요청 시, HTS 서버는 관련 정보에 대한 관리, 감시, 제어 기능을 하며, 실제 거래와 결제는 증권사 전산 시스템과의 연결을 통해 이루어진다. 안전한 시스템 운영을 위해 HTS 클라이언트, HTS 서버, 증권사 전산 시스템은 각각 접근통제, 사용자 식별 및 인증, 보안 통신 등의 보안기능을 제공한다.

5.1.2. HTS 보안기능

HTS는 다음과 같은 보안기능을 갖는다.

• 식별 및 인증

HTS 서버는 서버를 관리하는 관리자와 HTS 클라이언트를 통해 접속하는 회원을 식별 및 인증한다.
HTS 클라이언트는 HTS 서버로부터 회원의 정보를 통해 회원의 식별 및 인증을 받는다. 또한, 회원의 증권 거래를 위한 결제 정보에 대해 증권사 전산 시스템으로부터 식별 및 인증을 받는다.



[그림 26]. HTS 운영환경

• 감사

HTS 서버는 인가받은 회원의 접속에 대한 감사 정보를 저장하고, 정상적으로 접속하는지 감시한다. HTS 클라이언트는 회원의 HTS 서버로 인증된 접속을 하는지 감시하고, 감사 정보를 저장한다. 또한, 인가받은 회원의 증권 거래에 대하여 안전한 거래인지 감시하며, 감사 정보를 남긴다. 증권사 시스템 장애 발생 시에는 사건에 대한 감사 정보를 남긴다.

• 관리

HTS 서버는 HTS에 등록한 회원 정보 및 회원의 증권 거래 정보를 입력받아 데이터베이스에 안전하게 저장하고 관리한다. HTS 클라이언트는 회원이 사용하는 PC에 저장되는 회원의 개인 정보 및 회원의 증권 거래 정보를 관리하며, 클라이언트 프로그램의 버전을 관리하여 자동으로 서버로부터 설치 프로그램을 다운받아 업데이트를 수행한다. HTS 서버와 클라이언트는 정확한 운영과 정보 기록을 위해 신뢰할 수 있는 타임스탬프를 제공한다.

• 보안통신

HTS 서버는 HTS 클라이언트나 증권사 전산 시스템과 안전한 보안 통신을 한다. HTS 클라이언트는 HTS 서버나 증권사 전산 시스템과 안전한 보안 통신을 한다.

• 키보안

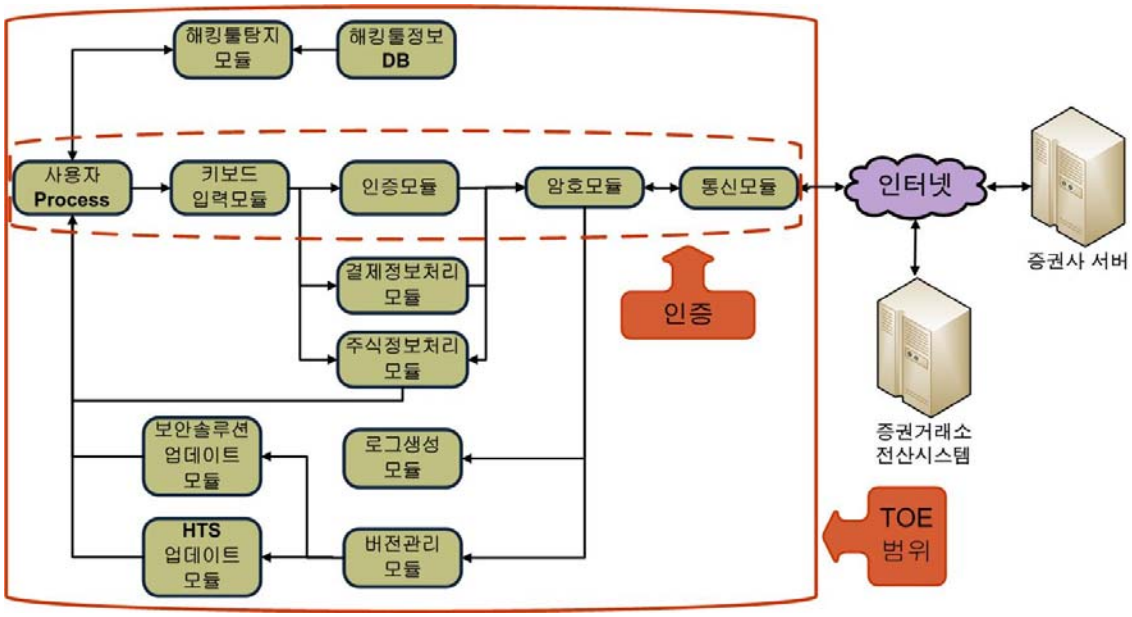
HTS 서버와 클라이언트는 보안 통신 및 데이터 보호를 위해 암호화를 수행하며, 암호화를 위해 키를 안전하게 관리한다.

• 해킹방지

HTS 클라이언트는 사용자 입력 정보를 안전하게 받고, HTS 서버로 안전하게 전송하며, 사용자 PC에 안전하게 저장하기 위해 해킹을 방지하는 기능을 제공한다. 이 기능은 키로깅이나 백도어 프로그램 등의 해킹 툴을 탐지 및 제거한다.

