# Security Vulnerability Analysis and Forensic Data Research to Attacks on Mobile Stock Trading System in WiBro Network

**Woo-Sung Chun**[†] **and Dea-Woo Park**[††]

Department of IT application Technology, Hoseo Graduate School Of Venture, KOREA

**Summary**
A financial transaction is becoming activation, and financial accident is frequently occurring at mobile terminals by a spread of the Ubiquitous Era on the latest date. We execute an attack regarding mobile stocks transactions system from WiBro networks at this paper, and we study a Security Vulnerability Analysis infringement attack accidents. We generate Forensic data use WireShark, and monitoring calls an actual stock trading process in WiBro networks in order to analyze mobile stocks transactions, and analyze, and detect Vulnerability, and analyzing a packet. We ensure a basis of study detect port, and detect Security Vulnerability through analyses aggressive analysis aggressive viral penetration, authentication packet analysis, analysis aggressive a DDoS network, analysis aggressive a terminal mobile WiBro, a HTS program that there was in order to open through the scanning that used NetScan Tools, and analyze, and generate Forensic data, and to be able to be used as to criminal investigation and legal data.

***Key words:***
*WiBro, Vulnerability, Forensic, Hacker Attack, DDoS*

## 1. Introduction

The Republic of Korea at IT powerful country at 3 place the national information-oriented quotient world, 3 place the month average personal Internet use timely world and the world-wide beginning e-government introduction and the Internet banking personal member 4 ten million people etc, superhigh speed Internet infra and finance IT are developmental to advanced nation level.

2007 and 2008 with end stock market liveliness on-line stock trading member the increase and stock trading amount reach to 1,572 trillion won as well on a large scale with 7,500,000 people. While whole transacting business on-line transaction value is cold under the specific gravity is 8th case (79.6%) in 10th case.

But it is 2007 on-line private data outflow 25,000 case, Hacking and Phishing and Pharming, Vishing, the damage of the individual in compliance with Worm Virus and the financial institution is magnified in as much as 2008 years and 2009 years [1].

2008 August 29th, the home page of the 30th height bud securities in compliance with the hackers encountered a DDoS(distributed denial of service) attack. It requested the investigation in the company sympathetic Seoul region National Police Office cyber investigation unit [2]. Amount of damage 6 ten million won occur, and the large size bank which strengthened security even is showing to thing with Vulnerability from Do hacking to the 2009 April Kookmin Bank hacking accident phosphorus MulDrop methods that occurred, and we leave emphasis to forensic data generation in order to submit criminal corroborative facts to legal proof through integrities of crime data [3] and original anger proof in the terror response center cyber the National Police Agency, and we are investigating.

To recently a financial transactions the financial transaction value which leads the carrying Internet which uses WiBro networks it is activated, the government and the security company and the bank etc. financial institution it activates. Also it is caused by with supply of WiBro whole aspect four north and when where it stands recently, or, applies the Internet electronic transaction [4].

There must be a necessity which will analyze the security vulnerability which from the financial transactions which leads WiBro carrying Internet it prepares in financial accident the security vulnerability of mobile stock trading from WiBro, from the present paper, among those it must analyze forensic fundamental data it must create and the stability and a security characteristic of financial transactions from the carrying Internet which will approach in future it must secure the reliability and security stability could be guaranteed in about our country finance IT which is a IT superhigh speed Internet use powerful country.

From the present paper from 1 chapter introduction necessity and objective and scope of research WiBro carrying Internet networks, mobile HTS, it investigates mobile HTS use transactions analyzes, WiBro mobile HTS programs, the financial transactions hackings and phishing present conditions of recent times from 2 chapter relation researches. 3 chapters it analyzes experimental environments and stock trading network analyzes and vulnerability analyzes, stock trading contents packet analyzes and WiBro mobile stocks vulnerabilities from WiBro mobile HTS vulnerability analysis experiments. 4 chapters attack analyzes and forensic data lifestyle frost it stands in about Wibro mobile stock trading systems and in about virus permeation attack and authentication packet 5 chapter conclusions and a hereafter research the infringement (damage) which it follows in attack analysis,

***Dea-Woo Park***[††]*(**corresponding author**)*
Manuscript received December 5, 2009
Manuscript revised December 20, 2009

WiBro network attack analysis, WiBro mobile communication terminal attack analysis, WiBro mobile HTS program attack analysis and attack and vulnerability analysis to lead, it puts out it presents.

