THE EFFECT OF VULNERABILITIES AND THREATS ON HOME COMPUTER SECURITY IN NIGERIA.

BY

GLORIA NGOZI ORAGUI B.ENG ELECTRICAL ELECTRONICS ENGINEERING
(ELECTRONICS AND COMPUTER OPTION)
(20094699188)

A THESIS SUBMITTED TO THE POSTGRADUATE SCHOOL FEDERAL UNIVERSITY OF TECHNOLOGY, OWERRI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE (MASTER OF SCIENCE), M.Sc. IN (INFORMATION MANAGEMENT TECHNOLOGY)

OCTOBER, 2012

CERTIFICATION

I certify that this work "The Effect of Security Vulnerabilities and Threats on Home Computers in Nigeria." was carried out by Oragui Gloria Ngozi (Registration Number 20094699188) in partial fulfillment for the degree of (Masters of Science in Information Management Technology) of the Federal University of Technology Owerri.

……. ……

DR. B. C. ASIEGBU **DATE**

PROJECT SUPERVISOR

…… ……..

DR MRS F. EZE

HEAD OF DEPARTMENT **DATE**

…… ……..

PROF. NZOTA

DEAN S.M.A.T **DATE**

…… ……..

ENGR. PROF. MRS K.B. OYOH

DEAN POSTGRADUATE **DATE**

…… ……..

Dr. Ukadia

EXTERNAL EXAMINER **DATE**

DEDICATION

I dedicate this thesis to My Unique Parents Mr & Mrs Dennis Oragui who have given me a decent education also to my lovely sisters Dr. Peace Oragui an Angel on Earth, Chartered Accountant N.K Oragui and my other siblings who God Used for Reality.

ACKNOWLEDGMENT

I wish to thank my Supervisor Dr. B.C. Asiegbu for his smart advices, directions and guidance throughout my research work. I thank you Sir.

I also wish to thank the persons who took part in my user survey. Their collaboration was very important for this thesis. And I will not forget to acknowledge all the books, journals, websites that are mentioned within.

In a very special way, Am expressing my gratitude to Mr. and Mrs. Dennis Oragui, my parents for being there for me at any time of the day and their contributions toward the successful completion of this work.

Persons like Engr. Dr. Sir Jek Obichere (Lecturer E.E.E. FUTO) and lovely Engr. Gold Ogoo Ezekwonna who has been so Wonderful.

My entire Course Mates especially Rtrd. Comdr. Nathaniel Nnadi, Our Course Rep. Ifeanyi and others who contributed one way or another during the course of my study.

I believe that the study area of this thesis will become significantly more important in the future.

TABLE OF CONTENTS

ABSTRACT

This thesis examined some security related issues that might be unknown to computer users in Nigeria. It addressed the security vulnerabilities and flaws in most popular home computer operating systems. The study also concentrated on important computer security issues like worms, spyware, viruses etc. The researcher used the survey method for data collection via questionnaire method; therefore the data collection system in the research is primary data. The research reviewed previous works and publications in this area (computer security) by looking at books, articles, and research reports etc. Data collected from the survey on Home Computer Security threats like Virus or Worms, Spyware, Firewall, Operating System, Internet & Email were subjected to multiple regression using SPSS software. The output displayed in the Anova Table 4.4 at 0.05 level of significance showed that there is significance effect of vulnerabilities and threats on home computer security in Nigeria. The research also revealed from findings that many home computer users in Nigeria do not practice security at all or are ignorant to practice security, while some users are unaware of different security vulnerabilities and the ways to combat them. The work recommended solutions to improve security and eradicate vulnerabilities and threats on home computers in Nigeria, the major solution being awareness through media, schools, public places and any other places where computer security is required. In conclusion, computer security issues are important when one considers national productivity and economic development through enhanced information and communication technology services in Nigeria.

CHAPTER ONE

1.0 Introduction

1.1 The Background of the Study

Today there exists a computer in almost every home in developed countries, and even though the less developed world are still far behind, computerization is increasing fast. The huge amount of home computers and the massive Internet usage has improved the information flow in various ways. People now have access to the information they need around the clock and can electronically communicate with people around the world. It is hard to list all the benefits, but there are also some important problems that need to be addressed. Ordinary people have basically unwillingly become system administrators of their own home computers. Most of them don't have any basic knowledge on how to protect their computers from the ever increasing threats on the Internet. Malicious code writers use the Internet to launch various attacks on computer systems around the world. Organized crime uses the Internet to steal important information such as credit card numbers. Shady corporations install programs that monitor surfing patterns without the knowledge of the users.

The current situation shows that many home PCs both in the country and abroad have become victims of virus and worm infections, DDOS agents and many others as discussed in the paper. Based on my observation, the increasing number of worms transmitted via emails affecting home users are as a result of unawareness of the threat and improper countermeasures such as safe handling of email attachments and not keeping an updated anti-virus in their PCs. CERT Incident IN-2001-07 has reported of a new worm targeting home users running on Windows operating system, W32/Leaves worm, discovered in July 2001 and CERT Advisory CA-2001-20 has reported of over 23 000 machines had been infected with this worm.

Lemos Robert in his article in ZDNet News (February 16, 2000), (Retrieved from <http://www.kb.cert.org/vuls/id/492515, accessed 29 September 2011) has quoted Eugene Spafford (2006), a computer science professor and security expert from Purdue University that home users don't have the right security

tools and understanding about why they need them and they are much more likely to be prone to attack or their machines used in DDOS, coordinated attacks.

Therefore what is the state of home computer security in Nigeria today? What are the threats against home computer users in Nigeria today? And what can be done to improve the current situation? These are the questions that this thesis will try to answer.

1.2 Statement of Problem

With the increase in numbers of home PC come many associated issues, a key one being information security which give rise to the importance of information security. Home computer users, now a significant part of this interconnected world, do not have the knowledge of threats and vulnerability, even if they do many are ignorant of it and neglect to use even the most basic computer security solutions available even with the current threat of numerous types of security exploits present in online computing activities, while some do not want to practice security at all.

Reasons for this behavior have yet to be satisfactorily explained.

Information security is a foundational element of every country starting from home computer, so computer users need to address this critical issue.

On the basis of the difficulties stated above, this work is geared towards examining the effect of Security Vulnerability and threats on Home Computers in Nigeria.

1.3 Research Objectives

The main objective of the study is to recast to include the specific objectives effect of security vulnerability and threats on home computer in Nigeria.

The specific objectives include:

1. To identify computer security vulnerabilities and threats.

2. To examine the effect of computer security vulnerabilities and threats as a whole on home computer.
3. To examine the effect of each computer security vulnerabilities and threats on home computer.
4. To make policy recommendation based on the findings of this work.

1.4 Research Questions

On the reason of the statement of the problem and objectives of the study, the researcher poses the following questions to herself:

1. What are the computer security vulnerabilities and threats?
2. To what extent are the computer security vulnerabilities and threats as a whole affected home computers in Nigeria?
3. To what extent has each computer vulnerability and threats affected home computers in Nigeria?
4. What policy recommendation can be made?

1.5 Research Hypothesis

On the basis of the statement of the problem, objectives of the study and research questions, the following research hypothesis have been formulated:

Ho_1: There is no significant effect of computer security vulnerabilities and threats as a whole on home computer.

Ho_2: There is no significant effect of each computer security vulnerability and threats on home computer.

1.6 Scope and Limitation of the study

This thesis will focus on the home computer users, security vulnerabilities in the most common operating systems and applications of today, different kinds of threats against home computers such as worms, virus, and spyware. The thesis will also try to recommend some measures in order to improve home computer security in the future.

This thesis will not focus on issues related to physical security such as thefts and hardware failures, nor issues related to wireless connectivity, telecommuting(long distance communication by the use of telephone, radio, television, etc) and corporate(organisations) laptops used at home. Security problems related to future not yet mainstream technology such as Internet connected consumer electronics and has also been left out on purpose. One other important topic that won't be addressed in this thesis is the spam problem.

The limitations faced in the course of carrying out these studies:

i. Limited time
ii. Inadequate literature and materials
iii. Reluctance on the part of home computer users to speak their minds freely
iv. Lack of adequate funds

Considering the fact that with the limitations, the researcher is not able to move round the whole nation considdering the financial aspect involved. In order to circumvent this bottleneck, the researcher had to devise an easier way by reducing the sample size of interview respondents and hence adopting a convenience representative sampling method.

The study was also constrained by the limited time considering how many trips was involved and meeting adequately the schedules of the respondents. Also, the researcher was constrained by time seeing she had to combine her personal work schedule with the several trips to and from one location to another.

Also the reliability as well as integrity or validity of the data collected was influenced by the fact that due to confidentiality considerations most of the people interviewed were constrained in releasing as much information as might be deemed necessary for a thorough research due to shyness, being uneducated and language barriers. However, these limitations have been taken care of that they do not affect the results of the study.

1.7 The Significance of the study

The significance of this study can be seen in the fact that computer security can be applied in the development of national policy framework as a guild to home users through advertising, press, education and other type of awareness program to facilitate economic and social growth. In this respect the study will improve our understanding of the following issues as they apply in the Nigerians situation.

- The relevance of computer security for home computer users for a developing country like Nigeria
- Expected benefits derived by impacting computer security to home computer
- The barriers that prevent home computer users from applying computer security
- The challenges home computer users encounter when applying home computer security

1.8 Justification of the Study

The result of the study will provide security measures against computer vulnerabilities and threats for home computer users, general public, government and the nation at large or any other body who have been under computer vulnerabilities and threats of several sorts.

Home computers if properly managed and secured will help in any other area involving computer security and thereby enhancing the economic productivity of the country. In respect to the statement above, this work therefore seek to identify and provide effective computer security solution to home users.

1.9 Organization of the Work

This dissertation is divided into five chapters. Chapter one contain the background of the study which provides a general overview of the research topic, statement of the problem, the research objectives; questions, hypothesis, scope and limitation; significance of the study and the document in general.

Chapter 2 provides the literature review. This chapter from data collected, that windows being the most used operating systems reviews the theoretical and

empirical literature pertaining to Security of Windows XP Home Edition, Windows 7 as case studies, their vulnerabilities and threats.

Chapter 3 presents the methodology, the method and source used, also describes the population, the full data collection, the sample selection, the user survey and results of the study.

Chapter 4 discusses the data analysis. The model used is also presented. Additionally, the model also includes the demographic moderators of gender, age, and education. Finally, the dependent variable, computer security is taken from the security literature and Chapter 5 discusses summary, recommendation, possible solutions and conclusion.

CHAPTER TWO

2.0 Literature Review

2.1 Historical Development of Home Computer and Threats

The growing use of broadband connections gives home computer users faster and "always on" access to the Internet. These home computer users are often unaware of how to protect themselves from getting successfully attacked. Broadband and "always on" connections together with security unaware users has made home computer users the prime target for recent virus and worm attacks; however it doesn't stop with that, home computer users are also the prime target of scammers and companies with shady business practices.

This chapter focused on the technical aspects of home computer security. It will not focus on the pure "social engineering" aspect when a user is tricked into installing a malicious program; however it is important to know that design flaws, bugs and too slack default settings is often used by attackers to trick the user into running such malicious code. Microsoft Windows, the preferred choice of operating system among home computer users, can be configured in secure ways, but default installations are often very insecure due to bugs and slack default security settings. Home computer users without enough knowledge and interest in computers are unlikely to change default settings in Windows in order to improve their computer security. This chapter will show how such slack default security settings is the main problem from a technical point of view today.

2.1.1 Relevant Operating Systems

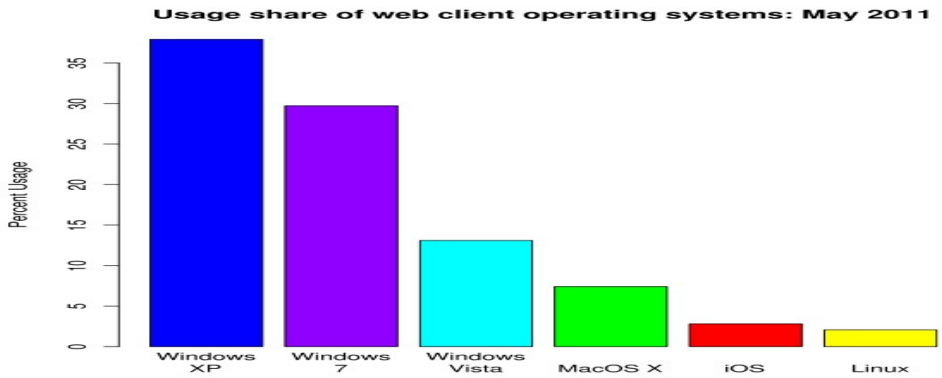

Figure 2.1 Usage Share of Web Client Operating Systems: May 2011

Source: Upload.wikimedia.org/w accessed 28 September, 2011.

2011	Win 7	Vista	Win 2003	Win XP	Linus	Mac	Mobile
June	37.8%	6.7%	0.9%	39.7%	5.2%	8.1%	0.9%
May	36.5%	7.1%	0.9%	40.7%	5.1%	8.3%	0.8%
April	35.9%	7.6%	0.9%	40.9%	5.1%	8.3%	0.8%
March	34.1%	7.9%	0.9%	42.9%	5.1%	8.0%	0.7%
February	32.2%	8.3%	1.0%	44.2%	5.1%	8.1%	0.7%
January	31.1%	8.6%	1.0%	45.3%	5.0%	7.8%	0.7%
2010	**Win 7**	**Vista**	**Win 2003**	**Win XP**	**Win 2000**	**Linus**	**Mac**
December	29.1%	8.9%	1.1%	47.2%	0.2%	5.0%	7.3%
November	28.5%	9.5%	1.1%	47.0%	0.2%	5.0%	7.7%
October	26.8%	9.9%	1.1%	48.9%	0.3%	4.7%	7.6%
September	24.3%	10.0%	1.1%	51.7%	0.3%	4.6%	7.2%
August	22.3%	10.5%	1.3%	53.1%	0.4%	4.9%	6.7%
July	20.6%	10.9%	1.3%	54.6%	0.4%	4.8%	6.5%
June	19.8%	11.7%	1.3%	54.6%	0.4%	4.8%	6.8%
May	18.9%	12.4%	1.3%	55.3%	0.4%	4.5%	6.7%
April	16.7%	13.2%	1.3%	56.1%	0.5%	4.5%	7.1%
March	14.7%	13.7%	1.4%	57.8%	0.5%	4.5%	6.9%
February	13.0%	14.4%	1.4%	58.4%	0.6%	4.6%	7.1%
January	11.3%	15.4%	1.4%	59.4%	0.6%	4.6%	6.8%
2009	**Win 7**	**Vista**	**Win 2003**	**Win XP**	**Win 2000**	**Linus**	**Mac**
December	9.0%	16.0%	1.4%	61.6%	0.6%	4.5%	6.5%
November	6.7%	17.5%	1.4%	62.2%	0.7%	4.3%	6.7%
October	4.4%	18.6%	1.5%	63.3%	0.7%	4.2%	6.8%
September	3.2%	18.3%	1.5%	65.2%	0.8%	4.1%	6.5%
August	2.5%	18.1%	1.6%	66.2%	0.9%	4.2%	6.1%
July	1.9%	17.7%	1.7%	67.9%	1.0%	4.3%	6.0%
June	1.6%	18.3%	1.7%	66.9%	1.0%	4.2%	5.9%
May	1.1%	18.4%	1.7%	67.2%	1.1%	4.1%	6.1%
April	0.7%	17.9%	1.7%	68.0%	1.2%	4.0%	5.9%
March	0.5%	17.3%	1.7%	68.9%	1.3%	4.0%	6.0%
February	0.4%	17.2%	1.6%	69.0%	1.4%	4.0%	5.8%
January	0.2%	16.5%	1.6%	69.8%	1.6%	4.0%	5.8%
2008	**Vista**	**Win 2003**	**Win XP**	**Win 2000**	**Win 98**	**Linux**	**Mac**
December	15.6%	1.7%	71.4%	1.7%	0.1%	3.8%	5.3%
November	15.1%	1.6%	72.0%	1.8%	0.1%	3.8%	5.3%
October	14.4%	1.7%	72.0%	1.9%	0.2%	3.8%	5.5%
September	13.2%	1.8%	73.3%	2.2%	0.2%	3.8%	5.2%
August	12.5%	1.9%	73.9%	2.4%	0.2%	3.9%	4.9%
July	11.5%	2.0%	74.7%	2.6%	0.2%	3.9%	4.8%
June	10.0%	1.9%	74.6%	2.6%	0.2%	3.7%	4.8%
May	9.3%	1.8%	74.0%	2.9%	0.3%	3.6%	4.7%
April	8.8%	1.9%	73.3%	3.3%	0.5%	3.7%	4.6%
March	8.5%	1.9%	72.7%	3.7%	0.6%	3.9%	4.4%
February	7.8%	1.8%	72.4%	4.0%	0.8%	3.8%	4.3%
January	7.3%	1.9%	73.6%	4.0%	0.8%	3.6%	4.4%
2007	**Vista**	**Win 2003**	**Win XP**	**Win 2000**	**Win 98**	**Linux**	**Mac**
November	6.3%	2.0%	73.8%	5.1%	1.0%	3.3%	3.9%
September	4.5%	2.0%	74.3%	5.4%	0.9%	3.4%	3.9%
July	3.6%	2.0%	74.6%	6.0%	0.9%	3.4%	4.0%
May	2.8%	1.9%	75.0%	6.5%	0.9%	3.4%	3.9%
March	1.9%	1.9%	76.0%	7.2%	0.9%	3.4%	3.8%
Jan	0.6%	1.9%	76.1%	7.7%	1.0%	3.6%	3.8%