5.2. 위협

평가기준을 적용할 HTS의 평가 범위로 HTS의 보안 기능인 식별 및 인증, 감사, 관리, 보안통신, 키관리, 해킹방지 등이 포함된다. 평가 범위 내의 HTS가 가질 수 있는 모든 위협을 도출하기 위해 보호할 자산을 추출하고, 자산을 손상시키는 위협원을 파악하여, 앞에서 서술한 HTS의 취약성과 위협원의 자산에 대한 공격방법을



[그림 27]. HTS의 보안기능 및 평가범위

통해 위협을 도출한다.[9]

5.2.1. 보호해야할 자산

자산은 TOE에 의해 보호되는 정보나 자원이다.[10] HTS에서는 개인정보가 중요한 자산이 된다. HTS가 보호해야 할 개인정보는 저장 정보, 입력 정보, 전송 정보 등 세 가지로 분류한다.

- 저장 정보 : 사용자 PC에 저장된 사용자의 공인인증서 및 HTS에 로그인하기 위한 아이디와 비밀번호 등의 정보
- 입력 정보 : 사용자가 HTS 서버로부터 인증받기 위해 입력하는 정보로서 HTS 로그인 아이디와 비밀번호, 공인인증서 비밀번호, 계좌 비밀번호 등이 포함
- 전송 정보 : HTS 서버와 HTS 클라이언트의 통신을 통해 전송되는 정보로 HTS 로그인 아이디와 비밀번호, 계좌번호, 주민등록번호 등으로 이루어짐

이러한 개인정보가 유출될 경우, 사용자에게 경제적, 사회적으로 큰 피해를 입힐 수 있으므로 반드시 보호되어야 한다.

5.2.2. 위협원

HTS의 위협원은 자산에 공격적인 행동을 하는 실체로서 공격자, 인가된 사용자, 특권을 부여받은 사용자, 관리자, 시스템 소유자와 개발자 등 다섯 가지 유형으로 분류한다.[9]

공격자는 위에서 제시한 공격 시나리오의 공격자 또는 정당한 사용자로 가장하려는 인가받지 않은 사용자로 개인정보를 획득 및 손상시키려는 존재이다. 이러한 공격자는 해킹툴을 이용하여 개인정보를 획득할 수 있는 수준을 갖는다. 해킹툴은 본 논문의 취약성 분석에 사용된 원격 시스템에 대한 키로깅과 파일 접근 및 변경, 복사가 가능한 백도어 프로그램이나 키로깅 프로그램, 스니핑 프로그램 등을 포함한다.

5.2.3. 취약점 및 공격방법

앞에서 서술한 공격 방법을 통해 분석한 HTS의 취약점은 아래와 같이 세 가지로 분류된다.

- 해킹툴을 사용하여 입력 정보 및 저장 정보를 취득하거나 손상
- 전송 패킷을 스니핑하여 패킷으로부터 의미 있는 개인정보가 담긴 전송 정보를 취득
- 앞의 두 가지 방법을 통해 취득한 정보를 이용한 인증 및 개인정보를 악용

5.2.4. 위협 도출

위협은 앞에서 파악한 자산과 위협원, 공격방법을 통해 도출한다. 즉, 위협은 위협원에 의해 자산이 공격방법으로 손상됨을 서술한다.

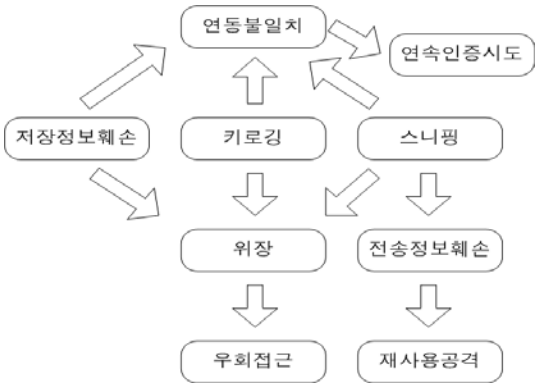
위에서 분석한 취약점에 의한 직접적인 위협은 '키로깅', '스니핑', '저장정보훼손' 등이 있다. 세가지 위협을 통해 '결함코드', '위장', '전송정보훼손', '연속인증시도', '재사용공격' 등의 위협이 도출되며, '연동불일치'와 '위장' 위협을 통해 '우회접근' 등의 위협이 도출된다. 도출 과정은 [그림 28]과 같다.

본 논문에서 제시한 취약성 외에 HTS에 영향을 미칠 수 있는 위협을 추가적으로 추출하여 평가기준의 완벽성을 기한다. 추가적인 위협은 [표 8]의 취약성 DB로부터 추출하며, '결함코드', '잔여정보', '배포설치', '관리부실' 등이 있다.

HTS에 가해질 수 있는 위협은 아래 [표 9]와 같이 명세한다.