## 2. Related Work

### 2.1 WiBro carrying Internet networks

Next generation mobile communication technique WiBro(Wireless Broadband) the superhigh speed carrying Internet network which it uses stands when where or even while moving the web search of course, this mail, multimedia and video conference, VoIP service etc. is the world-wide first Mobile 2.0 services it will be able to use the Internet information and the contents which are various [5].

WiBro carrying Internet networks the standard 802.11e in standard. This is it uses 2.4GHz frequencies which exist and 5GHz frequency ranges the equipment of 2.3GHz substitute actors from Korea and with problem of Channel interference etc. develops it is a field which it standardizes [6].

### 2.2 Mobile HTS

HTS is groove trading with home trading system. The investor goes to the security company, or, it does not use a transformation not to be, it is a system which puts out the direct stockjobbing order to use the computer from the family or job. On-line leads in single word and it is a system stockjobbing.

With end of 1980's simply it will be able to inquire the stocks current price in order on the beginning of 1990's, to 1997 after that the Internet environment gets better with the fact that it is developed from the family investment information system which is provided it introduced from the various security company. The stocks current price it sees to initially with, only market order functional degree it comes in at 2000's is not and various analysis even of course selling and buying consultation there is a possibility of doing.

### 2.3 HTS use transactions analyzes

Korean securities futures trading from small from 2004 until 2008 gas price securities market, investigation it compares the order medium by transactions present condition of KOSDAQ market, Table. 1 is to show a KOSDAQ market order medium by sales value at year by.

The Wireless terminal the sales value specific gravity increases rapidly in 2005 years, it recorded the increase numerical figure of top in 2008 years again to decrease and HTS decreases increased a little steadily in 2007 years. From 2008 year order medium by transactions present - conditions gas price securities market the sales value specific gravity which leads the business terminal with 50.77% previous year 52.88% preparation 2.11% decrement, the sales value specific gravity which leads HTS previous year was under 40.14% preparation 0.41% increasing with 40.55%, KOSDAQ market the sales value specific gravity which leads the business terminal with 16.49% previous year 19.46% preparation 2.97% decrement, the sales value specific gravity which leads HTS previous year 76.42% preparation 2.08% increased with 78.50%.

From order medium by sales value specific gravity (gas price securities market) of the investor the individual led HTS mainly, the foreigner and the agency led and the business terminal they transacted business [7].

Table 1: KOSDAQ order medium by sales value (%)

| *Year* | *Business Terminal* | *Cable Terminal* | *Wirless Terminal* | *HTS* | *etc* |
|---|---|---|---|---|---|
| 2004 | 26.38 | 1.56 | 1.98 | 69.84 | 0.25 |
| 2005 | 21.37 | 1.32 | 2.14 | 74.8 | 0.37 |
| 2006 | 18.76 | 1.24 | 1.95 | 77.32 | 0.74 |
| 2007 | 19.46 | 1.02 | 1.83 | 76.42 | 1.27 |
| 2008 | 16.49 | 0.89 | 2.18 | 78.5 | 1.91 |

### 2.4 WiBro mobile HTS programs

Fig. 2 from WiBro whole aspect PAD established PDA HTS programs in PDA and the screen which it executes it made. WiBro networks it leads and the stock trading whole aspect PDA it leads and market conditions, quotient, securities news and quick time etc. securities pertinent information as a real-time it confirms and the users are safe and conveniently, one card it does not stand it uses an user authentication function and a annexed service.

KT login of separate way without the current price and information confirmation are possible with WiBro whole aspect terminals. There is a stockjobbing function and a CMA variant function and the quick upload speed and service charge are cheap. The service possible area is the Seoul former area, the capital region and the condition part area, service use method login of separate way without the current price and information confirmation are possible with KT WiBro whole aspect terminals [8].