2006	Win 2003	Win XP	Win 2000	Win 98	Win NT	Linus	Mac
November	1.9%	74.9%	8.0%	1.0%	0.3%	3.5%	3.6%
September	2.0%	74.6%	9.2%	1.4%	0.3%	3.5%	3.6%
July	2.0%	74.3%	10.1%	1.5%	0.3%	3.4%	3.6%
May	2.0%	74.2%	10.7%	1.6%	0.2%	3.4%	3.6%
March	1.8%	72.9%	11.9%	2.0%	0.3%	3.4%	3.5%
Jan	1.7%	72.3%	13.1%	2.4%	0.3%	3.3%	3.5%
2005	**Win 2003**	**Win XP**	**Win 2000**	**Win 98**	**Win NT**	**Linus**	
November	1.7%	71.0%	14.6%	2.7%	0.4%	3.3%	
September	1.7%	69.2%	15.8%	3.2%	0.5%	3.3%	
July	1.6%	65.3%	17.7%	3.9%	0.6%	3.5%	
May	1.4%	64.5%	19.4%	3.9%	0.8%	3.3%	
March	1.4%	63.1%	20.2%	4.7%	0.9%	3.2%	
January	1.2%	61.3%	21.6%	5.3%	1.0%	3.2%	
2004	**Win XP**	**Win 2000**	**Win 98**	**Win NT**	**Win95**	**Linux**	**Max**
November	59.1%	23.7%	5.6%	1.2%	0.1%	3.1%	2.7%
September	55.9%	26.2%	6.4%	1.5%	0.2%	3.1%	2.6%
July	52.5%	28.4%	7.5%	1.9%	0.2%	3.1%	2.4%
May	51.0%	29.6%	8.2%	2.0%	0.3%	2.9%	2.5%
March	48.0%	31.1%	9.4%	2.4%	0.4%	2.6%	2.4%
January	44.1%	33.6%	10.4%	3.0%	0.4%	2.7%	2.4%
2003	**Win XP**	**Win 2000**	**Win 98**	**Win NT**	**Win 95**	**Linux**	**Mac**
November	42.6%	36.3%	10.9%	3.5%	0.4%	2.6%	2.2%
September	38.0%	37.9%	12.1%	4.1%	0.5%	2.4%	2.0%
July	33.9%	40.6%	12.6%	5.3%	0.6%	2.3%	1.9%
May	31.4%	41.0%	13.9%	5.8%	0.7%	2.2%	1.8%
March	29.1%	41.9%	14.8%	6.6%	0.8%	2.2%	1.8%

Table 2.1 Operating Systems Platform Statistics

Source: www.w3schoolslog.files accessed 28 September 2011.

From the above table 2.1 and figure 2.1, a few noteworthy things are found in this statistics:

The Statistics is collected from W3schools log-files over a period of seven (7) years. Windows XP is the most popular operating system followed by Windows 7, alternatives to Microsoft Windows mainly Linux and MacOS have got a very small market cap. The statistics visualizes the ratios between different operating systems on usage share of web client operating system, not the ratios between operating systems used at home. The statistics still provides a rough estimate on which operating systems was the most popular ones at the time of writing.

The statistics includes both corporate users and home users. Windows 7 is the latest release of Microsoft Windows, a series of operating systems produced by Microsoft for use on personal computers, including home and business desktops, laptops, notebooks, tablet PCs, and media center PCs according to

Microsoft Security Bulletin (2011, Pg. 1). Windows 7 was released to manufacturing on July 22, 2009, Ricciuti, Mike (2007). CNET News Ricciuti, Mike (2007) and reached general retail availability on October 22, 2009, from Microsoft, (2009) Accessed 2011-09-28, less than three years after the release of its predecessor, Windows Vista. Windows2000 was aimed primarily at the corporate market while Windows 98 was primarily aimed at the consumer market. Windows XP targets both the corporate and the consumer market. One other important observation is that Windows 98 is more often used on older computers than Windows XP. An old computer is less likely to be connected to the Internet than a new one. This leads to the conclusion that Windows 98 actually had a larger market cap when studying home computers only, while Windows 2003 and 2000 had a smaller market cap.

This chapter will focus on the two most common operating systems: Windows XP Home Edition and Windows 7. Windows 2003, and 2000 will not be treated primarily due to the similarities with Windows XP and the corporate profile also Window Vista similarities with windows 7. MacOS and Linux will not be covered because of their low market cap.

2.2 Security Vulnerabilities and threats impacts

2.2.1 Case study: Windows XP Home Edition

Windows XP Home Edition is the most popular operating system used by home computer users today. Its importance is expected to grow as old computers that are running Windows 98 are upgraded or replaced by new ones. This case study will focus on the default settings of the operating system and their importance from a user security perspective. The reason for focusing on the default settings is that most default settings are unlikely to be changed by the end user and that they affect security maybe more than anything else. A clean copy of Windows XP Home Edition was installed and used in this case study to examine what is good and what is not so good out of a security user perspective.

2.2.1.1 Initial Vulnerabilities

Windows XP Home Edition contains several remotely exploitable vulnerabilities [MS03-026, MS03-039, MS03-043, MS04-011] in its initial state. Vulnerabilities that allow an attacker to take control of the computer as soon as it is connected to the Internet or any other infected network unless special precautions are taken. Some of these initial vulnerabilities have successfully been exploited by the Blaster and Sasser worms and their variants.

The Blaster and Sasser worms are still active on the Internet. This makes Windows hard to update without getting infected since the preferred way of updating Windows is to connect to the Internet and run Windows Update. Windows XP Home Edition also contains numerous other vulnerabilities that allow attackers to take control of the computer if the user can be tricked into visiting a specially crafted web page, or by receiving a malicious email, or by playing an audio file, or by opening a help file...

2.2.1.2 Windows Update

No information was given to the user that Windows needed to be updated after the installation. The user gets notifications about registering Windows and about registering a passport account for MSN Messenger, but not any security notifications. The Windows Update icon is not found in the main start menu. The user has to click on the programs submenu to find the Windows Update icon. Windows is set to automatically download new patches from Windows Update and prompt the user when they are ready to be installed. Windows does not automatically download new patches before Service Pack 1 is installed. Service Pack 1 has to be downloaded and installed manually through Windows Update. At first the service pack was installed and the computer was restarted. No indication that there were more available patches to download were initially given, but after a while windows had found them and reminded the user that there were new available updates to install.

2.2.1.3 Access Control

Windows XP and other Windows NT based operating systems utilizes Access Control Lists, ACLs to restrict or allow access to objects in the operating system. Processes, user accounts, resources, files, directories, etc., are all objects of a certain type according to Dieter Gollmann (1999),. This security model is very flexible and allows Windows XP Professional to be configured in very secure ways. The fine grained security model of Windows XP Professional has been simplified in Windows XP Home Edition. There exist two different levels of rights available for users: computer administrator and limited. An account with administrator privileges has access to the whole computer. An account with administrator privileges can create and delete user accounts, install programs and delete files belonging to any user. A limited account can't install most programs, can't access some files on the computer, can't create and change settings in the computer that would affect other users. By default new users are given administrator privileges as shown in Figure 2.2 below.

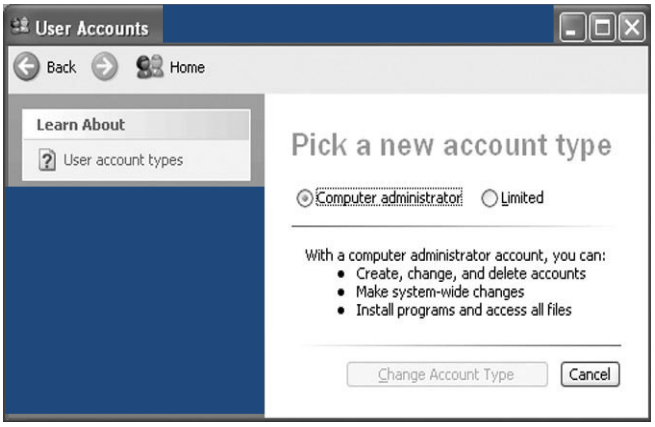

Figure **2.2.** Available user privileges in Windows XP Home Edition.

A default user is created during the installation. This default user is given administrator privileges and is automatically logged on to the system. It is easier to run as an administrator, since the user then has got full access to everything. This also means that potential attackers that successfully gain access to the computer through a program the user is running automatically gets administrator privileges. The preferred way from a security point of view would be to give the default user limited privileges only, but this will make things more complicated for the user. This illustrates one of the main problems of

computer security today: in order to get a secure system the user has to be restricted, but if the user is restricted too much the computer isn't usable anymore.

2.2.1.4.1 Hidden File Extensions

Windows XP Home Edition hides extensions for known file types by default to make things easier for the user. This is not completely transparent to the user since the user still has to deal with file extensions in some application programs. This weakness is often used by email worms to trick the user into opening an executable attachment. The user might receive an email containing a file with a double file extension, e.g. *ILOVEYOU.TXT.VBS* but will only see *ILOVEYOU.TXT* and open it, because text files are harmless and contain no worms... This technique of using double file extensions is commonly used by today's email worms. The ILOVEYOU.TXT.VBS is a real example of a worm called I Love.

2.2.1.4.2 Show File extensions

It is possible for the user to enable file extensions by changing a setting in Windows Explorer. However some file extensions remain hidden even after changing this setting according to the U.S. National Security Agency (NSA) from Paul Bartock Trent Pitsenbarger (2003). Some of these hidden file extensions might masque malicious code. These hidden file extensions are mainly different types of links including shortcuts *.lnk* and Internet shortcuts *.url*.

2.2.1.5 Email Settings

This case study will focus on the built in email program, Outlook Express 6.0. This Outlook version offers the options: "*Warn me when other applications try to send as me*" and "*Do not allow attachments to be saved or opened that could potentially be a virus*". Both these options are enabled by default. The first option warns the user when a program or potential worm accesses the address book or tries to send email messages through Outlook Express. Many recent

email worms come with their own email engine and utilizes other sources than the address book to gather email addresses, i.e. scan the file system for email addresses.

The second option blocks potentially harmful attachments. It is best to have both these options enabled out of a security perspective. But the option to block potentially harmful attachments is pretty draconian according to the NSA from Paul Bartock Trent Pitsenbarger (2003) and they suggest that it's possible to disable this setting and rely on perimeter defence, e.g. virus scans at the Internet Service Provider (ISP) and local anti-virus software. Outlook Express 6.0 also uses the *Internet Explorer Security Zones* to determine what should be allowed to run in the emails. The default zone used by Outlook Express is the *Restricted Sites Zone*. The default settings in this zone is already very conservative from a security perspective; however the NSA suggests some alterations to these settings according to Paul Bartock Trent Pitsenbarger (2003). Changing the settings according to NSA's suggestions will counter known attacks that use active content contained within the body of the received email messages.

2.2.1.6 Internet Explorer

A common vector of attack is to trick the user into opening a web page that contains malicious code. In some cases when legitimate sites have been hacked it's not even necessary to trick the user into visiting the pages. The malicious code on the web pages is then loaded on to the user's computer using some known or unknown Internet Explorer vulnerability.

More vulnerability is related to Internet Explorer than any other Windows component. Chances are that Internet Explorer will contain several newfound vulnerabilities if Windows hasn't been updated for a month or two. It is also important to remember that Internet Explorer might open a helper program if it encounters a special file, for example Internet Explorer might open Microsoft Word inside the current window if a word file is encountered. Word might contain vulnerabilities unless it is updated. This means that an attacker can gain

access to a computer if the computer user clicks on a specially crafted word file on the web. Security holes in Internet Explorer are often used to install a special class of programs called spyware. A spyware program might report surfing habits to the program creator, serve ads that the user doesn't want to see, act as an ad-server serving ads to other users on other computers, or change the phone number on the Internet connection (if dialup is used) to an expensive pay number. More information about spyware can be found in sections below. Another disturbing trend is that Trojans stealing information such as credit card numbers, SSNs and online banking passwords is becoming increasingly popular to install this way. More information about trojans can be found in sections below.

2.2.1.7 The Internet Connection Firewall

Windows XP Home Edition comes with a built in firewall called "Internet Connection Firewall" also known as "ICF". This is a basic firewall that blocks incoming traffic not initiated by the computer. It successfully shields the computer against worms exploiting the RPC-DCOM and LSASS vulnerabilities; however this firewall is not enabled by default. The user has to manually enable the firewall. The firewall doesn't protect against potentially malicious web pages that exploit security holes in Internet Explorer. The ICF runs as a normal Windows service which means that it's disabled during start-ups and shutdowns. This allows worms that use the RPC-DCOM or LSASS vulnerabilities to infect vulnerable computers when they are starting up even if the firewall setting is enabled! The firewall is enabled some time after the desktop is presented to the user.

2.2.1.8 Messenger

The messenger service in Windows is not to be confused with MSN Messenger or YAHOO Messenger. The messenger service is enabled by default and allows administrators to send messages to the users using the computers. The messenger service is vulnerable for an attack in its unpatched state that could result in a full system compromise. A patch [MS03-043] is available.

2.2.1.9 System Restore Service

The system restore service backs up selected system and program files so that the system can later be restored into a previous state if something should go wrong. This is usually a desirable service, but it might back up viruses if the computer has been infected. Windows prevents external programs from accessing system restore files including anti-virus programs. Symantec recommend restarting the system restore service after a virus infection. Restarting the service will result in the deletion of old backups that might be infected. Instructions how to do this can be found on Symantec's web site, http://www.symantic.com/about/news/release/article.jsp?prid=20070319_0. Accessed 28 September, 2011. Symantec corp. (2007).

2.2.2 Case Study: Windows 7

Windows 7 is available in six different editions - Starter, Home Basic, Home Premium, Professional, Enterprise, and Ultimate. The different editions of Windows 7 have been designed and marketed toward people with different needs from Microsoft accessed 2nd November, 2011. The Starter edition has been designed and marketed for lower cost notebooks, Home Basic for emerging markets, **Home Premium for normal home users,** Professional for businesses, Enterprise for larger businesses and corporations, and Ultimate for enthusiasts from Microsoft accessed 2nd November, 2011. All editions support the 32-bit (IA-32) processor architecture and all editions except Starter support the 64-bit (x86-64) processor architecture. Windows 7 was released to manufacturing on July 22, 2009, according to Brandon LeBlanc(2009) and reached general retail availability on October 22, 2009, from Microsoft. (June 3, 2009. accessed 2nd Nov. 2011, less than three years after the release of its predecessor, Windows Vista. Windows 7's server counterpart.

Some standard applications that have been included with prior releases of Microsoft Windows, including Windows Calendar, Windows Mail, Windows Movie Maker, and Windows Photo Gallery, are not included in Windows 7;

from Microsoft (www.techpluto.com/softwares-missing-in-windows-7/. Cited 2nd Nov. 2011), most are instead offered separately at no charge as part of the Windows Live Essentials suite according to LeBlance, Brandon (2008).

In this case study the focus will also be on the default setting of the operating system and their importance from a user –security perspective. A clean copy of Window 7 were also installed and used to examine what is good and what is not good out of a security – user perspective.

2.2.2.1 Initial Vulnerability

Ninety percent (90%) of critical windows 7 vulnerabilities are mitigated by eliminating admin rights. The removal of administrator rights from windows users is a mitigation factor for 90% of critical windows 7 vulnerabilities, according to research by beyond trust. The result demonstrated that as companies mitigate to windows 7 they will need to implement a desktop privileged identity management solution, to reduce the risk from an unpatched Microsoft vulnerabilities without inhibiting their users' ability to operate effectively.

Users are also to be blame for the vulnerabilities because of their confusions and problems encountered when trying to move from vista to windows 7. They have difficulties completing the download or installation of the product. They were unable to upgrade from windows vista to the new operating system. Where the user is currently a 32-bit version of windows such as windows vista, but purchased the 64-bit version of windows7 as one cannot lunch setup for the 64-bit version of windows 7 while running a 32-bit operating system. (www.bleepingcomputer.com/virus-remo. Accessed 2nd Nov. 2011.) In Windows 7, the settings have changed for UAC, allowing the system to be more malleable and flexible for users. Certain applications which are digitally signed are fast-tracked through UAC by default to reduce the unnecessary user interaction. To put it simply, through application attached, it allows malware to be automatically elevated to administrator user status which in turn allows it

full, unrestricted access to the computer and global settings. The vulnerability shows itself when this third-party application calls on malicious code “by proxy” (substitute) through an existing Windows application, which never invokes the UAC prompt.

2.2.2.1.1 The consequences

Microsoft have since stated they will not be fixing this flaw as it is “by design”, and Malware can silently elevate with Windows 7’s default UAC. The fact of the matter is, this vulnerability opens up Windows 7 like a cracked nut; exposing the possibility of a malware attack instigated unknowingly by the end user at any given time.