5.2.5. 가정사항

위에서 도출한 위협은 HTS에 직접적인 영향을 미



[그림 28]. HTS의 위협 도출 과정

[표 8]. 취약점 및 취약점 정보를 얻을 수 있는 주요 정보원

분류	이름
취약성 분석 인터넷 사이트	CERTCC-KR(http://www.certcc.or.kr) CERTCC(http.cert.org) BUGTRAQ(http://www.securityfocus.com) PacketStormSecurity(http://www.packetstormsecurity.org) MITRE(http://cve.mirte.org) SANS ICS(http//ics.sans.org) CIAC(http://www.ciac.org/ciac) BLACKHAT(httt://www.blackhat.com) MCAFEE Threat Center(http://www.mcafee.com/us/threat_center)
취약점 분석 자료를 제공하는 사이트	Zdnet(http://ww.zdnet.com) Security New Portal(http://www.securitynewportal.com)
위협 및 취약점 데이터베이스	JISEC Threats Database JISEC Vulnerabiltiy Database

[표 9]. HTS에 가해질 수 있는 위협

위협	설명
T.스니핑	인가받지 않은 사용자가 스니핑 프로그램을 이용하여 전송 정보를 얻어 도용할 수 있다.
T.연동불일치	다양한 컴포넌트 사이에서의 모순과 불일치 때문에, 다수의 보안제품과 시스템을 써서 구현되는 복합화된 HTS의 보안기능은 부적당할 지도 모른다.
T.우회접근	인가받지 않은 사용자는 HTS평가범위의 보안기능을 우회하여 HTS평가범위에 접근하여, 사용자의 금융 관련 정보를 손상시킬 수 있다
T.위장	인가받지 않은 사용자는 키로깅과 스니핑을 통해 얻은 사용자 개인정보를 이용하여 정당한 사용자로 가장할 수 있다.
T.저장정보훼손	인가된/비 인가된 사용자는 백도어 프로그램의 파일 제어 기능을 이용하여 사용자 PC의 저장 정보를 취득하여 도용할 수 있다.
T.전송정보훼손	인가받지 않은 사용자는 HTS클라이언트와 HTS서버의 통신에서 전송 정보를 변경하여 사용자의 금융 관련 정보를 훼손할 수 있다.
T.키로깅	인가받지 않은 사용자가 백도어 프로그램이나 키로그 프로그램의 키로깅 기능을 이용하여 사용자 입력 정보를 얻어 도용할 수 있다.
T.연속인증시도	인가받지 않은 사용자는 HTS에 연속적으로 인증을 시도하여 입력 정보 및 인가된 사용자의 권한을 획득할 수 있다.
T.결함코드	개발자는 명세서에 따라서 수행되지 않거나 보안상의 결함이 있는 코드를 포함하여 보안솔루션의 연동이 적절하게 이루어지지 않거나 개인정보를 유출시킬 수 있다.
T.관리부실	HTS 보안기능의 관리 행동으로 인한 HTS의 변화는 보안기능을 동작 못하거나 오류를 일으키게 할 지 모른다.
T.배포설치	HTS의 배포 또는 설치 과정에서 HTS의 보안을 손상시킬 수 있다.
T.잔여정보	HTS의 보안기능이 자원을 재사용할 경우, 객체의 정보가 적절하게 제거되지 못해 위협원이 정보에 불법적으로 접근할 수 있다.
T.재사용공격	위협원은 인가된 사용자의 인증 데이터를 재사용하여 HTS의 보안기능에 접근할 수 있다.

[표 10]. HTS가 운영되는 시스템의 가정사항

구분	설명
A.보안유지	네트워크 구성 변경, 호스트의 증감, 서비스의 증감 등으로 내부 네트워크 환경이 변화될 때, 변화된 환경과 보안정책을 즉시 TOE 운영정책에 반영하여 이전과 동일한 수준의 보안을 유지한다.
A.신뢰된 관리자	TOE의 인가된 관리자는 악의가 없으며, TOE 관리 기능에 대하여 적절히 교육받았고, 관리자 지침에 따라 정확하게 의무를 수행한다.
A.동적관리	TOE는 동적으로 변하는 보호대상 자산의 변화를 적절하게 다룰 수 있도록 관리된다.
A.안전한 설치/운영	TOE는 안전한 방식으로 설치 및 운영되는 기본적인 운영시스템을 바탕으로 한다.
A.운영체제보강	운영체제상의 취약점에 대한 보강작업을 수행하여 운영체제에 대한 신뢰성과 안정성을 보장해야 한다.
A.HTS평가범위내접근	HTS가 동작하는 운영체제는 HTS가 동작하기 전에 사용자의 식별 및 인증 기능을 제공해야 한다.

[표 11]. HTS의 조직의 보안정책

구분	설명
P.감사	TOE는 보안과 관련된 행동에 대한 책임을 추적하기 위해 보안관련 사건을 정확하게 기록하고 안전하게 유지해야하며, 기록된 감사데이터를 적절하게 검토할 수 있어야 한다.
P.안전한 관리	인가된 관리자는 안전한 방법으로 TOE를 관리할 수 있어야 하며, TSF 데이터를 최신상태로 유지하여야 한다.
P.복구	TOE가 복구되어야 할 때, 안전한 상태로 복구되어야 한다.
P.암호	TOE에서 사용되는 암호 알고리즘 및 모듈은 국가정보원장이 승인한 것을 사용하여야 한다.