Fig. 2 HTS program in KT WiBro

### 2.5 Financial transactions hackings and Phishing present conditions of recent times

2005 exchange bank hacking keylogging [9] method and damage 72,000,000 won and, 2006 the safety settlement and relief click hacking event and 2007 real-time account variant hacking event occurred. If to existing shows off the hacking technique of oneself specially the objective for was strong, to 2006 after that the hacking of monetary profit objective is increasing rapidly.

According to National Intelligence Service 2006 phishing instance 1226th case middle bank and the insurance company etc. financial relation agency 871st case, the transactions sites which go round with 68.8% are becoming target of hacking. The electronic transaction enterprise one phishing degree 380th case (30%) it rises in the object.

Phishing [10] data fishing pulls out the general Email dispatch is the first phase private with intention. Phishing Mail the users approach with a social engineering methodology [11] with 'Change the password. When answer back within 24 hours, the account stands still.' etc. and is linked in Email the internet address which to under click they make. Address and click with actual site it makes and suspicion account number, password, resident registration number and authentication it stands to make a password etc. financial pertinent information input it becomes without from stomach site and the home page connect which is disguised with same features[12].

The National Intelligence Service in order to close phishing damage presented a real site and the imitation site distinction law. The normal site payment account input is not a necessity and when login doing, the separate way screen floats and when pressing the inquiry button, becomes the balance indication and it is to be a normal site (phishing sites the balance inquiry being not right)[13].

Even other than Hacking and Phishing there is a possibility which will be security vulnerability and attack to about Pharming, Vishing and Worm Virus[14].

## 3. WiBro mobile HTS vulnerability analysis experiments

### 3.1 Experimental environment

For the vulnerability analysis of mobile stock trading system from WiBro, networks it composed the experimental environment for WiBro mobile stocks factual account experiments in the graduate school laboratory. The experimental environment with afterwords is same.

# gateway systems: Microsoft Windows XP Home Edition Version 2002 Service Pack 3

CPU: Intel (R) Core (TM) 2 Quad CPU Q9400 @ 2.66GHz

RAM: 3.00GB RAM

# connection systems: Microsoft Windows XP Home Edition Version 2002 Service Pack 3

CPU: Genuine Intel (R) CPU T2400 @ 1.83GHz

RAM: 2.00GB RAM

# use terminal systems: KT WiBro - LG-KU1p

# HTS - south Korean investment securities eFriend HTS programs.

It used a connection system above gateway system and WiBro base stations were located within 200m and within the building from WiBro repeaters from within 1~2m scopes above reception rate 90% upload 1Mbps, they experimented from the place it will be able to maintain the speed of download 2.5~2.8Mbps.

It respects a packet analysis it stands and to establish WireShark v1.2.1 WinPcap degrees it establishes and the packet transmission which becomes accomplished from the network as a matter of at real-time the monitor ring it does [16].

### 3.2 Stock trading network analysis and vulnerability analysis

KT WiBro whole aspect terminals it will lead from WiBro carrying internet networks and it will confirm the possibility user authentication function and annexed service market conditions, quotient, securities news and quick time etc. securities pertinent information as a real-time, it was.

NetScan it uses Tools 5.1 and WireShark it leads and address scanning host from packet where it analyzes. It sets a IP point initially with Start IP address: 210.183.254.1 and it sets scanning a IP point last with End IP address: 210.183.254.254. Fig. 3 got same scanning results.

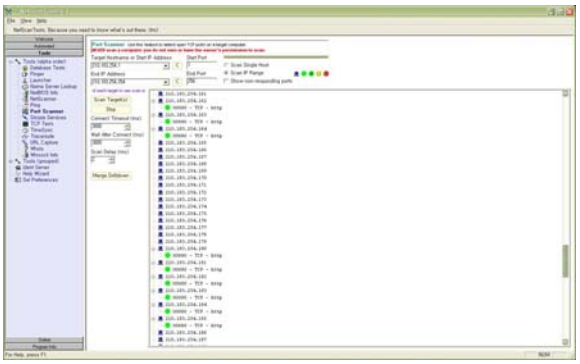

Fig. 3 NetScan Tools 5.1 stocks transaction network Scanning

It used VisualRoute 2009 programs and it tried to track the course of Mobile stock trading systems. Tracking analytical resultant Fig. 4 it comes like network path as a matter of hop with PC and eFriend servers the result which it sees it will see and experiment connection it will be able

to grasp on network connection center the fire-wall or IDS and IPS etc. security equipment are established is a possibility the fact that one fire-wall is established from the Fig. 4 it will be able to confirm. And Source IP (125.152.13.173) it comes the environment of the connection network with text there is a possibility of knowing the location of Destination IP (210.183.254.149) from the map and expression it does as a favor. And NodeName (records) with which Port (80 port - TCP - HTTP) with the map where the connection is maintained a vulnerability it will be analyzed and it will be able to discover.