2.2.2.2 Windows Updates

In windows 7 information was given to the user that Windows needed to be updated after the installation, also some other security notifications. The Windows Update icon is found in the main start menu and can be automatically be updating when connected to the internet. Windows is set to automatically download new patches from Windows Update and prompt the user when they are ready to be installed. Windows does not automatically download new patches before Service Pack 1 is installed. Service Pack 1 has to be downloaded and installed manually through Windows Update. At first the service pack was installed and the computer was restarted. No indication that there were more available patches to download were initially given, but after a while windows had found them and reminded the user that there were new available updates to install.

2.2.2.3 Access Control

With window 7, there is now much more control over how user access control can be configured. Before it was either off or on.

1. Open the control panel
2. Click on all control panels items
3. Click on action centre

4. On the top left, click on user account control settings
5. There are now four settings you can choose from

Windows 7 has many services that one may or may not require. By default, there can be many services enabled that one actually don't need and it's one's job to optimize his or her setup for best performance. First of all, one should know how to disable services in Windows 7. One should read the notes about each service and then decide if turning them off is a good idea for one's PC depending on one's needs. It is a list of services that can be safely disabled, but care should be taken on what should be turn off when trying to optimize PC.

The default setting for User Account Control in Windows 7 has been criticized for allowing untrusted software to be launched with elevated privileges without a prompt by exploiting a trusted application from Thadani, Rahul (2010). Microsoft's Windows kernel engineer Mark Russinovich acknowledged the problem, but noted that malware can also compromise a system when users agree to a prompt from Microsoft. Accessed 2nd Nov. 2011.

User Account Control

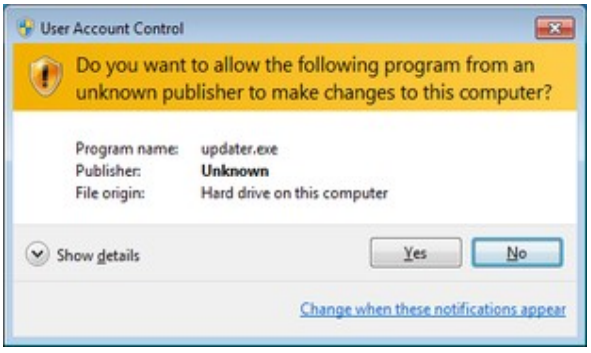

Fig. 2.3 User Account Control dialog in Windows 7 when loading unsigned code

Fig. 2.4 User Account Control dialog in Windows 7 when loading signed code

User Account Control (**UAC**) is a technology and security infrastructure introduced with Microsoft's Windows Vista and Windows Server 2008 operating systems, with a more relaxed version also present in Windows 7 and Windows Server 2008 R2 from the work of Nash Mike (2008). It aims to improve the security of Microsoft Windows by limiting application software to standard user privileges until an administrator authorizes an increase or elevation. In this way, only applications trusted by the user may receive administrative privileges, and malware should be kept from compromising the operating system. In other words, a user account may have administrator privileges assigned to it, but applications that the user runs do not inherit those privileges unless they are approved beforehand or the user explicitly authorizes it. In Windows 7, Microsoft updated UAC in several ways. By default, UAC does not prompt when certain programs included with Windows make changes requiring elevated permissions. Other programs still trigger a UAC prompt. The strictness of UAC can be changed to either always prompt, or to never do so.

Tasks that trigger a UAC prompt

Tasks that require administrator privileges will trigger a UAC prompt (if UAC is enabled). The following tasks require administrator privileges from Brandon LeBlanc (2009):

- Running an Application as an Administrator
- Changes to system-wide settings or to files in %SystemRoot% or %ProgramFiles%
- Installing and uninstalling applications
- Installing device drivers
- Installing ActiveX controls
- Changing settings for Windows Firewall
- Changing UAC settings
- Configuring Windows Update
- Adding or removing user accounts
- Changing a user's account type
- Configuring Parental Controls
- Running Task Scheduler

- Restoring backed-up system files
- Viewing or changing another user's folders and files
- Running Disk Defragmenter

Common tasks, such as changing the time zone, do not require administrator privileges from Microsoft.(June 3, 2009. Accessed 2nd Nov. 2011), (although changing the system time itself does, since the system time is commonly used in security protocols such as Kerberos). A number of tasks that required administrator privileges in earlier versions of Windows, such as installing critical Windows updates, no longer do so in Vista from Nash, Mike (2008). Any program can be run as administrator by right-clicking its icon and clicking "Run as administrator", if administrator rights will be required a prompt will usually be shown. Should this fail the only workaround is to run a Command Prompt as an administrator and launch the package from there.

2.2.2.4 Hidden File Extension

View File Extensions

Viewing file extensions helps in preventing against opening rogue files with double extensions by enable viewing file extensions from Explorer. By default, Windows 7 hides the file extensions of known file types in Explorer views. The reasoning - this keeps the display clean, as often a file's icon signifies its type. However, as in Windows Vista and earlier, this default setting is a potential security risk. It is possible that you can receive a file via e-mail with an extension of ".txt", or a file with a Notepad icon. Unfortunately, this file could have a hidden second extension, meaning that if you double-click the file, you may actually execute spyware or other malware instead!

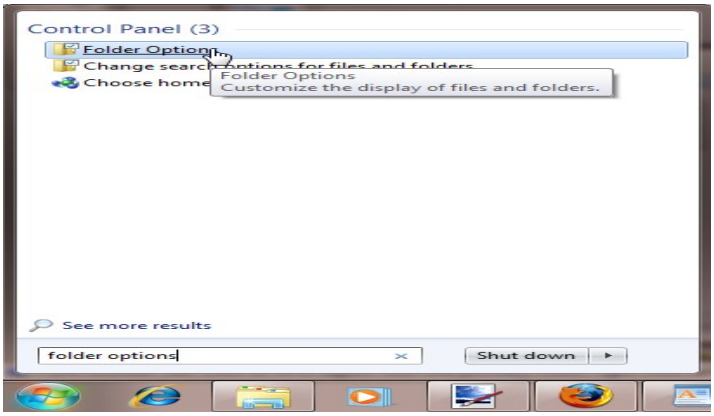

Figure 2.5 Folder Option from Start Button

The "fix":

1. Click the "Start" button, type folder options and click the "Folder Options" link that appears.

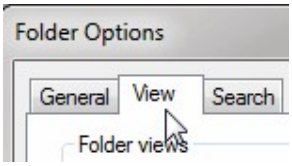

Figure 2.6: Folder Option View

Accessing Folder Options from the Windows 7 Start Button

2. When the "Folder Options" multi-tabbed dialog box appears, click the "View" tab.

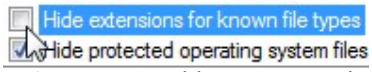

Figure 2.7: Folder Option Hide protected operating system files

3. Uncheck "Hide extensions for known file types".

4. Click "OK" to close the dialog box.

This tip was written for Windows 7 RC. Screenshots and information are subject to change between this and the official release of Windows 7.

How to Hide or Show Known File Type Extensions in Windows 7

Information

A file name extension is a set of characters added to the end of a file name that identifies the file type or format that determines what **default program** should open it. This will show one how to have **Windows 7** hide or show known file type extensions. By default in windows 7, known file types are set to hide.

Figure 2.8: Files Type Extensions Set to Show and Hide

SOLUTION

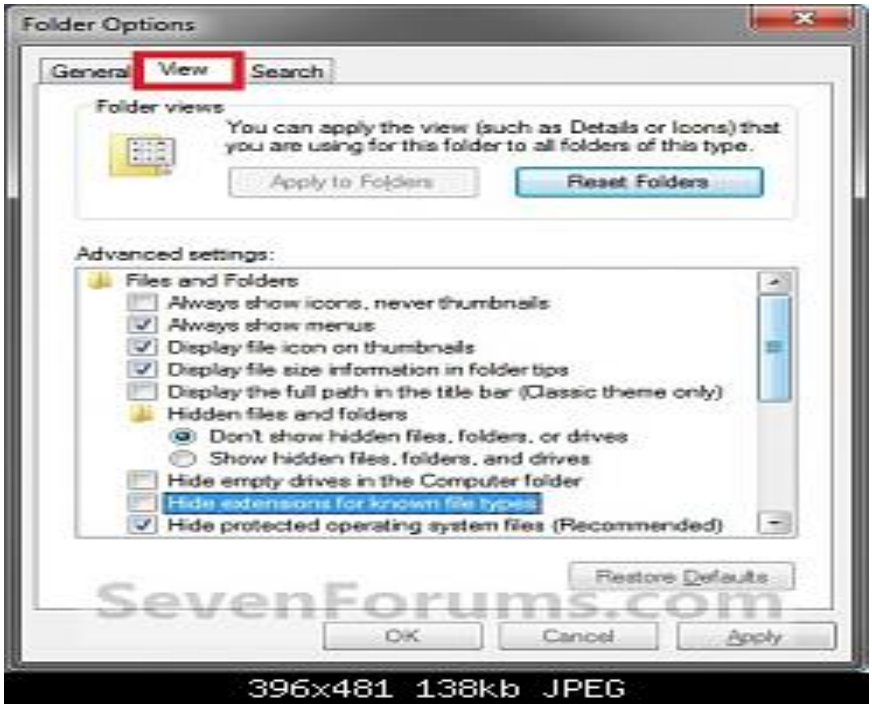

Figure 2.9: Through Folder Options

1. Open **Folder Options**, and click on the **View** tab. (See screenshot above)

2. To Hide Known File Type Extensions

A) Check the **Hide extensions for known file types** box, then click on **OK**. (see screenshot above)

NOTE: *This is the default setting*.

3. To Show Known File Type Extensions

A) Uncheck the **Hide extensions for known file types** box, then click on **OK**. (see screenshot above)

2.2.2.5 Email Settings

With window 7, one have got new choices for how to use email along with some changes from what may be used to in windows vista or windows XP. Windows mail and outlook express aren't included in Windows 7. To use email, one need to install a new program – windows live mail. Once the program is up and running, then email can be imported into it. With windows live mail one can read and reply to mails even when offline. When back online, new email messages will download to your pc and any messages in outbox will be sent.

2.2.2.6 Internet Explorer

Vulnerabilities affect most versions of Microsoft's internet explorer web browser. The hole if exploited could allow remote attackers to circumvent defensive features in fully patched windows 7 and windows vista and run malicious code on vulnerable systems. A common vector of attack is to trick the user into opening a web page that contains malicious code as discussed in Windows XP. Windows 7 will allow users to disable Internet Explorer

Overview

Microsoft has released out-of-band updates to address critical vulnerabilities in Internet Explorer.

2.2.2.7 Other Services and Aspects

Windows 7 includes a number of new features, such as advances in touch and handwriting recognition, support for virtual hard disks, improved performance on multi-core processors from Windowsvienna.com. (Accessed 2nd Nov. 2011) and Blogs.zdnet.com (Accessed 2nd Nov. 2011), improved boot performance, Direct Access, and kernel improvements. Windows Security Center has been renamed to Windows Action Center (Windows Health Center and Windows Solution Center in earlier builds), which encompasses both security and maintenance of the computer. Windows 7 also has a lot of services enabled by default. Some of them can also be accessed from the network and therefore pose as a potential security threat.

2.2.2.8 **The Internet Connection Firewall**

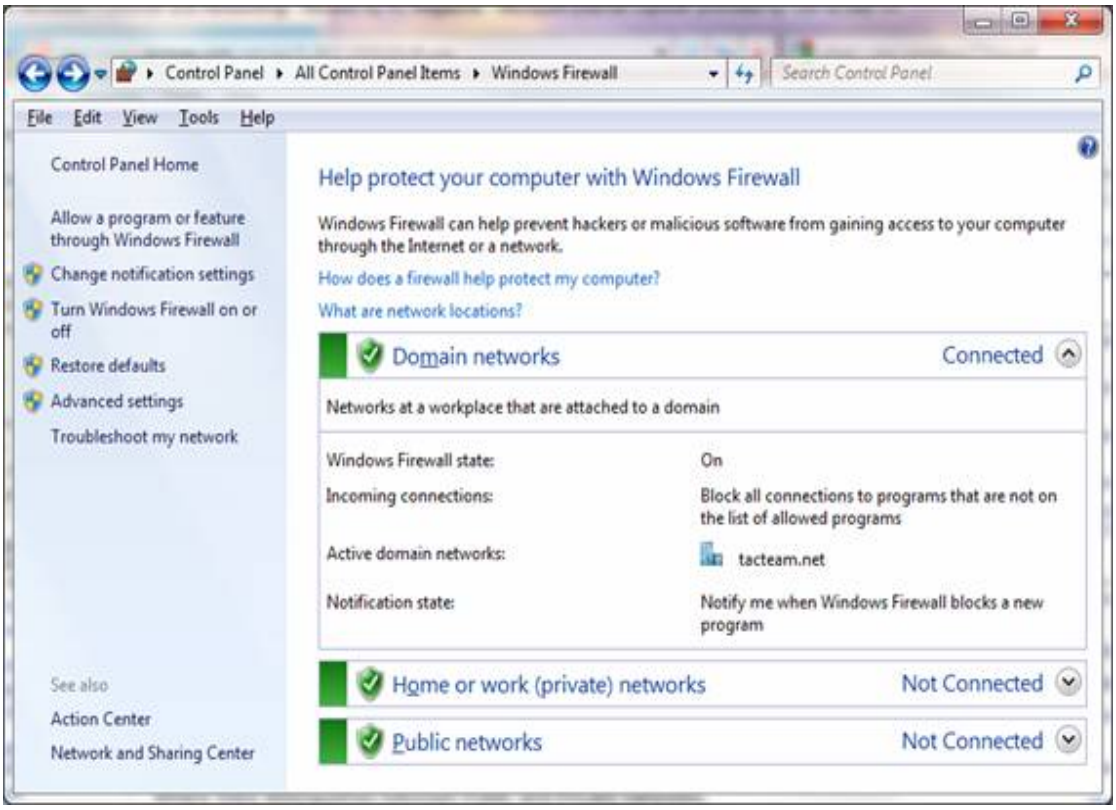

Figure 2.10: Introducing the Windows 7 Firewall

Windows 7 comes with a built in firewall called "Internet Connection Firewall" also known as "ICF". This is a basic firewall that blocks incoming traffic not initiated by the computer. It successfully shields the computer against worms; however this firewall is not enabled by default. The user has to manually enable the firewall. The firewall doesn't protect against potentially malicious web pages that exploit security holes in Internet Explorer. The ICF also runs as a normal Windows service which means that it's disabled during start-ups and shutdowns. This allows worms that use the RPC-DCOM or LSASS vulnerabilities to infect vulnerable computers when they are starting up even if the firewall setting is enabled! The firewall is enabled some time after the desktop is presented to the user. As with Vista, the basic settings for the Windows 7 firewall are accessed via the Control Panel applet as shown in Figure 2.9. With all network types, by default the Windows 7 firewall blocks connections to programs that are not on the list of allowed programs. Windows 7 allows you to configure the settings for each network type separately, as shown in Figure 2.10.

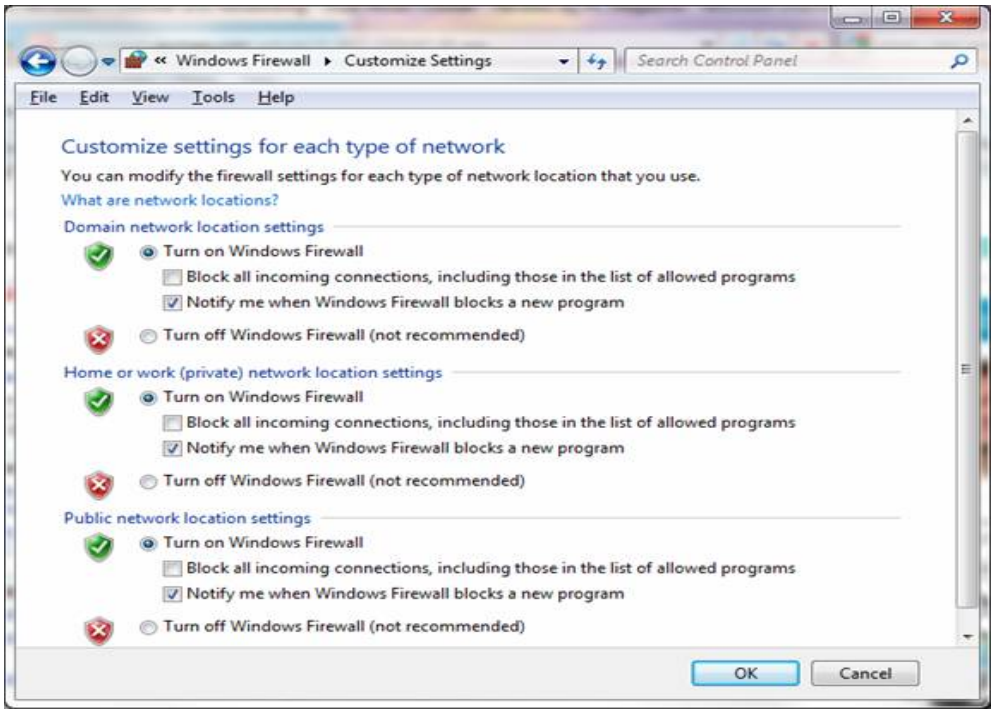

Figure 2.11: Windows 7 allows you to configure settings separately for each network type

2.2.2.9 **Messenger**

The messenger service in Windows7 needs to be installed-windows live mail and allows administrators to send messages to the users using the computers. The messenger service is vulnerable for an attack in its unpatched state that could result in a full system compromise.