치는 위협이며, HTS에 간접적으로 영향을 미치는 운영환경에 대한 위협 사항은 가정사항에서 해결해야 한다. 즉, 안전하게 운영되어야 하는 HTS는 본 논문에서 제안하는 [표 10]의 가정사항이 만족되는 환경에 설치되어야 한다.

5.2.6. 조직의 보안정책

위에서 도출한 위협을 해결하기 위해서는 보안목적을 강제적으로 수행하기 위한 규정이 필요하다. 조직의 보안정책은 이러한 규정에 대해 서술한다. 안전하게 운영되어야 하는 HTS는 [표 11]에 제시된 보안정책을 수행해야 한다.

5.3. 보안목적

위의 위협을 해결하기 위한 보안목적을 [표 12], [표 13]과 같이 도출하였다. 위협과 보안목적의 대응관계는 [표 14]에서 제시한다. HTS의 평가기준은 본 논문에서 분석한 HTS에 직접적으로 영향을 미치는 취약점을 해결하기 위한 것이므로, HTS가 만족해야 할 보안목적은 HTS에 직접적인 위협에 대한 사항만 다룬다. 운영환경에 대한 보안목적은 위에서 제시한 가정사항과 조직의 보안정책에서 만족하므로 별도로 도출하지 않는다.

기능평가 항목으로 위에서 제시한 HTS의 보안목적을 만족시키기 위한 보안기능요구사항은 공통평가기준 2부의 보안기능요구사항 컴포넌트를 바탕으로 도출하였다. 모든 기능평가 항목은 [표 15]에서 나타내고 있는 바와 같이 모든 보안목적을 만족하여 HTS의 보안성을 평가하기 위한 기준으로 정당성을 갖는다. 따라서 안전한 증권거래를 위한 HTS는 본 논문에서 제시한 [표 15]의 기능평가 항목을 모두 만족해야 한다.

[표 12]. 위협으로부터 보안목적 도출

위협	보안목적
T.키로깅	- 키로깅에 사용되는 해킹툴 방지 기능 필요(해킹툴방지)
T.스니핑	- 전송 정보 보호 기능 필요(전송정보 보호)
T.위장	- 안전한 식별 및 인증 기능 필요(식별 및인증)
T.저장정보훼손	- 원격 시스템 파일 제어에 사용되는 해킹툴 방지 기능 필요(해킹툴방지) - 저장 정보 보호 기능 필요(저장정보 보호) - 저장 정보의 암호화/복호화에 사용되는 키의 보안 기능 필요(키 보안)
T.전송정보훼손	- 전송 정보 보호 기능 필요(전송정보 보호) - 전송 정보의 암호화/복호화에 사용되는 키의 보안 기능 필요(키 보안)
T.연속인증시도	- 안전한 식별 및 인증 기능 필요(식별 및 인증)
T.우회접근	- 보안기능의 우회 시도로부터 자체 기능을 보호하는 기능 필요(자체기능보호)
T.연동불일치	- HTS를 구성하는 보안 제품 및 시스템이 안전하고 적절하게 연동 필요(해킹툴방지)
T.결함코드	- HTS의 코드에 결함이 있는지, 연동되는 보안솔루션을 적절하게 적용하고 있는지 검사하는 기능 필요(결함코드검사)
T.관리부실	- HTS의 안전한 설치/운영/관리 기능 필요(관리)
T.배포설치	- HTS의 안전한 설치/운영/관리 기능 필요(관리)
T.잔여정보	- HTS가 운영환경에 남기는 잔여정보는 재사용을 방지하기 위해 완전하게 제거되는 기능 필요(잔여정보제거)
T.재사용공격	- 인가된 사용자의 인증 데이터를 재사용하여 HTS에 접근하는 것을 방지하는 기능 필요(식별 및 인증)