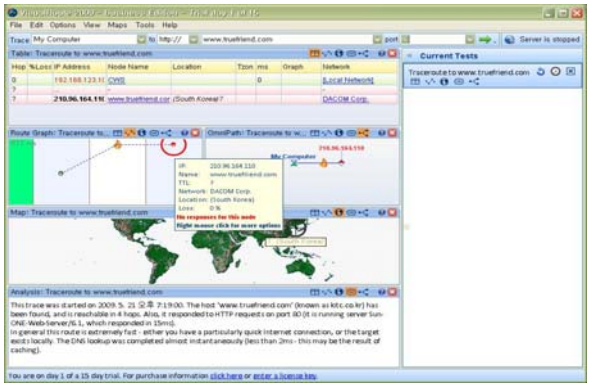

Fig. 4 WiBro Mobile path chase screen that use VisualRoute 2009

### 3.3 Stock trading contents packet analysis

WiBro it leads and it connects it uses it connects stocks transaction value it uses WireShark where they are Snipping Tool and it uses packet WinPcap where it connects a financial data in experiment PC in about the present condition which becomes accomplished and transactions contents etc. in security company server, HTS programs and in the Internet and capture.

Fig. 5 to use WireShark and it is packet WiBro mobile stock trading contents the cap department.

The first time window to seem currently information which are basic is discovered from packet packet number(No.35) where it is collected, packet is collected the time(Time 1.951771), Source IP (125.152.11.96) which send packet it comes Destination IP (210.183.254.184), Protocol (TCP) and Info (icp>dc [ACK] Seq=118 Ack=8161 win=65535 Len=0) packet in packet-list territories, the vulnerability appeared. The second time window to seem information (Frame 35(54 bytes on wire, 54 bytes captured) | Ethernet II, src:LgElectr_18:dd:d2 (00:e0:91:18:dd:d2), Dst:valo_98_0b_01 (00:0a:7d:98:0b:01) | Internet Protocol, src: 125.152.11.96 (125.152.11.96), Dst: 210.183.254.184 (210.183.254.184) | Transmission Control Protocol, src port: icp (1112), Dst port: dc(2001), seq: 118, Ack: 8161, Len:0) class in about packet where in packet detail territories it designates with mouse, it will be able to grasp information which is detailed. The third window to put out control language features as in packet byte territories (0000: zero A 7d 98 B 01 e0 109 dd d2 53.}..... .X…E.) packet it is mechanical indolently.

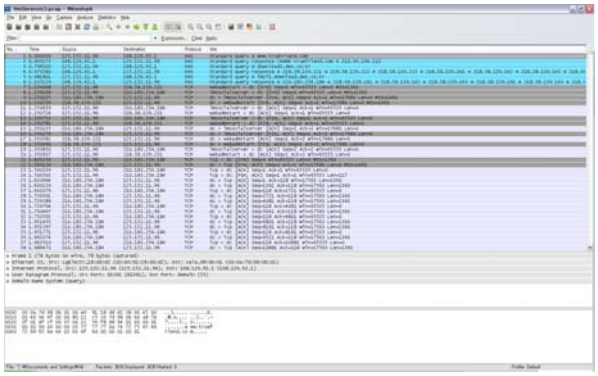

Fig. 5 WireShark v1.2.1 stocks transaction packet collection

### 3.4 Vulnerability analysis

From mobile stock trading system of WiBro networks it did an actual stock trading right time WireShark packet collection and analytical contents with character and it executed a vulnerability analysis.