2.2.2.10 **System Restore Service**

System Restore points are deleted after restarting Windows 7-based computer.
It is a way to undo system changes to your computer without affecting your personal user files, such as e-mail, documents, or photos.

System restore also back up viruses if the computer has been infected. Windows prevents external programs from accessing system restore files including anti-virus programs. Symantec recommend restarting the system restore service after a virus infection. Restarting the service will result in the deletion of old backups that might be infected. Instructions how to do this can be found on Symantec's web site from Ricciuti, Mike (2007).

2.2.2.11 **How to do a system restore:**

NOTE: *Be sure to temporarily disable your antivirus program first to prevent it from possibly preventing you from doing a system restore*.

1. Open the Start Menu, type **rstrui.exe** in the search box, and press Enter.

A) Go to step 5. **OR 2.** Open the Start Menu.

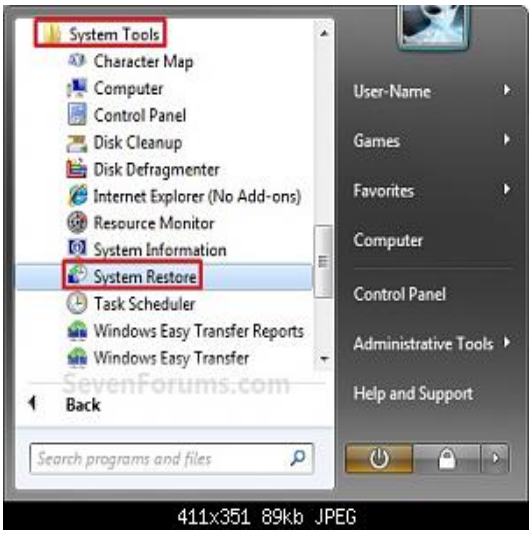

Figure 2.12 Start up Menu

A) Click on **All Programs**, **Accessories**, **System Tools**, and **System Restore**. (See screenshot below) B) Go to step 5. **OR 3.** Open the **Control Panel (All Items View)**. Click on the **Recovery** icon. B) Click on the **Open System Restore** button. (See screenshot below)

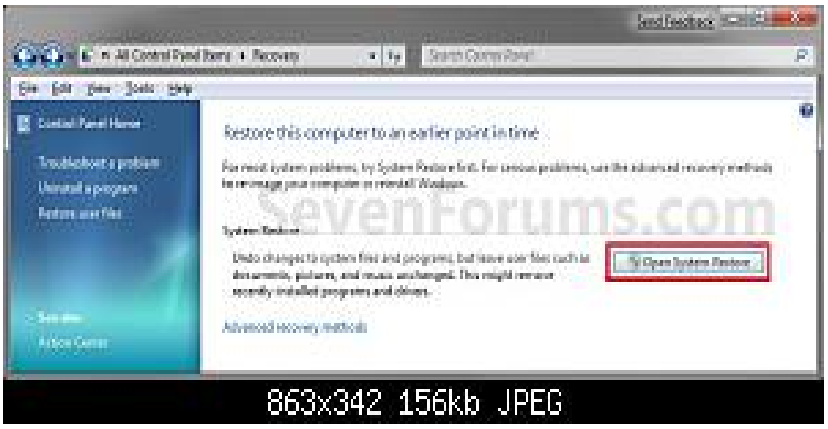

Figure 2.13: System restore button

C) Go to step 6 or 7 below. **OR 4.** Open the Start Menu. A) Right click on the **Computer** button and click on **Properties**. B) Click on the **System Protection** link. (See screenshot above).

Figure 2.14: System Protection Link **Figure 2.15:** System Restore Button

C) Close the **System** window. (See screenshot above) D) Continue on to step 5.

5. Click on the **System Restore** button. (See screenshot above)

6. Click on the **Finish** button. (See screenshot below)

7. Click on **Yes** to confirm. (See screenshot below)

Figure 2.16: System Restore Yes Confirm Screenshot

WARNING: *This will immediately restart your computer to finish the system restore.*

8. After the computer has restarted, click on the **Close** button. (See screenshot below)

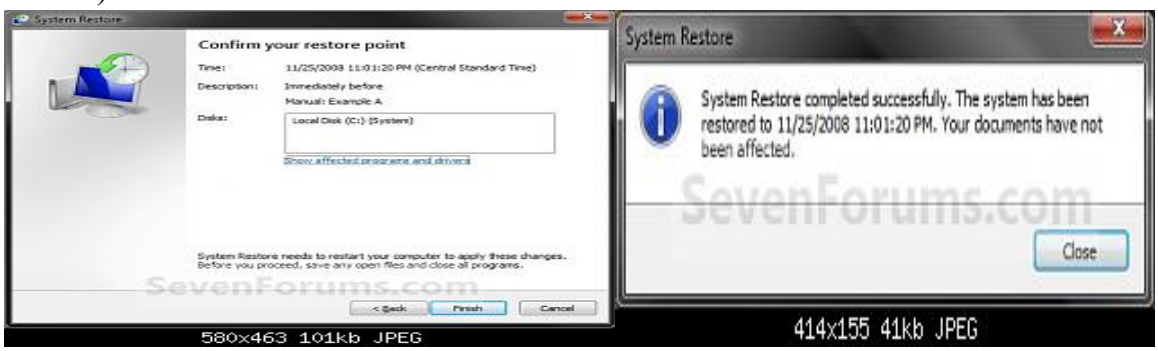

Figure 2.17: System Restore Close button Screen Shot

2.2.3 Recent Vulnerabilities

This section will address some recent security vulnerabilities in both the Windows operating systems and in some commonly used application programs. Only vulnerabilities that are discovered or exploited after July 1st 2003 are discussed.

2.2.3.1 RPC-DCOM: one month from patch to attack

Microsoft released a security bulletin and a patch [MS03-026] on July 16, 2003 to fix vulnerability in the RPC interface that the Blaster worm uses that would allow an attacker to execute arbitrary code on the victims computer. This vulnerability affected all NT based operating systems including Windows 2000 and Windows XP and was remotely exploitable.

2.2.3.2 The messenger service

The messenger service in Windows is not to be confused with MSN Messenger. The messenger service is enabled by default and allows administrators and software to send messages to the users using the computers. It is not normally of any use for the home computer user. The messenger service is vulnerable for an attack in its unpatched state that could result in a full system compromise. A patch is available [MS03-043]. This vulnerability is remotely exploitable like the RPC-DCOM vulnerability the Blaster worm uses. This service has also been targeted by spammers since it allows them to send text advertisements to Windows NT, 2000 and XP systems. Microsoft recommends enabling the ICF and disabling the messenger service.

2.2.3.3 Internet Explorer

Microsoft's Internet Explorer is the most popular browser today. Figure 2.18 below clearly illustrates this. The three most popular browsers are all different versions of Internet

The usage share of web browsers. Source: www.w3schoolslog accessed 29th September 2011

Median values from summary table:
Internet explorer 40.9%
Firefor 26.8%
Google Chrome 17.6%
Safari 6.9%
Opera 2.7%
Mobile browsers 6.5%

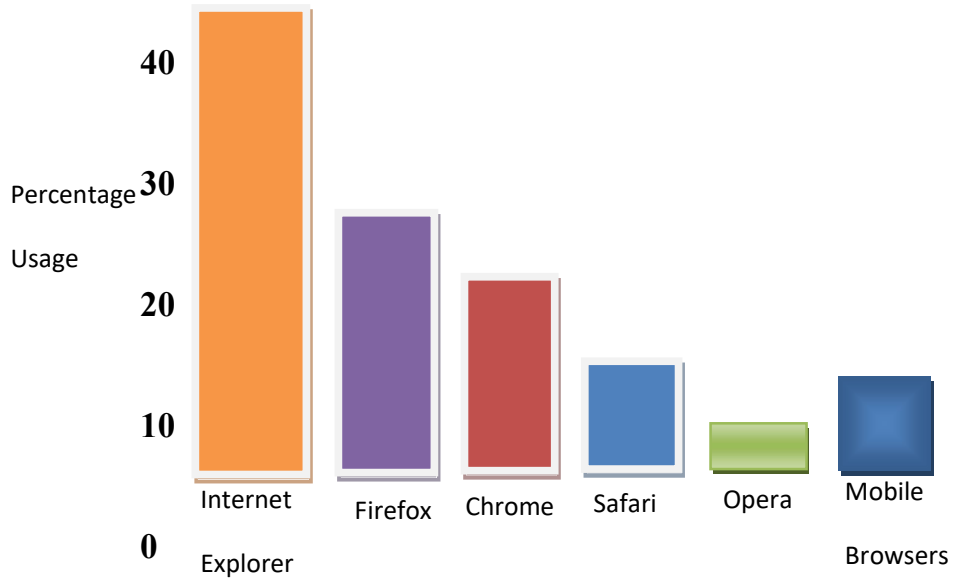

Figure 2.18: Usage share of web browsers: June 2011
Source: www.w3schoolslog accessed 29th September 2011

Internet Explorer has shown that it is prone to different vulnerabilities in the past. Internet Explorer has been the Windows application/component in the past with most vulnerabilities, and the list of vulnerabilities would be too long to list here together with descriptions of each vulnerability. Some of these vulnerabilities are less dangerous and might lead to a DoS attack crashing the browser, while others have been more serious {allowing execution of malicious code. Shady companies have not been late to exploit these Internet Explorer bugs to install spyware programs or dialers without the user's knowledge on computers running an unpatched version of Internet Explorer. Some recent vulnerabilities in Internet Explorer have also been exploited by scammers to trick users to give up their passwords or credit card numbers by making the computer user believe they are visiting the real page, such as www.paypal.com or www.ebay.com. This type of attack is called phishing. More information

about phishing attacks can be found in sections below. It is important to understand that other browsers also contain vulnerabilities, but the combination of the most used browser and new fresh vulnerabilities makes Internet Explorer prone to attacks. If a computer user wishes to use Internet Explorer for web surfing it is very important to keep Windows up-to-date with security patches. It is also important to keep in mind that multiple external applications use Internet Explorer and the built in Windows components to render HTML pages and HTML emails, so an Internet Explorer vulnerability might affect both the browser and the email program...

2.2.3.4 Application Programs

It is common that home computer users know that they have to update Windows, and that they do so when they get reminders that new updates are available for installation. However it is not enough to simply keep the operating system up-to-date. The application programs installed might also contain vulnerabilities that can be exploited by an attacker to take control of the computer. The application Programs are much less likely to be updated than Windows itself. This is an important observation since Internet Explorer and other programs often invoke helper applications when displaying a file the application itself cannot understand. Examples of such helper applications that Internet Explorer use to display documents are Adobe Acrobat Reader and Microsoft Word. This introduces a new vector of attack. Vulnerability in Adobe Acrobat Reader, Microsoft Word or any other commonly used helper application will result in a vulnerable Internet Explorer. If the user visits a web page containing a specially crafted file or document that is displayed with the help of a vulnerable helper Application, the user's computer could end up running malicious code. The user could also be tricked into clicking on an email attachment containing a malicious document or follow a link to a malicious document. This could result in execution of malicious code. This thesis will only contain a brief overview of these problems for a few commonly used application programs in home computers. Thus:

2.2.3.4.1 Microsoft Office

Microsoft Office is by far the most popular office suite at the time of writing of this thesis. It is widely used by both business users and home computer users. Microsoft Office contains several vulnerabilities [bid: 9010, 8835, 8761] in its unpatched state. It is unlikely to have been patched ever according to the user survey in Chapter four. The result of this is that a potential attacker could execute malicious code on a user's machine without the user's authorization even if Windows is fully up-to-date with the most recent security patches. An attacker could send an email containing a word attachment or embed the word document in a malicious web page. Internet Explorer would then invoke Microsoft Word as a helper application to be able to show the malicious document to the user.

2.2.3.4.2 Security Software

Security software such as firewalls and anti-virus programs are becoming increasingly popular due to recent worm outbreaks. Security software is meant to protect the computer from attacks, but it is important to remember that security software is just software... Software can contain vulnerabilities, security software is no exception.

The Witty worm is a recent example of what can happen when something goes really wrong. The Witty worm started to spread in March, 2003. It spread through Internet Security Systems Inc.'s BlackICE and RealSecure products exploiting a buffer overrun vulnerability [bid: 9913] in the firewall included in those products. The worm overwrote random sectors of the hard disk effectively corrupting data including the operating system until the computer crashed. Other examples of recent vulnerabilities are the vulnerabilities in Symantec's popular Norton Internet Security software suite [bid: 9912, 9915, 10333, 10334, 10335, 10336]. All these vulnerabilities are related to the firewall included in Norton Internet Security. Some vulnerabilities allow an attacker to perform a

DoS attack against the computer running the firewall, while others allow an attacker to execute malicious code on the vulnerable computer.

2.2.3.4.3 Instant messengers

Two of the most commonly used instant messaging programs today are Microsoft's MSN Messenger and America Online's ICQ. Both MSN Messenger and ICQ have a history of security vulnerabilities. Some vulnerabilities could be "used" to perform a DoS attack against the instant messaging program, while other vulnerabilities could be used to have a look at the local file system or/and steal information. Instant messaging programs introduce yet another vector of attack that worms can use to spread. Spammers can also make use of instant messaging programs to deliver advertisements to the users. Instant messaging spam is called spim. The spam and spim problems are not treated in this thesis. The most popular instant messaging networks are controlled by large corporations. This gives them some degree of control that they can make use of if a serious vulnerability is found. They can lock out old vulnerable clients and force the users to upgrade to a secure client. Recent instant messaging clients auto-update themselves in the background; often without the user's knowledge.

2.2.3.4.4 Adobe Acrobat Reader

Adobe's Acrobat Reader is the most commonly used program to read *.pdf fi*les. So far no serious exploits of Adobe's Acrobat Reader have been reported. There have been *.pdf* viruses, but they have not affected Acrobat Reader. SecurityFocus.com has got a report of a buffer overflow vulnerability in Acrobat Reader 5.1 [bid: 9802], but it's unknown if this buffer overflow vulnerability can be used to execute malicious code at the time of writing.

2.2.3.4.5 Macromedia Flash Player

Macromedia Flash is a vector graphics based graphics animation program by Macromedia according to Wikipedia (http://en.wikipedia.org, accessed 28-09-2011). The files called "flash files" may be included in web pages to view in a web browser. The most common use is in animated ads on web pages.

Macromedia Flash Player for Internet Explorer is included in Windows by default. Macromedia's Flash Player has had several security vulnerabilities in the past, allowing an attacker to supply executable code in a flash animation or crash the user's browser by supplying a malicious flash animation [bid: 5340, 10057]. Macromedia's Flash Player is an interesting vector of attack because it is so popular in online advertisements. If malicious flash content could be inserted into an ad it would be possible to turn a legitimate site into a malicious site.

2.2.3.4.6 Winamp

Winamp is a popular media player. It is mostly used to play mp3s but it supports almost any format out there via plugins. Winamp has had several vulnerabilities in the past. Most of them are only exploitable if the attacker already has got access to the computer; however one serious security vulnerability was reported last year to bugtraq. This vulnerability [bid: 8567] could allow an attacker to run malicious code on the computer if the user is tricked into playing a specially crafted MIDI file in Winamp.

2.2.3.4.7 QuickTime

Apple's QuickTime Player had very few vulnerabilities in the past. One recent vulnerability [bid: 7247] describes how QuickTime Player fails to properly handle some types of URLs. An attacker might be able to execute commands on the computer running QuickTime Player by supplying specially crafted URLs.

2.2.3.4.8 Real Player

Real Network's Real Player is the main competitor of Microsoft's Media Player together with Apple's QuickTime. It is common that content providers on the web, such as newspapers and tv-stations publish streams for both Real Player and Microsoft's Media Player. The various versions of Real Player contain several vulnerabilities. Several of these vulnerabilities [bid: 9579, 9378, 8453] would allow an attacker to execute malicious code if the user can be tricked into opening a malicious video clip or video stream.

2.2.3.4.9 KaZaA and P2P applications

KaZaA is a popular peer-to-peer (P2P) application. KaZaA allows users to search and download music, documents, images, software, videos and movies. Some of the older versions of KaZaA Media Desktop contain vulnerabilities [bid: 7680, 6747, 6543] that would allow an attacker to perform denial of service attacks or execute malicious code on the computers that are running the vulnerable KaZaA version. KaZaA and other P2P applications are interesting because they introduce yet another vector of attack for malicious code such as worms and viruses. Several worms make use of P2P networks to spread. A common technique is to create a copy of the worm in a shared folder with an attractive name, such as a crack or keygenerator for popular applications, or as a media file using a double file extension e.g. britney-nude.avi.exe. A user searching for cracks, key generators or any other program might download the worm and execute it. Another interesting observation is that a peer in a peer-to-peer network is aware of its neighbour peers. This could allow for a worm that exploits a vulnerability in a commonly used P2P client to spread very fast.