[표 13]. HTS의 위협을 해결하기 위한 보안목적

보안목적	설명
O.해킹툴방지	HTS평가범위에 접근하는 백도어 프로그램의 동작을 방지하여 공격자에게 인가된 사용자의 데이터가 노출되지 않게 한다.
O.전송정보보호	HTS평가범위는 HTS클라이언트와 HTS 서버 간 통신의 전송 정보를 인가되지 않은 노출 및 변경으로부터 보호해야한다.
O.저장정보보호	HTS평가범위는 사용자 PC에 저장된 저장 정보를 인가되지 않은 노출, 변경, 삭제로부터 보호해야한다.
O.식별 및 인증	HTS의 평가범위 내 기능은 사용자를 유일하게 식별 및 인증 해야 하고, 연속인증 실패에 대해 대응해야 한다.
O.키보안	개인 정보 및 사용자의 금융 관련 정보를 보호하기 위한 암호화/복호화 키는 안전하게 보호되어야 한다.
O.자체기능보호	HTS평가범위는 처음 실행될 때부터 HTS평가범위 보안기능 변경, 비활성화, 우회 시도 등에 대하여 자신을 보호해야 한다.
O.감사	HTS평가범위는 보안과 관련된 행동의 책임추적이 가능하도록 보안관련 사건을 기록 및 유지해야 하며, 기록된 데이터를 검토할 수 있는 수단을 제공해야한다.
O.관리	HTS는 안전한 방법으로 배포, 설치되어야 하며, HTS평가범위는 HTS평가범위의 인가된 관리자가 HTS 평가범위를 효율적으로 관리할 수 있는 관리 수단을 안전한 방법으로 제공하며 TSF 데이터를 최신상태로 유지하는 수단을 제공하여야한다.
O.결함코드검사	개발자가 생성한 코드에 결함이 있는지 검사되어야 하며, 결함이 있는 코드가 HTS평가범위 내부 구성요소 간에 영향을 주는지 또는 연동되는 보안솔루션을 적절하게 적용하고 있는지 검사되어야 한다.
O.잔여정보제거	HTS 운영 시에 재 할당된 자원으로 부터 접근권한에 사용가능한 잔여정보를 취득할 수 없어야 한다.

[표 14]. HTS의 위협과 보안목적의 대응관계

	O.해킹툴방지	O.전송정보보호	O.저장정보보호	O.식별및인증	O.키보안	O.자체기능보호	O.감사	O.결함코드검사	O.관리	O.잔여정보제거
T.키로깅	X									
T.스니핑		X								
T.위장				X						
T.저장정보훼손	X		X		X				X	
T.전송정보훼손		X			X					
T.우회접근						X	X			
T.결함코드								X	X	
T.연속인증시도				X			X			
T.적절한연동	X									
T.관리부실									X	
T.배포설치									X	
T.잔여정보			X						X	X
T.재사용공격				X						

[표 15]. 기능평가 항목

보안기능	기능평가 항목	내용
도청방지	F01.해킹 프로그램 탐지	해킹 프로그램의 동작을 탐지하고 경고 및 자동 대응 수행 요구
	F02.키보드 입력 정보 누출 방지	키보드 입력 정보가 기록되거나 외부로의 누출을 방지하는 기능 요구
보안감사	F03.감사 데이터 생성	감사대상 사건들의 감사 레코드 생성 요구
	F04.사용자 신원 연관	사건을 발생시킨 사용자의 신원과 감사 대상 사건을 연관 시키는 기능 요구
	F05.감사 검토	감사 레코드의 정보를 읽을 수 있는 기능 요구
	F06.선택 가능한 감사검토	감사 검토 도구가 검토될 감사 데이터를 기준에 기반하여 선택할 수 있는 기능 요구
	F07.감사 증적 저장소 보호	감사 증적 저장소는 인가되지 않은 삭제 및/또는 변경으로부터 보호되어야 하는 기능 요구
	F08.감사 데이터 손실 예측 시 대응 행동	감사 증적의 임계치를 초과할 경우 취해야 할 대응행동 명세 기능 요구
	F09.감사 데이터의 손실 방지	감사 증적 저장소가 포화되는 경우의 대응 행동 명세 기능 요구

보안 기능	기능평가 항목	내용
사용자 데이터 보호	F10.보안속성에 따라 객체에 대한 주체의 접근 제어	보안속성에 따라 객체에 대한 주체에 접근을 제어하는 규칙이 제공되어야 하며, 그에 따라 접근 통제가 수행하는 기능 요구
	F11.정보흐름의 통제	정보흐름을 제어하기 위한 보안정책이 제공되어야 하며, 정보흐름 보안정책과 보안속성에 따라 정보 흐름이 제거, 감시하는 기능 요구
	F12.전송 데이터의 무결성	HTS의 서버와 클라이언트 사이에 전송되는 데이터 및 데이터의 생산자, 송신처, 수신처의 무결성을 보장하는 기능 요구
	F13.전송데이터의 비밀성	HTS의 서버와 클라이언트 사이에 전송되는 데이터 및 데이터의 생산자, 송신처, 수신처의 비밀성을 보장하는 기능 요구
	F14.자원의 모든 이전정보 완전 삭제	모든 객체에 사용된 자원을 회수하는 경우 자원의 모든 이전 정보 내용이 가용하지 않음을 보장하는 기능 요구
암호 지원	F15.암호키 생성	명세된 암호 알고리즘과 키 길이에 따라 암호키가 생성될 것을 요구
	F16.암호키 분배	명세된 분배 방법에 따라 암호키가 분배될 것을 요구
	F17.암호키 파기	명세된 파기 방법에 따라 암호키가 파기될 것을 요구
식별 및 인증	F18.인증 실패 처리	사용자 인증시도 실패 횟수가 명세된 값을 넘으면 TSF가 세션 설정 과정을 종료 시킬 수 있을 것을 요구
	F19.인증	사용자가 사용자 신원을 인증하기 전에 어떤 행동을 수행할 수 있도록 허용
	F20.식별	사용자가 HTS의 평가범위 내 보안 기능에 의해서 식별되기 전에 어떤 행동을 수행하는 것을 허용
	F21.비밀정보의 정의 및 생성 검증, 사용 제어	인가된 사용자로 부터 생성된 비밀정보의 정의 및 생성 메커니즘을 제공해야 하며, 비밀정보의 사용이 강제되는 기능 요구
보안 관리	F22.보안기능관리	규칙을 사용하거나 관리 가능한 조건을 가진 TSF 기능을 인가된 사용자(역할)가 관리할 수 있도록 하는 기능 요구
	F23.보안기능 데이터관리	인가된 관리자가 HTS의 평가범위 내 보안 기능 데이터를 관리하도록 하는 기능 요구
	F24.관리기능 명세	HTS의 평가범위 내 보안 기능이 특정 관리기능을 제공할 것을 요구
	F25.보안역할	HTS의 평가범위 내 보안 기능이 인식할 수 있는 보안에 관련된 역할을 명세하는 기능 요구
보안 기능 보호	F26.내부전송 보안기능 데이터의 기본적인 보호	HTS의 평가범위 내 보안 기능 데이터가 HTS의 평가범위의 분리된 부분간에 전송될 때 보호될 것을 요구
	F27.보안기능 자체시험	HTS의 평가범위 내 보안 기능의 올바른 운영을 시험하는 능력을 제공하고, HTS의 평가범위 내 보안 기능 데이터와 실행 코드의 무결성을 검증하는 기능을 요구
안전한 경로/채널	F28.보안기능 간 안전한 채널	HTS의 평가범위 내 보안 기능이 자신과 다른 신뢰된 IT 제품 간에 안전한 통신 채널을 제공할 것을 요구
생명 주기 지원	F29.결함교정 및 버전 관리	HTS의 보안 결함이 발생 시, 개발자에게 결함에 대한 교정 절차가 이루어져야 함. 결함 교정에 따른 HTS의 업데이트와 버전 관리가 이루어져야 함