TCP it uses the resultant Internet protocol which and analyzes respectively TCP Stream contents in packet analyzes it knows this information and it will be able to analyze it uses MAC Address grasp Source IP : 125.152.13.158 and Destination IP : 210.183.254.158. Also packet analyzes it led and it knew Source Port : 62796(62796) and Destination Port : globe(2002) and packet led and 62Bytes, header length 20Bytes etc. TCP Stream SYN where one packet is putting in, information of ACK signal and IP address and the user it led and packet and it analyzed information which is necessary to a hacking it got. Also scanning it led and the pot and the being revealed which are being opened there was a possibility of knowing the pot which is connected and the vulnerability of the mobile stock trading system network and terminal system of WiBro networks for the attack of the hacker came to be analyzed.

## 4. In about WiBro mobile stock trading systems attacks and analyzes and forensic data creations

### 4.1 Virus permeation attack

It uses a social engineering method in the stock trading system owner who is the attack object of the hacker and there is a problem, inspection to send Email where is to

financial system, when scanning relation file files for a problematic inspection knock-down receiving the virus permeates. Link it led in HTS home pages and it permeated the virus (Worm.MSIL.Cxover and Email-Worm.MSIL.Letum).

It used NetBus programs and the attack person who is a hacker designated the system of oneself with server, under attacking boil virus program and JPG Merge JPG files (picture.jpg) and it used with virus file (Patch.exe) it combined it made it added auto executive it did it made and spam or scanning it led and in the condition which is possible and Autorun functions and with normal JPG file and style is analyzed with vulnerability with the IP which it transmitted the program which it does in the target system and the virus permeated.

Fig. 6 HTS whole aspect security programs establishes with ActiveX and i-DEFENSE is set in HTS program execution at the time of and it means that the Windows Defender warning floats in about virus attack.

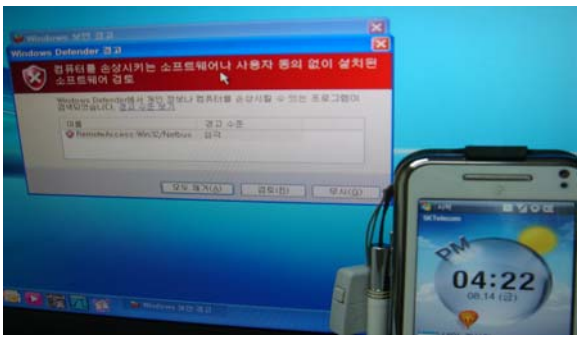


Fig. 6 Defender warning screen about virus attack

## 4.2 In about authentication packet attack analysis

The user input input-information from the situation where i-DEFENSE where it is a security program from the terminal of the mobile stock trading system which is the attack objective object is operated. HTS user ID deux852, connection password cws852, user authentication number deux **** it input. Already PC and patch files which are NetBus Client execution files which come to permeate to the notebook are executed.

Fig. 7 leads Paros and i-DEFENSE executes and with authentication server together it updates prosecuting attorney and virus Rule virus (BackDoor.Beizhu.2360 (2), Trojan.DownLoad.38444 and Win32.HLLW.Aytoruner.6326 (16) etc.) and ID and PW, authentication it stands it is a collection of forensic fundamental data which execute a computer virus scanning about etc.

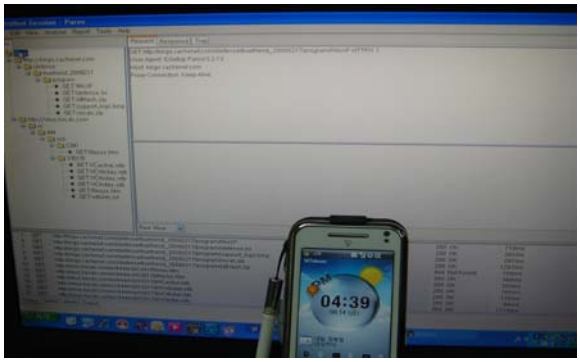


Fig. 7 Stock trading server folder and contents chase that use Paros

They are keylogger, programs it used All in One Keylogger v3.2 where and when the user inputs with the entry device every, Fig. 8 comes like the user where the critical intelligence contents of the user is identical in the screen of the hacker created entry device contents. The input contents of the namely user is exposed immediately to the screen of the hacker and the attack of the hacker succeeds and it is to seem. To about the connection terminal authentication packet of the namely hacker there being a security vulnerability to about keylogger attacks, it is to seem.