2.2.4 Threats

The aim of this section is to give an overview of the major threats of today and considerations of the threats in the near future.

2.2.4.1 Worms

Worms are definitely one of the biggest threats to the Internet today.

One of the most popular applications used on the Internet is email. It is used by huge numbers of Internet users to send and receive various messages every day. Email is enormously important for many people. But, many don't know that email is maybe the most vulnerable application in a company's network. Email and other Internet applications are used by malicious users as a very fast and powerful tool to spread computer viruses, especially computer worms. Computer worms are reproducing programs that run independently and travel across network connections. The main difference between viruses and worms is the method in which they reproduce and spread. A virus is dependent upon a host file or a boot sector, and the transfer of files between machines to spread,

while a worm can run completely independently and spread of its own will through network connections.

The name "worm" was taken from The Shockwave Rider, a 1970s science fiction novel by John Brunner. Researchers writing an early paper on experiments in distributed computing noted the similarities between their software and the program described by Brunner and adopted the name. Computer worms can be sorted in different ways, but generally there are two types of worms: host computer worms and network worms. Host computer worms are entirely contained in the computer they run on and use network connections only to copy themselves to other computers. Network worms consist of multiple parts, each running on different machines and using the network for several communication purposes. Propagating a segment from one machine to another is only one of those purposes. Network worms that have one main segment which coordinates the work of the other segments are sometimes called "octopuses".

2.2.4.1.1 Worm segments

Worm writers are aware of how important small size and simple construction is for the worm's ability to spread across the network. These two attributes make worms more effective and make possible very fast propagation. Generally, we can say that worms consist of three main segments: attack mechanism, payload and new target selection. Every computer system has its specific vulnerabilities and worms usually exploit them first. Buffer overflow vulnerabilities are the major part of the security holes that worms exploit. The worm's attack mechanism uses the vulnerabilities to copy itself onto the target system.

The payload is the part of the worm code that performs malicious actions against the infected host. The payload can be any type of program that performs various harmful actions on the host's computer system. A common payload for a worm is to install a backdoor in the infected computer. These backdoors are used by malicious individuals for sending junk email or to cloak a website's address of the victim. Spammers, the people who create and distribute junk email, are willing to pay for the creation of such worms. They cooperate with

worm writers and pay for lists of IP addresses of infected machines. Other malicious code writers try to blackmail companies with threatened Distributed Denial of Service (DDoS) attacks. The backdoors can also be exploited by other worms that spread using the backdoor opened by previous worms. There are also some simple worms that have no payload. They just spread themselves and generate huge network traffic. When the worm's code is executed, it attempts to spread again. A worm has to find new target computers that are vulnerable to its attack mechanism. The fact that worms can spread without human intervention and that they can use different techniques to spread makes them very successful in propagation. Worms can infect thousands of computers in a very short time period.

2.2.4.1.2 Spreading Methods

Worms can use multiple methods of spreading. Hybrid worms can have several different ways of spreading at the same time. Some worms use file sharing programs to propagate, some use network connections and backdoors on computer systems. But, the most used method in the past one-year period is email in combination with social engineering, that showed frightening results causing damages for billions of dollars around the world. When a potential victim receives a worm over email, it can be in the form of an attachment or it can be a part of the message. The attachment could claim to be anything from a Microsoft Word document to a picture of some celebrity. Clicking on the attachment to open it activates the worm, but in some older versions of Microsoft Outlook Express clicking on the attachment is not necessary to activate the worm if you have the program preview pane activated. Microsoft release security patches regularly to correct software problems, but not everyone keeps their computer up-to-date with the latest patches. Some worms spread with email messages without attachments meaning that it is enough to open a message to be infected. After the worm has been activated, it searches for a new list of email addresses to send itself to. It goes through the files on the infected computer, such as the email program's address book and the web pages the user has recently looked at, to find them. Once the worm has its list of email

addresses it sends emails with copies of itself to all the addresses it found and the cycle starts again. Some worms use the victim's email program to spread themselves through email, but many worms include a mail server within their code, so the victim's email program doesn't even have to be open in order for the worm to spread. This kind of worms is very aggressive and they produce thousands of copies causing huge network traffic. This process can lead to congestion problems on the Internet and even to server breakdowns at some Internet locations.

2.2.11 Summary

Worms are definitely one of the major threats to both home computer security and the Internet as a whole. These worms almost always contain an attachment and a text fooling the user to click on the attachment and activate the worm. For some of these worms it might be enough to open the email to get infected. Older worms used to send copies of itself to all addresses found in the address book of the infected computer. The more recent worms have their own built in email server, and harvests email addresses not only from the address book. Recent email worms like Netsky, Beagle and Mydoom all used some degree of social engineering to fool the computer users into clicking on the attachments.

Phishing attacks are increasing at an alarming rate. A phishing attack can be potentially very harmful because phishers target financial information and information that can be used for identity theft. A user might not notice the phishing attack before it is already too late, when the bank account is emptied.

Spyware is another problem that is increasing rapidly. Users are tricked into installing useful utility programs that are in fact only a front for an advertisement software that serves popups and harvests personal data sending it to the spyware vendor. Some spyware applications might even install itself automatically without the user noticing by exploiting security vulnerabilities in the browsers.

Different kinds of backdoors and trojan horses are often installed by various worms, allowing the worm writers to take control of the computer remotely and

use it for various harmful purposes. The most common purposes are DDoS attacks and spam distribution.

This clearly illustrates that all threats are related to each other and that different kinds of black hats are starting to work together. An example of this is that spammers are working together with worm writers to set up spam relays.

2.3 Contributions of Related Works and Research Gap

Research into threats and vulnerabilities of computer systems continues to grow because of its evolving nature and significant economic impact on Computer Users.

Works like The Common Criteria (CC) – *ISO/IEC 15408* contains one of few models that addresses threats and vulnerabilities together, showing representation and relationships of security concepts, in terms of *owner*, *safeguards*, *risks* and *assets* according to M. Conner et al (2005). But the CC's model is limited in perspective because it neither includes security *vulnerabilities and threats in home computer* in its representation or *relationships* of *vulnerabilities* to other security concepts. The CC's model is useful and therefore essential in its own rights, but the model needs to evolve to include other security concepts essential in protecting assets, given the ever-increasing incidents of vulnerabilities and threats.

A model of threat classification and control measures was proposed by Farahmand et al. (2003), which aims to identify possible outcomes to an attack. The model focuses on attacks and their resulting outcomes, but relationships of security issues, such as vulnerabilities and threats were not explicitly covered.

Other contributions in the literature exist, but most of which are either specifically addressing *vulnerability* issues according to Farahmand et al. (2003) or *threats* as in M. Conner et al (2005).

Thus, frameworks that possess the capabilities to model both threats and vulnerabilities issues together, and their relationships to other security concepts are pertinently a step forward.

The above incident reveals there still lays a gap, between the ultimate defence needed for Computer security vulnerabilities and threats and the existing defence in practise among home users. This gap needs to be rectified with proper countermeasures and defence mechanisms.

2.4 Relevant Models and Theories

Information security is a complex topic but for this research the foundations of the need for information security measures on home PC is broken down to the areas of threats encountered mostly while on the Internet and the mitigation techniques available to protect computing resources from these threats. This section of literature review will also develop the concepts to justify the need for security precautions which the research is based on.

2.4.1 Information Security

Internet borne attacks can take many forms. One form is email based, such as spam and phishing schemes designed to get users to reveal confidential data. Other attack types result in infections, such as computer viruses designed to cause damage. Trojan Horses are designed to create back doors or spread viruses or spyware, while computer worms are designed to spread themselves as rapidly as possible, creating network disruptions. These programs mentioned above that are designed to compromise computers, are collectively referred to as "malware." While some malware programs are designed to immediately cause noticeable interference with the normal operations of an infected computer, the more common and insidious type of malware is spyware, which silently resides on the host machines to steal private data stored on the computer, or to watch and report online activity looking for details about bank accounts, credit card numbers, and login and password information for a variety of exploitations. Often these malware programs also initiate the host computer into a botnet, a network of similarly infected computers all under the control of an unknown individual, called a botmaster. Either for their own agendas, or for rent,

botmasters can use compromised computers (also called zombies) to email spam, gather personal data, store and distribute illegal material, attack other computers and networks, or use them to launch attacks to cripple the critical infrastructures of nations such as power grids, telecommunications, commerce, or government services (Grizzard, Sharma, Nunnery, Kang, & Dagon, 2007; Rajab, Zarfoss, Monrose, & Terzis, 2006).

James E. Cartwright (2007), reported to Congress that "America is under widespread attack in cyberspace." During fiscal year 2007, the Department of Homeland Security received 37,000 reports of attempted breaches on government and private systems, which included 12,986 direct assaults on federal agencies and more than 80,000 attempted attacks on Department of Defense computer network systems. Most of these attacks were launched using zombie computers to mask the true source (Tkacik, 2007).

Cyber criminals are continuing to refine their attack methods to remain undetected and to create global, cooperative networks to support the ongoing growth of criminal activity (Symantec Corporation, 2007).

CHAPTER THREE

3.0 Methodology

3.1 Research Design

This research work is based on a well structured method using standard emperical tools. The Research design provides the plan or framework for data collection and analysis. It reveals the type of research, whether exploratory, descriptive or causal and the priorities of the researcher. Ghauri and Gronhaug, (2005). The reseach design will comprise combination of descriptive, exploratory and causal approaches. This is because the concept of computer security vulnerability and threats needs to be clarified, and existing models explored in order to investigate the causal relationships that exist among the variables under study.

It consist both qualitative and quantitative methods of data collection. An emperical analysis will be employed, this is due to the nature of variables and

context being investigated.The researcher has employed a case research approach as the method is particularly well suited for this research thesis since the phenomenon under investigation is difficult to study outside its natural context and also the concepts and variables under scrutiny are difficult to a large extent to quantify. Ghauri and Gronhaug, (2005).

The researcher make use of standard model and assumptions based on previously tested theories in computer security vulnerability and threats, the research will involve a deductive approach to drawing or making conclusions based on hypotheses drawn from studying existing literature. Ghauri and Gronhaug,(2005). The case study research will hence, involve data collection through multiples sources such as questionnaires, verbal reports, personal interviews, focus groups, electronic observations as primary data sources Ghauri and Gronhaug, (2005).

The research approach adopted in this research thesis is basically a deductive one in which the researcher have built hypotheses drawn from existing body of knowledge (literature review) and hence will have to be be subjected to empirical scrutiny/testing leading to acceptance or rejection of prior hypothesis. Ghauri and Gronhaug, (2005).
The interview was meant to give answers to several questions raised earlier in the thesis regarding home computer security. It was important to get feedback from real Nigerian users, not just computer security professionals and white papers, in order to avoid the usual label of a home computer user as a person that know little or nothing about computer security.

The most important security issues raised earlier in the thesis are all related to different kinds of vulnerabilities. One main class of vulnerabilities is weaknesses and security holes in the operating systems. It was important to find out how well the home computer users were protected against attacks exploiting these vulnerabilities. Did the users run Windows Update regularly to update their systems? Did the users update their application programs to avoid any security issues related to them? It was also important to find out how well protected the computers were against virus and worm infections, and other malware such as spyware and dialers. Had the users installed an anti-virus

program to protect their computers against viruses and worms, was the anti-virus software up-to-date, and how often was the antivirus software updated? Did the users know what a firewall was, and were their computers protected by one. Were the users aware of the dangers of spyware, dialers and other malware, if they were aware of the dangers did they protect themselves by running an anti-spyware program regularly? Another major threat to home computer security is the user. Did the users know how to behave on the Internet? Did they know how to use email without getting infected? When interviewing persons it is very important that the interviewer's opinions don't influence the answers of the interviewed person. One way to achieve this was to use a well constructed questionnaire that the interviewed persons were asked to complete without any interference of the interviewer. Another significant aspect of using a questionnaire is that all persons that took part in the interview answered the same questions.

An introduction to the survey was also added, to provide some instructions on how to complete the questionnaire, that they could explain their answers to specific questions by writing down an explanation at the other side of the questionnaire. Of course all the persons interviewed were anonymous; this is also clearly stated on the questionnaire. The resulting questionnaire can be found in appendix A.

3.2 Sources of Data

This area of computer security differs from the traditional science in that sense that results are often presented in non traditional ways. Scientific results in other areas are often presented in papers at scientific conferences. Computer security related results are often presented in a more informal way on the Internet. There are special sites and mailing lists for security professionals. The press should be interested in these issues because worm and virus attacks are interesting for a lot of people nowadays.

The inspiration and knowledge required and prompted to embark and complete this thesis was acquired from Prof. Eheduru's Gerald lectures in computer security and cryptology. Further on, the information needed was mainly to be

found on the Internet. A short survey was also conducted which produced several interesting results.

The sources of data for this research work are exclusive primary data sources. Primary data sources for this research work were obtained from structured and standardized copies of questionnaires targeted to about 250 respondents. Primary data gives credibility to the research result for the following reasons:

a. It reduces the interviewer's biases and interpretations of questions.
b. It allows the respondent(s) to think twice before answering a question.
c. It allows some privacy for some sensitive questions
d. It is a fair fast method of collecting data.

The major sources of secondary data include: textbook, newspapers, and conference and workshop papers and they were used mainly in literature review.

3.3 Method of Data Collection

This section deals with means and techniques through which data was collected for this research thesis. Both Primary and Secondary Data was used. Primary Data was collected through administration of structured questionnaires which were meant for testing and validating the prior hypotheses postulated through literature review which is the secondary source of data.

3.3.1 Sample Selection

The sample units are: Nigerian Population from all phase of the country with different occupation, randomly 250 samples.

A random sampling strategy was employed, the places the researcher visited as the limitations described earlier on permit include Imo State, Abia State, Rivers State, Anambra State, Cross River, Ebonyi State, Enugu State, Lagos State, Sokoto State and Katsina State. This sampling method is representative of the entire population of Home Computer Users. This research thesis is case study based and the States visited represent the four regions or parts(East, West, North and South) which made of 40% of the total number of Home Computer Users in Nigeria. As mentioned earlier, data was collected by means of questionnaires

from different occupations of Home Computer Users. This is as a reult of the nature of infomation/data being sought as certain sections required fixed response/s and others were open-ended questions allowing the respondent libery to discuss his opinion on the problem area and subject matter.

3.3.2 Method of Primary Data Collection

Primary data collection tools will be used for this project. One form captures information concerning the respondent and his experience in Computer Security Vulnerability and Threats aspects and the other form captures detail identification of the several aspects of Computer Security Vulnerability and Threats. This form that captured data on aspect of detail identification of the several aspects of Computer Security Vulnerability and Threats was designed based on the Likert five-point scale. The Likert summated involves statement relating to attitude in question (Osuala, 1982). In this case, the aspects of detail identification of the several aspects of Computer Security Vulnerability and Threats. The respondents are required to indicate the degree of agreement or disagreement with each of the statements. A numerical score is assigned to each degree of agreement/disagreement. The scores from the statement are added up to obtain the total score for each respondent. Example:

Strongly disagree	1
Disagree	2
Neutral	3
Agree	4
Strongly agree	5

The use of Likert five-point as an attitude measuring scale is well justified for this study and is rigidly followed as described by Banker et al (1994) as listed below:

i. Responses were selected and subjected to scoring based on the judgmental assessment on the degree of how the various aspects of Computer Security Vulnerability and Threats effects on home computers in Nigeria.

ii. Favorable and unfavorable statements of how the aspect of Computer Security Vulnerability and Threats effects on home computers in Nigeria were compiled.
iii. Collected statements in the form of a questionnaire were administered to a sample deemed to be reasonably representing the population being studied.
iv. Each respondent's score is obtained by adding up the scores of the responses to each statement.

These steps have been followed rigidly in obtaining data and opinion of respondents regarding aspect of Computer Security Vulnerability and Threats on home computers in Nigeria. Kauffman el al (1993) argue that attitude are complex and difficult to measure, and that individuals tends to make inaccurate judgment under difficult circumstances, therefore a scale such as Likert, which improves the measurement of attitudes, is ideal and although, it can be used to rank attitude, but cannot be used to measure difference between attitudes. Also attitude vary, respondents may obtain exactly the same score from agreeing with quite different items (Osuala 1982).

3.3.3 Population of Study and Sample Survey

3.3.3.1 Population

Population is the aggregate or totality in the universe of study. Population could be finite or infinite. The study of the entire population is known as enumeration for the purpose of this work, the population of interest for this study is all of the home computer users that are at least partially responsible for the implementation and maintenance of the software on their computers. Since this study focuses on the use of computer security such as antivirus, firewall, and anti-spyware, anyone who could benefit from this security is included in the population. The latest population statistics from the Nigeria Census Bureau show that there are approximately 10 million internet-enabled households in Nigeria (Nigeria Census Bureau, 2007). Most of the computer owners in this group manage their own software installations and this research is limited to

home computer users who self-identify a responsibility for maintaining their home computer.

The result of this study will be of interest to entire population. It will determine how the various aspect of computer security vulnerability and threats effects home computer users in Nigeria.