[표 16]. 보안목적과 기능평가 항목의 대응관계

	O. 해킹툴방지	O. 전송정보보호	O. 저장정보보호	O. 식별및인증	O. 키보안	O. 자체기능보호	O. 감사	O. 관리	O. 결함코드검사	O. 잔여정보제거
F01.해킹 프로그램 탐지	X	X	X							
F02.키보드 입력 정보 누출 방지	X	X	X							
F03.감사 데이터 생성							X			
F04.사용자 신원 연관							X			
F05.감사 검토							X			
F06.선택 가능한 감사검토							X			
F07.감사 증적 저장소 보호							X			
F08.감사 데이터 손실 예측 시 대응 행동							X			
F09.감사 데이터의 손실 방지							X			
F10.보안속성에 따라 객체에 대한 주체의 접근 제어			X	X				X		
F11.정보흐름의 통제		X		X				X		
F12.전송 데이터의 무결성		X		X				X		
F13.전송데이터의 비밀성		X		X				X		
F14.자원의 모든 이전정보 완전 삭제										X
F15.암호키 생성					X					
F16.암호키 분배					X					
F17.암호키 파기					X					
F18.인증 실패 처리				X						
F19.인증			X	X	X					
F20.식별			X	X	X					
F21.비밀정보의 정의 및 생성 검증, 사용 제어			X			X				
F22.보안기능관리						X		X		
F23.보안기능 데이터관리								X		
F24.관리기능 명세								X		
F25.보안역할								X		
F26.내부전송 보안기능 데이터의 기본적인 보호		X			X					
F27.보안기능 자체시험			X		X	X		X		
F28.보안기능 간 안전한 채널		X			X					
F29.결함교정 및 버전 관리									X	

Ⅵ. 결 론

2007년 11월 1일에 키로깅과 스니핑을 통해 HTS의 보안서비스를 재조사하였다. 여러 증권사의 HTS가 업데이트 되었고 [그림 29], [표 17]과 같이 파일 사이즈가 증가하였다. 키로깅과 스니핑의 결과는 [표 18]과 같다. 키로깅의 경우, 압축하고 패킹을 하여 이전에는 감지를 못했던 Netbus의 백도어 프로그램과 SKin2000 프로그램이 Myfirewall 등의 여러 보안 솔루션에서 발견이 되고 삭제되어 많은 HTS의 보안서비스가 이전보다 나아진 것을 볼 수 있다. 하지만 스니핑의 경우 몇몇 증권사의 HTS는 전과 같은 수준임을 알 수 있다.

본 논문에서는 국내 HTS에 적용된 보안서비스의 안전성을 조사하기 위하여 키로깅, 스니핑을 통한 HTS의 보안서비스를 분석하였다. 그리고 분석 결과로부터 아이디, 로그인 비밀번호, 공인인증서 암호 등의 개인정보가 노출된다는 것을 알 수 있었고, 문제점을 통해 HTS의 바람직한 평가기준을 도출하였다.

인터넷 뱅킹이 제공하는 보안서비스는 이전에 비해 많이 개선되었으나 HTS를 이용한 온라인 증권거래의 경우 보안서비스의 적용에 많은 문제점이 있었다. 본 논문에서 제시한 바람직한 평가기준을 따르면서 인터넷 뱅킹에 적용된 보안서비스의 기능을 HTS에 접목시킨다면 키로깅, 스니핑으로 인한 개인정보노출을 막고 이용자에게 더 안전한 보안서비스를 제공할 수 있을 것이다.