Fig. 8 Hacked user screen Capture that use Keylogger

The Fig. 9 the entry device leads from Keylogger programs and they are keylogging one data which appear in the monitor of the hacker.


Fig. 9 When input user through Keylogger, hacker's data collection screen

The data which the user inputs from Fig. 9 (aaaa1111aaaa1111aaaa1111) there is a possibility of seeing a contents from the screen of the hacker, the data which becomes password leads and in the condition which is encrypted from the terminal screen of the hacker a decode program, the screen which becomes the cap with the entry device every input hour it appears there is and the hacking possibility is a possibility of knowing the thing.

## 4.3 WiBro network attack analyzes

Use WiBro, from mobile stock tradings which networks VM from mobile communication terminals, downloading transactions stock company name and account number, after inputting account information of account ID and account password etc. from web, mobile communication terminal crossroad it transmits and it stores in account DB of mobile communication terminals the phase which it passes by.

Mobile stock trading system terminals AccessPoint lead from communication phase and with wired-network connection scanning it is under they lead and AccessPoint MAC address (00:0 A:7d:98:0d:01) where it finds out with MAC address of oneself and with AccessPoint and in the terminal and they change in about the terminal stomach in about AccessPoint stomach packet where it becomes accomplished from WiBro network and from like picture 11 and it analyzes the ID (deux852) of the user it comes to know system evening sunlights (Windows XP ((2600.Service Pack3)) Genuine Intel (R) CPU T2400 @ 1.83GHz NVIDIA GeForce Go 7400) of the user.

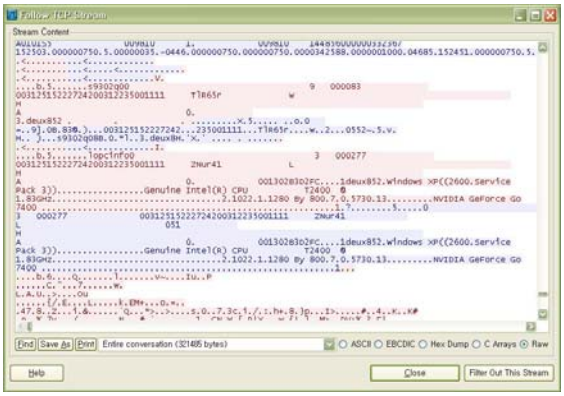


Fig. 10 Mobile stock trading person's ID and user systerm specifications contents data Capture in WireShark

## 4.4 WiBro mobile communication terminal attack analyzes

The communication terminal of WiBro carrying Internet information handling capacity the fixation style mammary gland terminal than writes more relatively is the critical point of the mobile terminal which. Advantage it aims and it executes DDoS attacks in about WiBro mobile communication terminals.

Scanning it led and currently it knew in about the IP to use DDoS HTTP 2.0 attack tools 80port it led and at per second 102,400Byte/50 time and traffic an attack PING of Death attacks it conducted the mortar it made the IP address (125.152.11.96) and of WiBro users. Attack result security contact service inside 2 minutes it cannot service where delay making users are smooth, it paralyzes the use of the user stock trading terminal.

Fig. 11 was the screen which records the result which receives DDoS attacks in WiBro terminals, WiBro the user service of the communication terminal stood still and the connection was wrong.

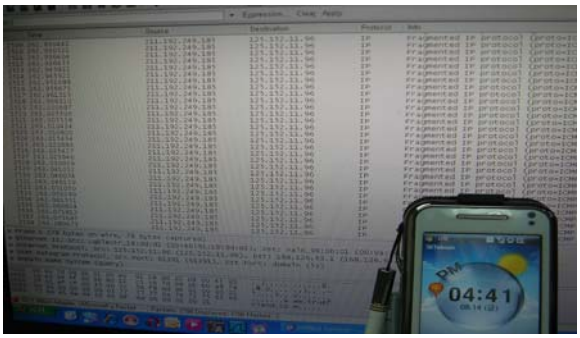


Fig. 11 Mobile terminal analysis that is attacked by DDoS

### 4.5 WiBro mobile HTS program attack analyzes

When with stomach AP the user with HTS programs like Fig. 13 and the user does a buying over order like item number and from Fig. 13 which it orders from "Mini stocks order" items and, when it tries to analyze capture one packet and there is a possibility of seeing the fact that the item number(034600) is identical from packet analyzes where the item number(034600) of Fig. 13 has become capture of Fig. 14. Packet where from namely HTS programs it becomes accomplished from the network as a matter of was not becoming the encryption which it listens not to be, the vulnerability which is the possibility of knowing a transactions particulars from attack analysis of the hacker was discovered. Also keylogger programs it will lead and order water content of the user it will be able to grasp.