3.3.3.2 Sample Survey

A common opinion among today's IT security professionals is that the average home computer user is normally not aware of the threats against their home computers. That many of them don't care, or don't know, about computer security at all, their computers is just another piece of consumer electronics like a TV-set or a DVD player. Because of their lack of interest, or knowledge, about computer security issues they miss important information provided by the different security and software vendors. As long as their computer functions normally in their opinion they are not interested in computer security issues. They only react when something disrupts their normal pattern of use. Then it is usually already too late. This user survey is an attempt to find out what some real Nigerian users think about computer security, and whether they are aware of the current security threats or not. This survey is also an attempt to investigate what their current state of security is, and if they are up-to-date with the latest software patches. The survey focuses on the security habits of some real Nigeria users with different backgrounds. About two hundred and fifty participants took part in the survey.

Due to limitation in resource(s) the researcher might find it difficult to conduct total enumeration (studying the whole population). The option is to limit the study to some of the objects selected from the population sample with a view to extending the finding to the entire population. Basic to all statistical inferences and decision based upon them is the uncertainty introduced by the use of a sample instead of entire population of interest. For example, in experimentation, where the population of observations might be infinite, man's inability to observe "all nature" is obvious. In the social and behavioural science or other applications involving a finite population, the large size of this finite population

still dictates that samples be taken from the population. In this research, the researcher has taken an approach, which ensures that the sample is representative of the population. There are many users of home computers in various parts of Nigeria. These users are professionals and non professionals. Instead of getting responses from all of the users, the researcher was able to interview some to represent the entire population. This decision was made due to resource constraints. The approach used in this survey is random sampling. About 250 sample sizes were used in this study based on the sample size using Tamen Sample calculation formula below:

Original Sample Collected = 670

Missing Values = 2

Population

$n = N/(1 + Ne^{\wedge 2})$; $668/(1 + 668 * .05^{\wedge 2}) = 250$

Where n = Sample size

e = sample error

N = Population

3.3.4 Questionnaire Distributions

The distribution of the questionnaire was purely exclusive because the respondents are expected to be at least skilled and educated in computer practice-related fields. The following will guide the researcher in distributing the questionnaire:

a. The respondent must be educated, at least possess secondary, OND or lower qualification in computer or computer-related disciple.
b. He must be willing to respond.
c. The respondent must not be less than 18 years of age

The above requirements were satisfied.

3.4 Method of Data Analysis

Data collected were subjected to multiple regression analysis electronically. In multiple regressions, F-test was utilized in determining level of significance and

t-test is also used to test for level of significance of each individual factors. The model describing the relationship between the dependent variable and independent variables is as given in the equation 3.1 below:

$Y = \beta_0 + \beta_2 x_2 + \ldots. + \beta_n x_n + €_1$ …… equation 3.1

Y = the dependent variable

Where X_1, X_2 …… X_n = independent variables

β_0 = a constant value of Y when all X values are 0.

$\beta_1 + \beta_2 + \ldots\ldots\ldots\ldots + \beta_n$ = net regression coefficients. For instance, β_0 measures the change in $X_{1\ldots\ldots n}$ while holding the other variables constant.

€ = independent and normally distributed random error term with mean zero.

For the purpose of this study, our

Y = Home Computer Security

X_1 = Virus or Worms

X_2 = Spyware

X_3 = Firewall

X_4 = Internet and E-mail

X_5 = Operating Systems

3.5 Test of Hypotheses

F-Test and T-test were employed in the testing of the Hypotheses.

3.5.1 F-Test

The F-test was employed to test the level of significance of all the independent variables. This test establishes whether or not a significant relationship exists between the dependent variables (Y) and the independent variables (X_1, X_2, X_3, X_4, X_5). Ho is accepted at a level of significance, if $F^* < F_1 - a\ (n-k-1)$, otherwise reject Ho and accept H_A.

However,

$$F = \frac{\left[\frac{RSS_1 - RSS_2}{P^2 - P^1}\right]}{\left[\frac{RSS_2}{n - P^1}\right]}$$

Where RSS_1 = the residual sum of squares of model 1

RSS_2 = the residual sum of squares of model 2

$(P^2 - P^1; n - P^1)$ = degree of freedom.

3.5.2 T-Test

T-Test is used to ascertain the degree to which each of the independent variables contributed to the significance, in the event of rejecting the null hypothesis, and as such should be included in the model. Ho is accepted at the 5% significance level if /t/<t.05(n-2), otherwise Ho is rejected.

However,

$$t = \frac{\ddot{X} - \mu_o}{\sigma / \sqrt{n}}$$

Where; σ = Sample Standard Situation

n = Sample Size

To test the specific strengths of the various independent variables with a T-test statistics.

T-Ratio = $\beta_k/€(\beta_k)$ …… equation 3.5 for k = 1

Where	β_k	=	Estimate of population parameter
	€	=	Standard error of the estimate
	K	=	Number of variables
	N	=	Number of observation

3.6 Decision Rule

If F-Ratio (calculated) is greater than F-Ratio (tabulated), at alpha level of significance, and (K-1), (N-K) degrees of freedom, then we reject H_0 and accept H_A and then conclude that there is some truth in the estimated model (i.e. the regression model is significant since the independent variables significantly accounts for the variation in the dependent variables. Or If $\beta_k/€(\beta_k) > t_{n-k}$: $\alpha/2$ level of significance, we reject Ho and accept HA and therefore conclude that the variable belongs to the model.

3.7 Validity of Research Instrument

My research instrument (via questionnaires) was duly evaluated by my intellectual supervisor and his administration in the selected variables. Besides, the instrument was given to professionals outside the pressure audience, and the result also confirms it genuineness and authenticity both in framing and content. Validity and reliability of findings and results will be key issues in this research. Validity has to do with whether the results obtained within the study are true (i.e. internal validity) as well as whether findings can be generalized in other cases and/or contexts. whereas reliability has to do with the stability or consistency of the measure employed. Ghauri and Gronhaug, (2005).

The validity of the findings or results is highly dependent on the truthfulness of the answers and opinions given by respondents when answering interviews and filling the questionnaires. However, this to some extent might not reflect the reality on ground accurately as respondents might not actually indicate their true opinions which are bound bynon-disclosure, confidentiality clauses, natural phenomenom and issues. Hence, the reseacher was limited in this regard.

CHAPTER FOUR

4.0 Results and Discussion

4.1 Sample Characteristics

The beginning of the survey contained variables relevant to the research model (gender, age, and education) as well as the primary operating system, which only used for description of the respondents. Table 4.1 shows the demographic results for gender, age, and education.

Male respondents accounted for a slightly larger portion of the respondents (51.1%). The largest number of respondents report that their education level is “High Institutions” (44.6%). The majority of respondents report that their primary operating system is Microsoft Windows, with Windows XP the most prevalent version.

Descriptive statistics of reported age (measure on a continuous scale) show the range of respondent ages was 18-79 with an average age of 37.3, with a standard deviation of 17.36, skew of .60, and a kurtosis of -1.06.

Variable	Frequency	Percent (%)
Gender		
Male	95	51.1
Female	91	48.9
Education		
Primary	8	4.3
Secondary	12	0.6
Colleges	16	8.6
University	83	44.6
Polytechnic	39	21.2
Career Training	22	11.8
Master's Degree	13	7.0
Doctorate Degree	2	1.1
Professional Degree	2	1.1
Primary Operating System		
Windows XP	60	32.3
Windows 7	55	29.6
Windows Vista	38	20.4
Windows 98	25	18.4
Apple OS X	-	-
Linux	-	-
UNIX	-	-

Table 4.1: ***Sample Characteristics***

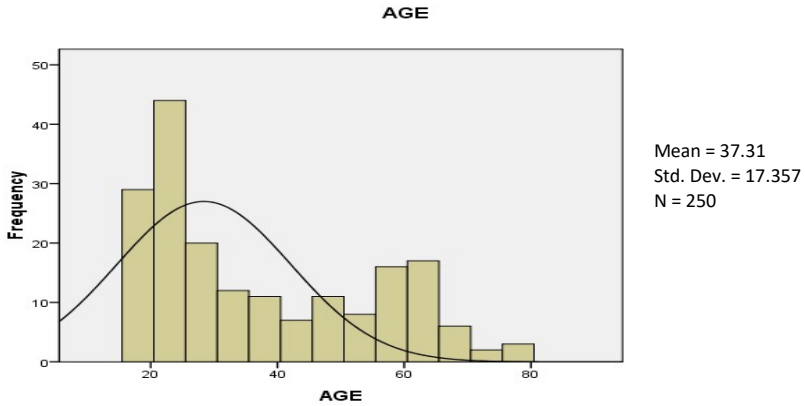

Fig. 4.1 Histogram of Respondent Ages

While these statistics would indicate a normal age distribution, a look at the histogram of respondent ages shown in Fig. shows that the descriptive statistics are misleading. The histogram shows that the distribution is bimodal with the highest peak occurring with users in the range of 20- 25 years of age. This is primarily the result of the snowball sampling being started primarily with

undergraduate students. However, the scatterplot of the age of respondent shown in Figure 16 illustrates the progression of the sampling by respondent and that as the snowball sampling continued, the sample grew more diverse in age. Had the sampling been allowed to continue deeper into the population, the sample should have become more normally distributed with respect to age and more representative to the target population with respect to all demographics. Heckathorn,(1997).

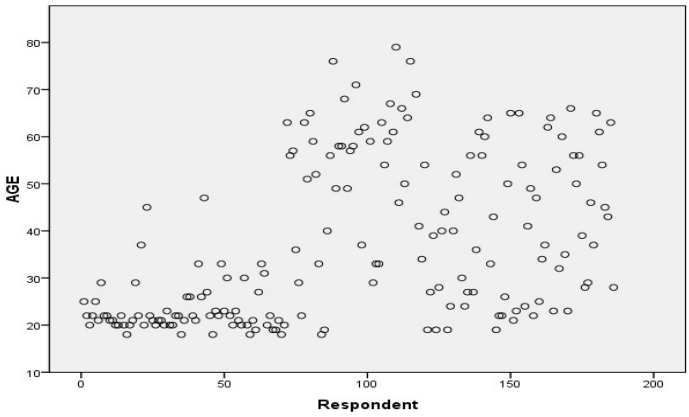

Figure 4.2 Scatterplot of Age and Respondent Number.

4.2 Model Estimation and Hypothesis Testing

4.2.1 Relational Model and Interpretation

In estimating the model, the tabulated data, Table 4.2 below were subjected to multiple regression analysis using SPSS software. The result obtained from multiple regression is as follows: **R = 0.952, R^2 = 0.906, Adjusted R^2 = 0.904, F_{cal} = 470.996, Sig = .000[a]**

Model	Variables Entered	Variables Removed	Method
	x5, x4, x3, x2, x1(a)	.	Enter

a All requested variables entered.

b Dependent Variable: y

Table 4.2: Variables Entered/Removed(b)

The Table 4.2 above shows that all the independent variables were entered, that none was removed; displaying the method Enter.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.952(a)	.906	.904	.68931

a Predictors: (Constant), x5, x4, x3, x2, x1

b Dependent Variable: y

Table 4.3 Model Summary(b)

The Table 4.3 above is the second piece of the output and gives the value of the coefficient of determination, "R Square and $S = \sqrt{MSE}$, the "Standard Error of the Estimate".

R Square being the amount of variance in the dependent variable that can be explained by the model. Since the R Square is 90% close to 1.0, the model produced perfect predictive accuracy.

Using the regression output on Table 4.5, we estimated the following Equation (4.1) – the relationship model:

$$\mathbf{Y = -4.35 + 0.294x_1 + 0.194x_2 + 0.265x_3 + 0.181x_4 + .245x_5 \ldots\ldots\ldots\ldots\ldots..(4.1)}$$

Where:

Y	=	Home Computer Security
X_1	=	Virus or Worms
X_2	=	Spyware
X_3	=	Firewall
X_4	=	Internet and E-mail
X_5	=	Operating Systems

The interpretation of the relationship model based on the output of our multiple regression analysis (as shown in Tables 4.3, 4.4, and 4.5) is as follows:

1. Equation 4.1 shows that level of relationship existing between home computer security (Y) and the five explanatory variables (X_1, X_2, X_3, X_4, X_5) is strong. The **R** is **0.952,** which indicates that **95.2%** correlation exists between home computer security and security vulnerabilities and threats on home computers in Nigeria.
2. Table 4.3 shows that 90.4% of the cumulative variations in the five independable variables-vulnerabilities and threats on home computers, when all possible error in estimation is taken into consideration.
3. The standardized error in the estimation of security vulnerabilities and threats on home computers in Nigeria success using the five variables (X_1, X_2, X_3, X_4, X_5) is 0.68931.

4.2.2 Hypothesis Testing

The hypotheses stated are tested using the relational model generated based on the result of the estimated coefficients and parameters. One method to test statistical significance of estimated model is through the coefficient of determination (R^2), calculated from the Regression. R^2 gives the proportion of the total variation in the dependent variable (Computer Security). The value for R^2 ranges from 0 to 1. In setting up the test, the following Hypothesis is tested:

4.2.2.1 Test of Hypothesis One

Ho_1: There is no significant effect of vulnerabilities and threats as a whole on home computer security in Nigeria.

H_{A1}: There is significant effect of vulnerabilities and threats as a whole on home computer security in Nigeria.

In testing the hypothesis, using the ANOVA Table 4.4 below.

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1118.964	5	223.793	470.996	.000[a]
	Residual	115.936	244	.475		
	Total	1234.900	249			

a. Predictors: (Constant), x5, x4, x3, x2, x1

b. Dependent Variable: y

Table 4.4 Anova Table

In model summary Table 4.3, R Square is 90.6%. Therefore the model produced a good predictive accuracy. The F_{cal} value of 470.996 in ANOVA Table 4.4 is highly significant at 0.05 level having $P_{value}(.000) < 0.05$. We therefore, reject the null hypothesis one that there is no significant effect of vulnerabilities and threats as a whole on home computer security in Nigeria and accept the alternative hypothesis one, that there is significant effect of vulnerabilities and threats as a whole on home computer security in Nigeria.

4.2.2.2 Test of Hypothesis Two

Ho_2: There is no significant effect of each computer vulnerabilities and threats on home computer security in Nigeria.

H_{A2}: There is significant effect of each computer vulnerabilities and threats on home computer security in Nigeria.

In order to test this hypothesis, the significance of the coefficient of each of the various components of each of the computer vulnerabilities and threats on home computer security as shown in Equation (4.1) is tested using the student t-test as shown in Table 4.5.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-4.364	.617		-7.072	.000
	x1	.294	.032	.319	9.127	.000
	x2	.194	.034	.180	5.752	.000
	x3	.265	.033	.234	8.140	.000
	x4	.181	.033	.153	5.558	.000
	x5	.245	.036	.223	6.901	.000

a. Dependent Variable: y

Table 4.5: Coefficients[a]

Ho_{2a}: There is no significant effect of Worms and Virus on home computers security in Nigeria.

H_{A2a}: There is significant effect of Worms and Virus on home computers security in Nigeria.

From the Coefficient[a] Table 4.5, $p < .05$, having x_1($\beta = 0.319$, $p = .000$) and $\mathbf{t_{cal}}$ **9.127**, implies that the value 9.127 is highly significant. Therefore **Ho_{2a}**: There is no significant effect of Worms and Virus on home computer security in Nigeria is rejected, accepting **H_{A2a}:** There is significant effect of Worms and Virus on home computers security in Nigeria.

Ho_{2b}: There is no significant effect of spyware on home computers security in Nigeria.

H_{A2b}: There is significant effect of spyware on home computers security in Nigeria.

From the Coefficient[a] Table 4.5, $p < .05$, having x_2($\beta = 0.180$, $p = .000$) and $\mathbf{t_{cal}}$ **5.752**, implies that the value **5.752** is significant. Therefore **Ho_{2a}**: There is no significant effect of spyware on home computers security in Nigeria. **H_{A2b}:** There is significant effect of spyware on home computers security in Nigeria.

Ho_{2c}: There is no significant effect of Firewall on home computers security in Nigeria.

H_{A2c}: There is significant effect of Firewall on home computers security in Nigeria.

From the Coefficient[a] Table 4.5, $p < .05$, having x_3 ($\beta = 0.234$, $p = .000$) and $\mathbf{t_{cal}}$ **8.140**, implies that the value 8.140 is highly significant. Therefore $\mathbf{Ho_{2c}}$**:** There is no significant effect of Firewall on home computers security in Nigeria is rejected, accepting $\mathbf{H_{A2c}}$**:** There is significant effect of Firewall on home computers security in Nigeria.

$\mathbf{Ho_{2d}}$**:** There is no significant effect of Internet and E-mail on home computers security in Nigeria.

$\mathbf{H_{A2d}}$**:** There is significant effect of Internet and E-mail on home computers security in Nigeria.

From the Coefficient[a] Table 4.5, $p < .05$, having x_4 ($\beta = 0.153$, $p = .000$) and $\mathbf{t_{cal}}$ **5.558**, implies that the value 5.558 is significant. Therefore $\mathbf{Ho_{2d}}$**:** There is no significant effect of Internet and E-mail on home computers security in Nigeria is rejected, accepting $\mathbf{H_{A2d}}$**:** There is significant effect of Internet and E-mail on home computers security in Nigeria.

$\mathbf{Ho_{2e}}$**:** There is no significant effect of Operating System on home computers security in Nigeria.

$\mathbf{H_{A2e}}$**:** There is significant effect of Operating System on home computers security in Nigeria.