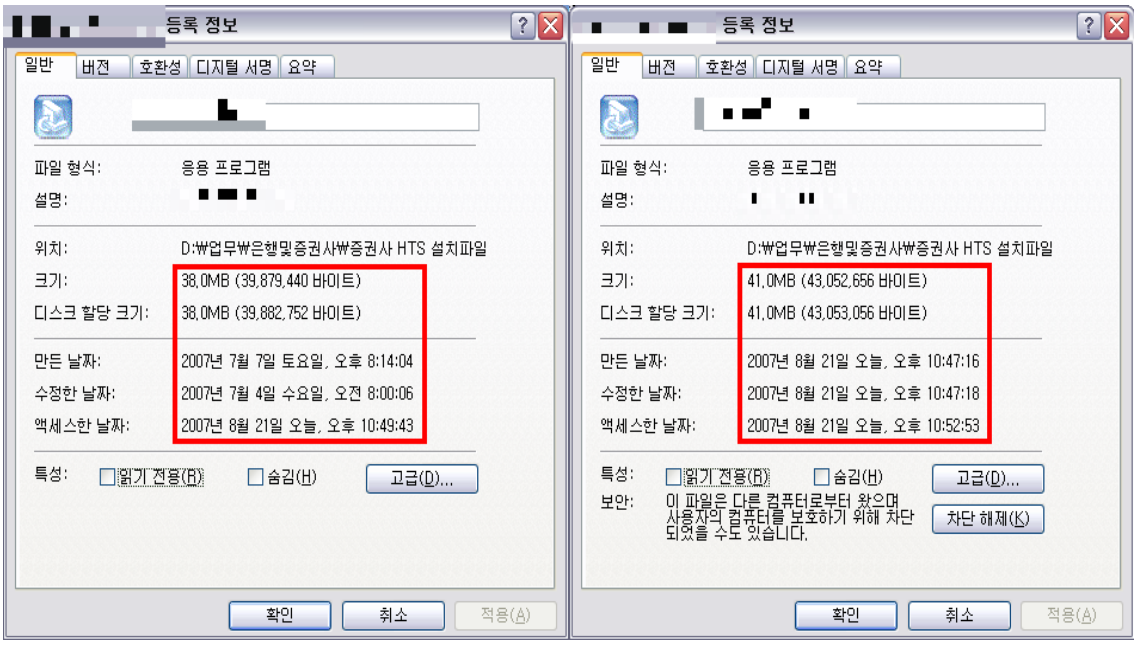
그리고 메모리를 읽어와 접근하는 방법과 관련하여 메모리에 보관된 주소 내 데이터를 변조하는 메모리 해

[표 17]. 각 증권사의 HTS 설치파일 사이즈 (단위 : MB)

증권사	파일 사이즈 (2007.07.04)	파일 사이즈 (2007.08.22)
A증권	34.2	45.2
C증권	18.5	18.8
D증권	27.1	32.0
K증권	21.1	23.4
L증권	23.2	23.6
M증권	38.0	41.0
N증권	19.1	20.1
P증권	25.6	25.8
V증권	12.8	15.6
AA증권	12.6	12.6

[표 18]. 증권사별 노출정보 (2007년 11월 1일)

증권사	키로깅				스니핑			
	아이디	로그인 비밀번호	공인인증서 암호	계좌비밀번호	아이디	로그인 비밀번호	주민등록번호	계좌번호
A증권	×	×	×	×	○	○	×	×
B증권	×	×	×	×	×	×	×	×
C증권	×	×	×	×	×	×	×	×
D증권	×	×	×	×	○	○	×	×
E증권	×	×	×	×	○	×	×	×
F증권	×	×	×	×	×	×	×	×
G증권	×	×	×	×	×	×	×	×
H증권	×	×	×	×	○	○	×	×
I증권	○	×	×	×	○	×	×	×
J증권	×	×	×	×	○	×	○	×
K증권	×	×	×	×	○	×	○	×
L증권	×	×	×	×	×	×	×	×
M증권	○	×	×	×	×	×	×	×
N증권	×	×	×	×	○	×	○	○
O증권	×	×	×	×	×	×	×	×
P증권	○	×	×	×	○	×	×	×
Q증권	×	×	×	×	×	×	×	×
R증권	○	×	×	×	○	×	○	×
S증권	×	×	×	×	×	×	×	×
T증권	×	×	×	×	○	×	×	×
U증권	×	×	×	×	×	×	×	×
V증권	×	×	×	×	×	×	×	×
W증권	×	×	×	×	○	×	○	×
X증권	×	×	×	×	×	×	×	×
Y증권	×	×	×	×	○	×	×	×
Z증권	×	×	×	×	×	×	×	×
AA증권	×	×	×	×	○	×	×	×
BB증권	×	×	×	×	○	×	×	×
계	4	0	0	0	15	3	5	1



[그림 29]. HTS의 업데이트 후 파일 사이즈 변경(좌 : 업데이트 전, 우 : 업데이트 후)

킹을 이용한 해킹 기법을 막는 방법과 HTS의 키로깅, 스니핑이 아닌 다른 취약점에 대한 분석과 그 대응책에 대한 연구가 향후 이루어져야 할 것이다.