Fig. 12 HTS program purchase item number order

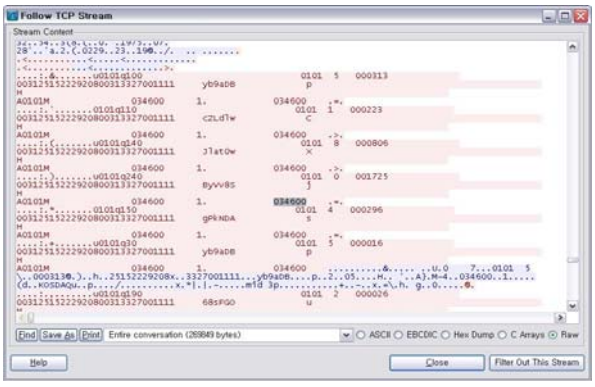


Fig. 13 HTS program purchase item number packet collection

### 4.6 The infringement which it follows in attack (damage) and vulnerability analysis

With the stock trading which uses WiBro being the carrying Internet from up experiment the same financial service plentifully was activated, ID and Password, electronic authentication it stood and HTS programs a vulnerability in about program, and system about transactions particulars etc. it leads it analyzed the attack which leads the vulnerability which is analyzed Forensic fundamental data it executed it created. Table 2 the tool by infringement which it follows in attack (damage) is to show the data which analyzes an analysis and a vulnerability.

Table 2: WiBro Mobile stocks transaction security stability infringement limitation

| ***Attack dividing*** | ***Attack tool*** | ***Infringement (damage)*** | ***Vulnerability*** |
|---|---|---|---|
| Virus permeation attack | NetBus | With spam or IP influx | Open wireless internet network |
| Authentication packet attack | KeyLogger, Monitoring program | "Actually" the disapproval prevention ineffectiveness and security in only password dependence, keyboard security program necessity | Service provision yes or no in plug-in manufacturers dependence, Very low-end generality, Certificate possession transaction possibility |
| WiBro network attacks | Phishing, Pharming, VoIP eavesdropping /monitoring | In ACR TCP syn and ICMP attack and IP spoofing attack | 802.16e safety yes or no, illegal RAS simulations |
| WiBro mobile terminal attacks | DDoS attack | Reproduction terminal use and illegal watch connection | VoIP eavesdropping possibility, DoS(DDoS) |
| WiBro mobile HTS program attacks | KeyLogger, Monitoring program | Keyboard security program (encryption) necessity | Open connection, in transmission packet data exposure |

Like dignity contents and the stock trading right time vulnerability from WiBro carrying Internet will be discovered, when considering the importance of financial transactions, the security reinforcement is necessary in about vulnerability.

## 5. Conclusion

Financial transaction value from the carrying Internet which uses WiBro it is activated from the present paper and also the transactions which uses HTS programs from mobile stock tradings is activated.

It connects by WiBro, packet where between server and the wool mobile terminal it exchanges from stock trading from mobile wireless network environment which networks and system it analyzed capture receiving vulnerabilities, the attack which leads the vulnerability which is discovered it executed. It analyzed mobile HTS program and the network of mobile stock tradings from WiBro and the scanners and packet analytical tools and the stock trading process which becomes accomplished actual it used monitoring it did and a vulnerability and packet and it analyzed it sought, an attack and a vulnerability, forensic fundamental data in about damage occurrence virus permeation attack analysis and authentication packet analysis, network attack analyzes, terminal attack analyzes and HTS programs it executed it analyzed it created.