From the Coefficient[a] Table 4.5, $p < .05$, having x_5 ($\beta = 0.223$, $p = .000$) and $\mathbf{t_{cal}}$ **6.901**, implies that the value 6.901 is highly significant. Therefore $\mathbf{Ho_{2e}}$**:** There is no significant effect of Operating System on home computers security in Nigeria is rejected, accepting $\mathbf{H_{A2e}}$**:** There is significant effect of Operating System on home computers security in Nigeria.

4.3 Result Discussion

Results of this study is discussed within the context of the following research questions.

Research Question One:

What are the computer security vulnerabilities and threats?

Computer Security Vulnerabilities and Threats are the weaknesses in system security procedures, system design, implementation, internal controls, and so

forth, that could be exploited to violate the system security policy; the possibility of an exploit or exposure to intimidation (threat), specific to a given platform. (ISACA-Information System Audit and Control Association, cited 2nd November 2011).

The vulnerabilities, threats and their channels as used in this study are:

Virus and Worms: **Virus** is a self-replicating and propagating program, usually operating with some form of input from the user, although generally the user is unaware of the intent of the virus. **Worm** is a self-reproducing program which is distinguished from a virus by copying itself without being attached to a program file, or which spreads over computer networks, particularly via email.

Spyware: Spyware is software that gathers information about a computer user without the user's knowledge or informed consent, and then transmits this information to an external third party such as an organisation that expects to be able to profit from it in some way. **Firewall:** A system or combination of systems that enforces a boundary between two or more networks. **Internet and E-mail: Internet** is a collaboration of more than hundreds of thousands of interconnected networks. It is a collection of LANs and WANs held together by internetworking (network of networks) devices. People access internet to download, upload, send, receive, update and transact information. It is a communication system that has brought a wealth of information to our fingertips and organized it for peoples use. Where **E-mail** is an electronic mail, it is a mail send via internet. **Operating System:** The layer of software that sits between a computer and an application, such as an accounting system or email program. Examples of common operating systems are Microsoft Windows and Linux. U.S. ASPI (2009).

Generally, equation 4.1 reveals that there exist a relationship between home computer security and computer security vulnerabilities and threats.

Question Two:

To what extent are the computer security vulnerabilities and threats as a whole affected home computer?

The test of hypothesis on this research question showed that there is significant effect of vulnerabilities and threats as a whole on home computer security in Nigeria. The conclusion was drawn from the statistic F-test in which F_{cal} value of 470.996 is significant at 0.05 level. This actually implies that vulnerabilities and threats as a whole on home computer created a tremendous impact on home computer security. Furthermore, computer security provides a platform for home computer users in Nigeria because it would be extremely difficult for a country to manage their economy well when information cannot be protected by her citizens and in that case home computer users as a starting point is the starting basis for security conscious and awareness of a standard economical nation. As a result it is very crucial for Nigerian's home computer users to imbibe computer security at their finger tips and a candid way to do or solve this home computer security issue is given in the recommendation section.

Question Three:

To what extent has each computer vulnerability and threats affected home computer?

The Coefficient Table 4.5 and test of hypothesis two, discussed above showed that the vulnerabilities and threats factors; Virus or Worms (x_1(β = 0.319, p = .000), $\mathbf{t_{cal}}$ **9.127**), Spyware (x_2(β = 0.180, p = .000), $\mathbf{t_{cal}}$ **5.752)**, Firewall (x_3(β = 0.234, p = .000), $\mathbf{t_{cal}}$ **8.140**), Internet and E-mail (x_4(β = 0.153, p = .000), $\mathbf{t_{cal}}$ **5.558)**, and Operating System(x_5 (β = 0.223, p = .000), $\mathbf{t_{cal}}$ **6.901**), are all significance at 0.05 level of significance. These mean that the suggested factors are very relevant in measuring security models. (Okonkwo, 2002).

Question Four:

What policy recommendation can be made?

The policy recommendations measures can be established based on the statement of problem, test of hypotheses and research questions. The policy recommendations include:

- Putting into policy by the government to the ordinary users a means of creating increased general awareness of the home computer security related issues.
- Policy should be made regarding journalists who reach out the important information of security to the general public, to do it in such a way that the user's view will always have something important on their computer confirmed.
- There is the need to set policy in utilizing home computer security in making advances in health, politics, education, business, agriculture, consumer goods, national security and poverty reduction in order for Nigeria to be economically competitive, politically stable, and socially secure. The country needs to focus its attention on the development, access, and implementation of ICTs both in the rural area where majority of the poor resides and in the urban centers.
- Formation of associations, and Community-bases organisations at rural areas will act as training centres and access points. From such group, the masses will be thought on how to impliment computers securely and policies.
- The problem of computer security vulnerabilities and threats can be solved by strengthening the local and regional technical schools and colleges.
- The target population for policy-making of poverty alleviation must be known in relation to each specific service.
- Nigerian governments should formulate national strategies to narrow knowledge gaps, including those for technology acquisition and distribution, education and training and expanding access to technologies through its economic reform of deregulation and privatizations

4.4 Chapter Summary

The main reason why many ordinary users do not worry about computer security is that they think there is nothing important on their computers, so why would someone want to attack their computer. Ordinary users don't read

security bulletins, they get their information from mainstream press, if they get it at all. As seen in chapter two mainstream press writes about hackers attacking computers in order to steal information. Articles like that further strengthens the opinion that virus writers and hackers only want important information, and that there is no need to protect the home computer. Both interest and knowledge are important factors that affect home computer security. Interest in home computer security leads to better protection of the home computer, and a better knowledge about security related issues. Knowledge about security related issues often leads to a better computer security, but the survey showed that there are exceptions. Some users are well aware of the threats, but still don't care to protect their computers. The survey shows that many users do not feel comfortable with automatically updating their software, such as anti-virus programs and operating systems. Most users prefer to manually update their software. The users feel that they will lose control over their own computer when allowing auto-updates. Some users don't trust Microsoft's Windows Update service, and prefer to update their anti-virus programs prior to updating Windows. Security products, such as firewalls, with too many advanced features can be counterproductive. If the security product asks too many questions in order to achieve the desired level of security it quickly becomes irritating. The user might uninstall the whole security product altogether instead of lowering the security settings.

The presence of spyware applications are very common in today's home computers. The survey confirmed this; several users had spyware applications installed without their knowledge. They thought it was normal with all the pop-ups, e.g. that Microsoft served popup ads on their Windows Update service. Most users were completely unaware about the dangers of spyware. The survey showed that the average level of awareness among ordinary home computer users is relatively low, and will probably remain relatively low in the near future. In order to raise the general level of awareness it is important to make use of mainstream media, to reach out to the majority of users with the right information in the right time. It is important to get the journalists interested and

educated in these issues, so that they report about this in right way. One other possible way to reach out to the general public could be to run advertisement campaigns.

CHAPTER FIVE

5.0 Conclusion and Recommendation

5.1 Summary of Findings and Conclusion

On the basis of analysis and result of this study, the findings of this study are summarized as follows:

Observations were made that home computer users do not apply security and if they do, are ignorant of the safest methods of computer security applications. This pave way for vulnerabilities and threats on home computers which have cost users, general public, the nation at large dearly in terms of lost of vital information, system break down without remedy and setbacks in the world of information security.

This study revealed that worms or virus, spyware, firewall, internet and e-mail, and operating system are factors used to conclusively investigate home computer security applications. They were applied in the evaluation and analysis of multiple regression analysis model using SPSS software, where the factors mentioned above are the independent variables explaining the change in the dependent variable computer security. The evaluation showed greater vulnerabilities and threats effectiveness on home computer security in Nigeria.

In conclusion, based on the summary of findings, to effectively have maximum security of home computers, awareness policies should be made by governments especially the aspect of clarity during the awareness or campaigns to the general public irrespective of geopolitical positions of Nigeria inhabitants because computer security issues are important when one considers national productivity and economic development through enhanced information and communication technology services in Nigeria.

5.2 Recommendations

On the basis of the summary of findings and conclusion, the following recommendations are made:

It is recommended that security software be installed at the point of computer purchase to increase awareness and users or buyers asked some computer security questions and to demonstrate them on the point of purchase.

It is also recommended that the vulnerabilities and threats factors used in this work be used as standard for evaluation even when future models are because of its wide and acceptability.

It is recommended that models for evaluation of computer security should imbibe more simplified ways of improving on the flaws inherent in the design models that lagged in the evaluation and analysis.

5.3 Future Research

This research provides a foundation for a number of future studies based upon the results presented in Chapter 4, and based on the limitations observed and other questions brought up during the course of the research. An obvious addition to this study would be a replication of the study in using different samples from the target population. There were many hypotheses that were not supported during the analysis of the data collected. Only through replication will the value of these hypotheses to the research model be fully known. Another sampling issue that could be addressed in future studies would be obtaining a sample that is more representative of the target population thereby increasing the generalizability of results obtained.

This study used computer security usage through the application of anti-virus, firewall, and anti-spyware software to evaluate the research model. However, future applications of the model could be extended to the behaviours involved in opening suspicious emails, using suspicious websites, file sharing, and other high-risk online activities. And finally, the application of the regression to the study of security adoption can be extended beyond the home environment to study security adoption behaviour in the corporate environment.

REFERENCES

America Online, & National Cyber Security Alliance. (2005). *AOL/NCSA online safetystudy*. Dulles, VA: National Cyber Security Alliance, Time Warner Inc.

America Online, & National Cyber Security Alliance. (2005). *AOL/NCSA online safetystudy*. Dulles, VA: National Cyber Security Alliance, Time Warner Inc.

Anti-phishing Working Group (2004). Available at: http://www.antiphishing.org/. [cited 28 September 2011].

Banker, R., Kauffman, R., and Kumar, R(1994). *"An Empirical Test of Object Based Output Measurement Metrics in a Computer Aided Software Engineering (CASE) Environment," Journal. 42, pp, 54-78.*

Blogs(2007). Available at blogs.zdnet.com. [cited 2nd November, 2011]

Boss, S. (2007). *Control, perceived risk and information security precautions: External and internal motivations for security behavior*. Ph.D. dissertation. Retrieved from Dissertations & Theses: Full Text. (Publication No. AAT 3284534)

Bradon, LeBlanc (2008). *"How Libraries & HomeGroup Work Together in Windows 7"*. *Windows Team Blog*. Microsoft.

Brandon, Leblanc (2009). *"The Complete Windows Experience – Windows 7 + Windows Live"*. *Windows Team Blog*. Microsoft.

CERT Coordination Center(2007)., available at web. http://www.cert.org. [cited 28th September 2011]

Computer Security Threats.(2011) Available at: www.bleepingcomputer.com/virus-remo., www.techpluto.com/softwares-missing-in-windows, www.technewsworld.com/story/31632.html, http://www.cs.berkeley.edu/~nweaver/worms.pdf, http://www.vmyths.com/hoax.cfm?id=275&page=3, http://www.ehow.com/phishing-virus.html. [cited 2nd November 2011]

Conklin, W. A. (2006). *Computer security behaviors of home PC users: A diffusion of innovation approach.* Ph.D. dissertation. Retrieved from Dissertations & Theses: Full Text. (Publication No. AAT 3227760)

Dieter Gollmann(1999). *Computer Security*. John Wiley & Sons Ltd, Baffin Lane, Chichester, West Sussex PO19 1UD, England.

eBay Inc. and AtHoc Inc.(2004). eBay buyer tools: toolbar. Available at: web.http://pages.ebay.com/ebay/toolbar/. [cited 28th September 2011]

F. Farahmand, S. B. Navathe, G. P. Sharp and P. H. Enslow (2003). "*Managing Vulnerabilities of Information Systems to Security Incidents*", *Proceedings of the ICEC 2003, Pittsburgh, PA ACM 1- 58113-788-5/03/09*

Ghuari , P & Gronhaug K(2005). "*Research Methods in Business Studies"* Pearson Education, London.

Grizzard, J. B., Sharma, V., Nunnery, C., Kang, B. B., & Dagon, D. (2007). "*Peer-to-peerbotnets: Overview and case study". Proceedings of the 1st USENIX Workshop on Hot Topics in Understanding Botnets.*

APPENDIX (A) - SURVEY QUESTIONNAIRE

Federal University of Technology Owerri (FUTO) - MSc Research Thesis Questionnaire.

Dear Respondent,

This questionnaire is part of my Research-Paper in partial fulfilment of my Postgraduate Study in IT (MSc) in the Department of Information Management Technology, Federal University of Technology Owerri. The Research Study purpose is an effort to analyse the effect of security vulnerabilities and threats on home computers in Nigeria.

This questionnaire is targeted at Home Computer Users.

This will take only a few minutes of your time and all answers are completely anonymous

Your response will be much appreciated as it will throw more light into this area of study. Thank you for participating in this survey.

yours faithfully

Oragui Gloria

For further clarification and inquiries please contact:

glorzionline@yahoo.com

Questionnaire:

Part A: Please *tick* the item below that best describes you.

A. Gender: Male ☐ Female ☐

B. Age Group: Under 18 ☐ 18-20 ☐ 21-30 ☐ 31-40 ☐ 41-50 ☐ 51-60 ☐ 61 or over ☐

C. Nationality: Nigerian others (Please specify) _____

D. Educational Background:

1. Primary School ☐
2. Secondary School ☐
3. Colleges of Education, Health, Land, Agriculture, etc ☐
4. Polytechnic ☐
5. University ☐
6. Career Training ☐
7. Master's Degree (M.BA, M.TECH, M.SC, M.ENG) ☐
8. Doctoral Degree (Ph.D, Ed.D, DBA, etc) ☐
9. Professional Degree (MD, JD, DDS,DVM, etc) ☐

D. Operating Systems:

1. Windows 98 ☐
2. Windows XP ☐
3. Windows Vista ☐
4. Apple OS X ☐
5. Linux (Red Hat, SUSE, Ubuntu, etc.) ☐ 6. Unix (BSD, HP, Solaris, etc.) ☐

PART B

This section is to measure **home computer security effects on home computers in Nigeria using various means of entrance of threats and vulnerabilities.** There is no right or wrong answer. Please choose your answers by ticking the corresponding box using the scale from 1 to 5 as shown below:

Strongly Disagree (SD)	Disagree (D)	No Opinion (N)	Agree (A)	Strongly Agree (SA)
1	2	3	4	5

Please indicate the degree to which you agree/disagree with the following statements.

x_1	VIRUS and WORMS					
		SD	D	N	A	SA
1	Virus and Worms definition/knowledge helps increases computer security					
2	Worms and Virus attack brings reduction computer security					
3	Computer system is corrupted by virus or worms					
4	Data is corrupted by virus or worms					
5	Data is lost to virus or worms					
6	Install anti-virus in computer increases computer security					
7	Setting anti-virus program to automatic update effectively reduce Virus and Worms attack					
x_2	SPYWARE					
		SD	D	N	A	SA
1	Spyware definition/knowledge helps increases computer security					
2	Spyware attack brings reduction in computer security					
3	Computer system is corrupted by spyware through my lack of security practice					
4	Data has been stolen by a hacker through spyware attack					
5	Data has been corrupted and lost through spyware attack					
6	Install anti-spyware in computer increases computer security					
7	Setting anti-spyware program to automatic update effectively reduce Virus and Worms attack					

x_3	FIREWALL					
		SD	D	N	A	SA
1	Firewall definition/knowledge helps increases computer security					
2	Firewall disenabling brings reduction to computer security					
3	Installing/enabling personal running firewall on computer boost security					
4	Leaving firewall program to its default setting brings maximum security					
5	Setting firewall program to personalized setting brings maximum security					
6	Tempering with firewall setting changes the way computer works					
7	Firewall settings should be a concern for users					

Appendix B-Analysis of Data using SPSS Software

Regression

Variables Entered/Removed(b)

Model	Variables Entered	Variables Removed	Method
1	x5, x4, x3, x2, x1(a)	.	Enter

a All requested variables entered.

b Dependent Variable: y

Model Summary(b)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.952(a)	.906	.904	.68931

a Predictors: (Constant), x5, x4, x3, x2, x1

b Dependent Variable: y

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1118.964	5	223.793	470.996	.000[a]
	Residual	115.936	244	.475		
	Total	1234.900	249			

a. Predictors: (Constant), x5, x4, x3, x2, x1

b. Dependent Variable: y

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-4.364	.617		-7.072	.000
	x1	.294	.032	.319	9.127	.000
	x2	.194	.034	.180	5.752	.000
	x3	.265	.033	.234	8.140	.000
	x4	.181	.033	.153	5.558	.000
	x5	.245	.036	.223	6.901	.000

a. Dependent Variable: y

APPENDIX C-RESULTS OBTAIED FROM RESPONDENTS (R1-R250)