참고문헌

[1] 금융감독위원회, "연간 전자금융 취급실적", *금융감독원 보도참고자료*, 2004 ~ 2007

[2] 김병조, "은행 인터넷뱅킹 첫 해킹당해 거액 빠져나가", *연합뉴스* 2005. 6. 30 뉴스, 2005.

[3] 금융보안연구원, "국내 금융관련 동향", *금융보안주간정보* 2007. 2. 26, 2007

[4] 네이버 용어사전 (http://terms.naver.com)

[5] 진강훈, 후니의 쉽게 쓴 시스코 네트워킹, *(주)사이버출판사*, 2002 ~ 2004

[6] 신동휘, 최윤성, 박상준, 김승주, 원동호, "네이트온 메신저의 사용자 인증 메커니즘에 대한 취약점 분석", 정보보호학회논문지, pp. 67-80, February 2007

[7] 성재모(금융보안연구원), "국내 금융정보보호 현황 및 동향", NETSEC-KR, 2007

[8] 정보통신부, "정통부, 인터넷 전송구간 개인정보 보호 강화나서", *정보통신부 보도자료* 2007.2.6, 2007

[9] ISO/IEC 2nd WD 15446, Guide for the production of protection profiles and security targets, 2007. 01. 22

[10] Common Criteria for Information Technology Security Evaluation, Version 3.1, *CCMB*, 2006. 9.

[11] 뱅크타운 홈페이지 (http://www.banktown.com)

[12] 비티웍스 홈페이지 (http://www.btworks.co.kr)

[13] 잉카 인터넷 홈페이지 (http://www.inca.co.kr)

[14] 소프트캠프 홈페이지(http://www.softcamp.co.kr)

[15] 이니텍 홈페이지 (http://www.initech.com)

[16] 한국정보인증 홈페이지 (http://www.signgate.com)

[17] 킹스정보통신 홈페이지 (http://www.kings.co.kr)

[18] STI security 홈페이지 (http://www.stitec.com)

[19] 소프트포럼 홈페이지 (http://www.softforum.co.kr)

[20] 안철수 연구소 (http://www.ahnlab.com)

<著者紹介>

이 윤 영 (Yun-young Lee) 학생회원
2007년 2월 : 성균관대학교 정보통신공학부(공학사)
2007년 3월~현재 : 성균관대학교 일반대학원 전자전기컴퓨터공학과 석사과정 재학 중
<관심분야> 정보보호 응용, 네트워크 보안

최 해 랑 (Haelahng Choi) 학생회원
2007년 2월 : 성균관대학교 정보통신공학부(공학사)
2007년 3월~현재 : 성균관대학교 일반대학원 전자전기컴퓨터공학과 석사과정 재학 중
<관심분야> 암호이론, 정보보호 응용, 포렌식, 네트워크보안

한 정 훈 (Jeonghoon Han) 학생회원
2007년 2월 : 성균관대학교 정보통신공학부(공학사)
2007년 3월~현재 : 성균관대학교 일반대학원 전자전기컴퓨터공학과 석사과정 재학 중
<관심분야> 정보보호, Digital Identity Management, 모바일 IP 보안, 보안성 평가

홍 수 민 (Sumin Hong) 학생회원
2005년 8월 : 덕성여자대학교 수학과(이학사)
2007년 3월~현재 : 성균관대학교 전자전기컴퓨터공학과 석사과정
<관심분야> 정보보호, 금융보안, 암호이론, 암호 프로토콜

이 성 진 (Sungjin Lee) 학생회원
2007년 2월 : 성균관대학교 정보통신공학부(공학사)
2007년 3월~현재 : 성균관대학교 휴대폰학과 석사과정 재학 중
<관심분야> 정보보호

신 동 휘 (Donghwi Shin) 학생회원
2002년 2월 : 성균관대학교 자연과학부 물리학과(이학사)
2002년 2월 : 성균관대학교 전기전자컴퓨터공학부(공학사)
2002년 3월~2002년 9월 : 성균관대학교 일반대학원 물리학과 석사과정
2006년 3월~현재 : 성균관대학교 일반대학원 전자전기컴퓨터공학과 석사과정 재학 중
<관심분야> 네트워크보안, 침투테스트, 정보보호 응용

<著者紹介>

김 승 주 (Seungjoo Kim) 종신회원
1994년 2월~1999년 2월 : 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월~2004년 2월 : 한국정보보호진흥원(KISA) 팀장
2004년 3월~현재 : 성균관대학교 정보통신공학부 교수
2001년 1월~현재 : 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년 4월~현재 : 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년 7월~현재 : 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장
<관심분야> 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호 (Dongho Won) 종신회원
1976년~1988년 : 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 : 일본 동경공업대 객원연구원
1988년~2003년 : 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, IT보안성평가연구회 위원장
<관심분야> 암호이론, 정보이론, 정보보호