From hereafter research from the carrying Internet WiBro which is discovered at this time in about vulnerability of stock trading system above securing the stability and a security characteristic of security method and security measure and financial transactions, necessary in about basis of assessment with standardization of one financial security machinery and tools the research is.

## References


[1] Hyeong-Yu Jang, "A Study to Promote Use and Reuse Intention in Electronic Banking Service : Focused on Internet Banking and Mobile Banking", KIECA, Journal of KIECA, Vol. 9. No. 1. pp. 307-330, March 2009.

[2] Smirni,http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=101&oid=001&aid=0002291156

[3] Ki-Hwan Kim, Dea-Woo Park, "A Study on Extraction of Mobile Forensic Data and Integrity Proof", KSCI, Journal of KSCI, Vol. 12. No. 6. pp. 177-185, December 2007.

[4] W Han, Y Wang, Y Cao, J Zhou, L Wang, "Anti-Phishing by Smart Mobile Device," IFIP International Conference, Network and Parallel Computing Workshops, 2007.

[5] T Yamakami, T ACCESS, "MobileWeb 2.0: Lessons from Web 2.0 and Past Mobile Internet Development," Multimedia and Ubiquitous Engineering, 2007.

[6] A Raniwala, T Chiueh, "Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network," IEEE Computer and Communications Societies, Proceedings IEEE, 24th Annual Join, INFOCOM 2005.

[7] Jeong-sik Yang, Jae-beom Hong, "The influence that the customer's characteristics have on the service quality, customer satisfaction and behavioral intention in on-line stock trading system", KIECA, Journal of KIECA, Vol. 6. No. 1. pp. 287-306, June 2006.

[8] Mahmoud Reza Hashemi, Elahe Soroush, "A Secure m-Payment Protocol for Mobile Devices," Electrical and Computer Engineering, Canadian Conference, 2006.

[9] MN Doja, N Kumar, "Image Authentication Schemes against Key-Logger Spyware," Ninth ACIS International Conference, 2008.

[10] Yong-Bong Yoo, "Strafrechtliche Ueberlegung des Phishingkriminalitaet", Korean Police Studies Association, Korean Police Studies Review, Vol. 6. No. 3. pp.277-298, December 2007.

[11] Yang-Seo Choi, Dong-Il Seo, "The private data outflow technique which leads a social engineering method of attack and confrontation plan analysis", KIISC, Journal of KIISC, Vol. 16. No. 1. pp. 40-48, February 2006.

[12] http://www.fnnews.com/view?ra=Sent1201m_View&corp=fnnews&arcid=0921270838&cDateYear=2008&cDateMonth=03&cDateDay=30

[13] Hee-Hwan Park, Dea-Woo Park, "A Study on New Treatment Way of a Malicious Code to Use a DLL Injection Technique", KSCI, Journal of KSCI, Vol. 11. No. 5. pp. 251-258, November 2006.

[14] Dea-woo Park, "A study about dynamic intelligent network security systems to decrease by malicious traffic," IJCSNS, International Journal of Computer Science and Network Security, Vol. 6, No. 9. pp. 193-199, September 2006.

[15] Dea-Woo Park, Jeong-Man Seo, "A Study of Security Method against Attack in TCP/IP", KSCI, Journal of KSCI, Vol. 10. No. 5. pp. 217-226, November 2005.

[16] A Orebaugh, G Ramirez, J Burke, "Wireshark & Ethereal network protocol analyzer toolkit," ISBN 1597490733, 9781597490733, Syngress 2007.


**WooSung Chun** received the B.S. degrees in Information Communication Security from Soongsil University Computer Institute, South Korea in 1999, respectively. Dr. Chun received the B.S. degrees in Information Communication Security from Hoseo Graduate School of VENTURE, South Korea in 2008. His interests include Information Security of computer and networks, Ubiquitous Computing, Web Programming, Mobile Communication, Forensic.

**Deawoo Park** is an Adjunct Professor of IT Application Science Department at the Hoseo Graduate School of VENTURE, South Korea. Dr. Park received the B.S. degree in computer science M.S. degree in 1998. He received the Ph.D. degree from the computer science department of the Soongsil University in 2004. His interests include Information Security of computer and networks, Ubiquitous Computing, Mobile Communication Security, and Forensics.