R	Y	X_1	X_2	X_3	X_4	X_5
1	25.00	25.00	25.00	25.00	25.00	25.00
2	20.00	23.00	22.00	22.00	22.00	22.00
3	25.00	26.00	27.00	23.00	24.00	26.00
4	21.00	22.00	23.00	21.00	22.00	23.00
5	21.00	22.00	23.00	21.00	22.00	22.00
6	25.00	25.00	24.00	24.00	24.00	25.00
7	23.00	21.00	22.00	24.00	24.00	24.00
8	23.00	24.00	21.00	24.00	22.00	24.00
9	24.00	22.00	21.00	23.00	25.00	26.00
10	24.00	25.00	26.00	26.00	23.00	22.00
11	24.00	24.00	23.00	25.00	25.00	23.00
12	25.00	26.00	24.00	23.00	24.00	24.00
13	22.00	21.00	22.00	23.00	20.00	23.00
14	23.00	22.00	23.00	24.00	25.00	25.00
15	25.00	24.00	23.00	26.00	23.00	23.00
16	22.00	23.00	22.00	21.00	24.00	22.00
17	23.00	24.00	23.00	22.00	23.00	24.00
18	25.00	26.00	26.00	24.00	23.00	24.00
19	20.00	22.00	21.00	20.00	22.00	22.00
20	25.00	26.00	25.00	25.00	24.00	24.00
21	21.00	22.00	22.00	23.00	22.00	24.00
22	21.00	22.00	22.00	20.00	21.00	22.00
23	26.00	25.00	24.00	25.00	25.00	24.00
24	23.00	22.00	22.00	24.00	24.00	24.00
25	23.00	24.00	22.00	22.00	22.00	21.00
26	22.00	21.00	23.00	22.00	24.00	21.00
27	25.00	24.00	23.00	24.00	23.00	26.00
28	23.00	22.00	24.00	25.00	24.00	25.00
29	25.00	26.00	24.00	23.00	24.00	26.00
30	22.00	21.00	23.00	22.00	23.00	23.00

31	**23.00**	**22.00**	**23.00**	**24.00**	**24.00**	**24.00**
32	**25.00**	**24.00**	**23.00**	**26.00**	**23.00**	**24.00**
33	**21.00**	**20.00**	**22.00**	**22.00**	**23.00**	**22.00**
34	**25.00**	**24.00**	**25.00**	**24.00**	**25.00**	**25.00**
35	**25.00**	**26.00**	**23.00**	**26.00**	**24.00**	**23.00**
36	**22.00**	**21.00**	**23.00**	**22.00**	**23.00**	**24.00**
37	**23.00**	**22.00**	**21.00**	**22.00**	**22.00**	**24.00**
38	**25.00**	**24.00**	**23.00**	**26.00**	**24.00**	**23.00**
39	**22.00**	**23.00**	**22.00**	**21.00**	**23.00**	**22.00**
40	**23.00**	**24.00**	**23.00**	**22.00**	**23.00**	**24.00**
41	**25.00**	**26.00**	**26.00**	**24.00**	**23.00**	**24.00**
42	**20.00**	**21.00**	**19.00**	**20.00**	**21.00**	**22.00**
43	**25.00**	**26.00**	**27.00**	**25.00**	**24.00**	**26.00**
44	**21.00**	**22.00**	**23.00**	**22.00**	**20.00**	**23.00**
45	**21.00**	**22.00**	**23.00**	**20.00**	**21.00**	**22.00**
46	**24.00**	**25.00**	**23.00**	**24.00**	**22.00**	**26.00**
47	**23.00**	**22.00**	**22.00**	**21.00**	**25.00**	**24.00**
48	**23.00**	**24.00**	**21.00**	**25.00**	**22.00**	**24.00**
49	**17.00**	**16.00**	**18.00**	**19.00**	**20.00**	**17.00**
50	**25.00**	**25.00**	**23.00**	**24.00**	**23.00**	**24.00**
51	**23.00**	**22.00**	**22.00**	**24.00**	**25.00**	**24.00**
52	**23.00**	**24.00**	**22.00**	**25.00**	**22.00**	**23.00**
53	**17.00**	**16.00**	**19.00**	**18.00**	**19.00**	**17.00**
54	**20.00**	**20.00**	**20.00**	**22.00**	**21.00**	**22.00**
55	**23.00**	**24.00**	**25.00**	**24.00**	**25.00**	**24.00**
56	**25.00**	**26.00**	**23.00**	**23.00**	**27.00**	**23.00**
57	**22.00**	**21.00**	**23.00**	**24.00**	**21.00**	**24.00**
58	**23.00**	**22.00**	**23.00**	**24.00**	**25.00**	**24.00**
59	**25.00**	**24.00**	**23.00**	**26.00**	**23.00**	**24.00**
60	**20.00**	**20.00**	**21.00**	**22.00**	**19.00**	**22.00**
61	**26.00**	**24.00**	**28.00**	**24.00**	**24.00**	**27.00**
62	**25.00**	**26.00**	**22.00**	**23.00**	**27.00**	**24.00**

63	**22.00**	**21.00**	**24.00**	**23.00**	**24.00**	**22.00**
64	**23.00**	**22.00**	**23.00**	**24.00**	**25.00**	**21.00**
65	**25.00**	**24.00**	**23.00**	**26.00**	**22.00**	**27.00**
66	**22.00**	**23.00**	**22.00**	**21.00**	**25.00**	**22.00**
67	**23.00**	**24.00**	**23.00**	**22.00**	**23.00**	**24.00**
68	**25.00**	**26.00**	**27.00**	**24.00**	**23.00**	**24.00**
69	**20.00**	**22.00**	**21.00**	**23.00**	**22.00**	**20.00**
70	**25.00**	**26.00**	**24.00**	**23.00**	**27.00**	**27.00**
71	**23.00**	**21.00**	**22.00**	**24.00**	**23.00**	**24.00**
72	**23.00**	**24.00**	**22.00**	**25.00**	**22.00**	**23.00**
73	**17.00**	**16.00**	**18.00**	**17.00**	**20.00**	**19.00**
74	**21.00**	**22.00**	**23.00**	**24.00**	**23.00**	**23.00**
75	**23.00**	**22.00**	**22.00**	**24.00**	**25.00**	**24.00**
76	**23.00**	**24.00**	**21.00**	**22.00**	**22.00**	**25.00**
77	**17.00**	**16.00**	**18.00**	**19.00**	**21.00**	**20.00**
78	**20.00**	**20.00**	**20.00**	**22.00**	**23.00**	**22.00**
79	**22.00**	**24.00**	**23.00**	**24.00**	**24.00**	**21.00**
80	**25.00**	**26.00**	**23.00**	**27.00**	**22.00**	**24.00**
81	**22.00**	**21.00**	**24.00**	**20.00**	**22.00**	**23.00**
82	**23.00**	**22.00**	**23.00**	**24.00**	**25.00**	**23.00**
83	**25.00**	**24.00**	**23.00**	**26.00**	**23.00**	**26.00**
84	**20.00**	**21.00**	**20.00**	**22.00**	**23.00**	**22.00**
85	**24.00**	**24.00**	**25.00**	**24.00**	**24.00**	**25.00**
86	**25.00**	**26.00**	**24.00**	**23.00**	**24.00**	**26.00**
87	**22.00**	**21.00**	**23.00**	**24.00**	**21.00**	**20.00**
88	**23.00**	**22.00**	**21.00**	**24.00**	**23.00**	**22.00**
89	**25.00**	**24.00**	**23.00**	**26.00**	**22.00**	**23.00**
90	**22.00**	**23.00**	**22.00**	**21.00**	**24.00**	**22.00**
91	**23.00**	**24.00**	**23.00**	**22.00**	**23.00**	**24.00**
92	**25.00**	**26.00**	**27.00**	**24.00**	**23.00**	**22.00**
93	**20.00**	**23.00**	**19.00**	**22.00**	**23.00**	**24.00**
94	**25.00**	**26.00**	**24.00**	**23.00**	**26.00**	**25.00**

95	17.00	16.00	19.00	18.00	20.00	19.00
96	20.00	21.00	19.00	22.00	23.00	22.00
97	24.00	24.00	26.00	24.00	24.00	25.00
98	25.00	26.00	24.00	24.00	26.00	26.00
99	22.00	21.00	23.00	24.00	24.00	23.00
100	23.00	22.00	23.00	24.00	25.00	24.00
101	25.00	24.00	24.00	26.00	25.00	25.00
102	22.00	23.00	22.00	21.00	22.00	23.00
103	23.00	24.00	23.00	23.00	23.00	24.00
104	25.00	26.00	27.00	24.00	24.00	25.00
105	20.00	23.00	22.00	22.00	20.00	21.00
106	25.00	26.00	26.00	27.00	25.00	24.00
107	21.00	22.00	23.00	22.00	21.00	23.00
108	21.00	22.00	23.00	22.00	22.00	21.00
109	24.00	25.00	25.00	26.00	24.00	25.00
110	23.00	22.00	22.00	23.00	24.00	24.00
111	23.00	24.00	23.00	24.00	23.00	24.00
112	17.00	17.00	19.00	18.00	17.00	19.00
113	20.00	20.00	21.00	22.00	21.00	22.00
114	22.00	24.00	23.00	24.00	21.00	24.00
115	25.00	26.00	24.00	24.00	23.00	25.00
116	22.00	21.00	22.00	22.00	23.00	22.00
117	23.00	22.00	23.00	24.00	23.00	22.00
118	23.00	24.00	21.00	25.00	22.00	24.00
119	17.00	16.00	18.00	20.00	19.00	17.00
120	21.00	23.00	22.00	21.00	22.00	20.00
121	23.00	20.00	22.00	24.00	24.00	22.00
122	23.00	24.00	23.00	24.00	22.00	25.00
123	17.00	18.00	18.00	17.00	19.00	16.00
124	20.00	21.00	20.00	22.00	23.00	22.00
125	24.00	24.00	25.00	24.00	26.00	24.00
126	25.00	26.00	23.00	23.00	24.00	26.00

127	22.00	21.00	22.00	23.00	23.00	22.00
128	23.00	22.00	23.00	24.00	21.00	25.00
129	25.00	24.00	23.00	26.00	23.00	24.00
130	20.00	20.00	19.00	21.00	22.00	18.00
131	19.00	18.00	17.00	20.00	21.00	20.00
131	25.00	26.00	23.00	24.00	24.00	26.00
133	22.00	21.00	23.00	22.00	23.00	24.00
134	23.00	22.00	23.00	22.00	23.00	22.00
135	25.00	24.00	23.00	24.00	25.00	24.00
136	22.00	23.00	23.00	24.00	23.00	22.00
137	23.00	24.00	23.00	22.00	23.00	24.00
138	24.00	26.00	24.00	24.00	26.00	24.00
139	18.00	20.00	19.00	18.00	20.00	21.00
140	19.00	21.00	19.00	20.00	21.00	18.00
141	16.00	18.00	17.00	19.00	18.00	16.00
142	24.00	23.00	25.00	24.00	23.00	25.00
143	22.00	21.00	24.00	22.00	21.00	24.00
144	23.00	23.00	25.00	23.00	23.00	24.00
145	25.00	27.00	24.00	25.00	27.00	24.00
146	22.00	24.00	21.00	22.00	24.00	23.00
147	25.00	26.00	27.00	25.00	24.00	26.00
148	24.00	23.00	25.00	24.00	23.00	24.00
149	21.00	20.00	23.00	21.00	22.00	23.00
150	22.00	24.00	20.00	22.00	24.00	21.00
151	23.00	22.00	23.00	24.00	24.00	24.00
152	25.00	24.00	23.00	26.00	24.00	25.00
153	22.00	23.00	22.00	21.00	22.00	22.00
154	23.00	24.00	23.00	22.00	23.00	24.00
155	25.00	26.00	26.00	24.00	27.00	25.00
156	20.00	24.00	20.00	25.00	23.00	20.00
157	25.00	26.00	24.00	22.00	24.00	26.00
158	21.00	22.00	23.00	20.00	21.00	22.00

159	21.00	22.00	23.00	22.00	20.00	22.00
160	24.00	25.00	23.00	24.00	25.00	26.00
161	23.00	22.00	22.00	24.00	24.00	24.00
162	23.00	24.00	22.00	21.00	22.00	24.00
163	17.00	16.00	18.00	19.00	19.00	18.00
164	20.00	21.00	22.00	22.00	21.00	22.00
165	20.00	22.00	23.00	21.00	22.00	23.00
166	25.00	26.00	24.00	24.00	26.00	24.00
167	22.00	21.00	23.00	22.00	23.00	23.00
168	23.00	22.00	23.00	24.00	24.00	25.00
169	23.00	24.00	21.00	25.00	22.00	24.00
170	17.00	16.00	18.00	20.00	17.00	19.00
171	25.00	25.00	23.00	24.00	25.00	26.00
172	23.00	24.00	22.00	24.00	24.00	24.00
173	23.00	24.00	20.00	25.00	22.00	25.00
174	18.00	16.00	17.00	19.00	20.00	18.00
175	20.00	21.00	20.00	22.00	22.00	19.00
176	25.00	24.00	26.00	24.00	23.00	24.00
177	25.00	26.00	25.00	24.00	24.00	24.00
178	22.00	21.00	23.00	20.00	22.00	23.00
179	23.00	22.00	23.00	23.00	24.00	22.00
180	25.00	24.00	23.00	26.00	23.00	24.00
181	20.00	20.00	19.00	21.00	22.00	21.00
182	22.00	24.00	24.00	24.00	21.00	23.00
183	25.00	26.00	22.00	24.00	24.00	24.00
184	22.00	21.00	23.00	20.00	21.00	23.00
185	23.00	22.00	24.00	24.00	24.00	23.00
186	25.00	24.00	23.00	26.00	22.00	23.00
187	22.00	23.00	22.00	21.00	24.00	22.00
188	23.00	24.00	23.00	22.00	23.00	24.00
189	25.00	26.00	27.00	24.00	23.00	24.00
190	20.00	22.00	19.00	21.00	22.00	19.00

191	25.00	26.00	26.00	24.00	26.00	24.00
192	21.00	22.00	23.00	23.00	23.00	23.00
193	21.00	22.00	23.00	22.00	22.00	23.00
194	25.00	25.00	24.00	25.00	27.00	27.00
195	23.00	21.00	22.00	23.00	22.00	24.00
196	23.00	24.00	22.00	24.00	25.00	24.00
197	17.00	16.00	18.00	19.00	20.00	19.00
198	20.00	20.00	20.00	22.00	23.00	22.00
199	25.00	24.00	25.00	24.00	24.00	25.00
200	25.00	26.00	24.00	24.00	23.00	25.00
201	22.00	21.00	23.00	22.00	23.00	23.00
202	23.00	22.00	23.00	24.00	24.00	25.00
203	25.00	24.00	23.00	26.00	24.00	24.00
204	20.00	20.00	21.00	22.00	19.00	21.00
205	25.00	24.00	25.00	25.00	25.00	24.00
206	25.00	26.00	23.00	23.00	23.00	24.00
207	22.00	21.00	22.00	23.00	21.00	23.00
208	23.00	22.00	23.00	24.00	24.00	24.00
209	25.00	24.00	23.00	23.00	23.00	24.00
210	22.00	23.00	22.00	21.00	23.00	21.00
211	23.00	24.00	23.00	22.00	23.00	22.00
212	25.00	26.00	24.00	24.00	23.00	24.00
213	22.00	24.00	23.00	21.00	20.00	23.00
214	25.00	26.00	27.00	23.00	26.00	24.00
215	21.00	22.00	22.00	23.00	20.00	23.00
216	21.00	22.00	23.00	22.00	21.00	22.00
217	25.00	25.00	24.00	25.00	24.00	27.00
218	23.00	21.00	22.00	24.00	22.00	24.00
219	23.00	24.00	21.00	26.00	22.00	24.00
220	21.00	18.00	19.00	21.00	20.00	21.00
221	25.00	25.00	24.00	25.00	27.00	25.00
222	23.00	22.00	22.00	24.00	25.00	24.00

223	23.00	24.00	22.00	24.00	22.00	24.00
224	17.00	18.00	19.00	21.00	17.00	20.00
225	20.00	22.00	20.00	18.00	19.00	21.00
226	25.00	24.00	25.00	25.00	25.00	25.00
227	25.00	26.00	25.00	24.00	26.00	24.00
228	22.00	21.00	23.00	20.00	21.00	22.00
229	23.00	22.00	23.00	23.00	24.00	24.00
230	25.00	24.00	25.00	26.00	23.00	24.00
231	20.00	21.00	19.00	22.00	21.00	22.00
232	25.00	24.00	25.00	24.00	25.00	24.00
233	25.00	26.00	23.00	24.00	24.00	24.00
234	22.00	21.00	22.00	23.00	21.00	23.00
235	23.00	22.00	23.00	24.00	24.00	22.00
236	25.00	24.00	23.00	23.00	24.00	26.00
237	22.00	23.00	22.00	21.00	23.00	22.00
238	23.00	24.00	23.00	22.00	23.00	24.00
239	25.00	26.00	27.00	24.00	23.00	24.00
240	20.00	22.00	21.00	22.00	21.00	22.00
241	25.00	26.00	24.00	26.00	23.00	24.00
242	23.00	21.00	22.00	24.00	25.00	24.00
243	23.00	24.00	22.00	24.00	25.00	22.00
244	17.00	18.00	20.00	19.00	18.00	19.00
245	25.00	25.00	24.00	24.00	26.00	27.00
246	23.00	22.00	22.00	24.00	24.00	23.00
247	23.00	24.00	22.00	21.00	22.00	24.00
248	19.00	21.00	20.00	18.00	22.00	20.00
249	22.00	21.00	20.00	22.00	23.00	22.00
250	25.00	25.00	26.00	26.00	25.00	24.00