FIREWALL INFORMATION AND SECURITY VISUALIZATION

Improving the usage and adoption of modern network firewalls by novice users

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE
FACULTY OF SCIENCE
AT THE UNIVERSITY OF CAPE TOWN
IN FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE

By
Mogamad Yaqeen Gasant
February 2007

Supervised by
Gary Marsden

Abstract

The increasing number of people having access to computers and the Internet and the numerous services provided by the Internet - e.g., Internet banking, online shopping, eBay, email - emphasizes the need for computer security which is understandable to novice users. Whilst the technology underlying a firewall is effective, most users have no idea how to configure the software to suit their needs.

This research focuses on personal firewalls because it is our belief and I will show that personal firewalls are more at risk than those of large corporations. Our hypothesis for this research is that many of the users who install personal firewalls lack the knowledge to properly configure them. We propose that the problem with a personal firewall is that most users do not have the correct conceptual models of interaction between computer, firewall, and security in order to configure these personal firewalls correctly. We aim to use information visualization [3] as a possible solution to the problem of novice users configuring their personal firewalls.

This dissertation presents a new information visualization personal firewall, which was designed and developed using a combination of human computer interaction methodologies and techniques as well as information visualization [3] and the piccolo toolkit [9].

Once we had completed studies on existing personal firewalls and novice users' personal firewall knowledge, we brainstormed possible visualization solutions and built a high-level prototype. We then refined the prototype with conceptual model extraction and expert evaluations and developed the new information visualization personal firewall using piccolo toolkit, Microsoft visual studio.net and C#. We then tested the usability of the new information visualization personal firewall and it was shown that visualization does improve the usage of novice users to a certain degree but design choices can be detrimental to the improvement of usage.

Acknowledgements

There are a number of people that need acknowledgement and many thanks because without their involvement, guidance and support this work would not have been possible. Firstly, I would like to thank Professor Gary Marsden, my supervisor. Thank you, Gary for all your guidance, support, encouragement, speedy feedback, and constant availability throughout the course of this study. It has truly been a wonderful experience for me.

I would like to thank my mom and dad for affording me the opportunity to reach this level of my studies and for the ongoing guidance and support throughout not only this research but also my whole life to date. I would like to also thank my siblings and in-laws for their support. To my beautiful wife, thanks for your support, guidance, patience and love that you have shown me throughout my studies. Last but not least, thanks to the socially aware computing group, the Collaborative Visual Computing (CVC) lab and all the interviewee volunteers. I value your guidance and support, thank you.

I acknowledge that all references are accurately recorded and that, unless stated, all work contained herein is my own.

This work was supported by NRF and Telkom SA Ltd.

Contents

Chapter 1: Introduction **1**

1. Introduction **1**

1.1 What is a personal firewall? 3

1.2 Motivation 3

1.3 Aim 5

1.4 Methodologies and techniques 6

1.4.1 Evaluation methodologies 6

1.4.2 Design techniques 8

1.5 Dissertation outline 9

Chapter 2: Literature Review **10**

2. Literature review **10**

2.1 Introduction 10

2.2 Experiment 1: The study of existing personal firewalls or computer security systems 10

2.3 Exploration of Existing Personal Firewalls 11

2.3.1 Panda Platinum Internet Security 12

2.3.2 ZoneAlarm Pro 16

2.3.3 Norton Internet Security 18

2.3.4 Microsoft Windows firewall 20

2.5 Information Visualization Origins and Exploration of Its Techniques 21

2.5.1 Origins of Information Visualization 21

2.5.2 Information Visualization Techniques 22

Chapter 3: Methodology **24**

3. Methodology **24**

3.1 Introduction 24

3.2 Metaphor Development and Experiments 24

3.3 Experiments and Methodologies 25

3.3.1 Experiment 2: The study of novice user's personal firewall or computer security system knowledge 25

3.3.2 System Design: Brainstorming and paper prototyping 27

3.3.3 Experiment 3: Conceptual model extraction and expert evaluation of the new information personal firewall prototype 28

3.3.4 Experiment 4: Task-Based evaluation of the new information visualization personal firewall 29
Chapter 4: Experiments, results and discussion 31
4. Experiments, results and discussion 31
4.1 Introduction 31
4.2 Summary of the experiment structure 31
4.3 Experiments and results 32
4.3.1 Experiment 1: The study of existing personal firewalls or computer security systems. 32
4.3.2 Experiment 2: The study of novice users' personal firewall or computer security system knowledge 38
4.3.3 System Design: Brainstorming and paper prototyping 43
4.3.4 Experiment 3: Conceptual model extraction and expert evaluation of the new information personal firewall prototype 48
Chapter 5: Evaluation of the new information personal firewall visualization... 54
5. Evaluation of the new information personal firewall visualization 54
5.1 Introduction 54
5.2 Screenshots of the visualization and how it works 54
5.3 Experiment 4: Task-Based evaluation of the new information personal firewall visualization 60
5.4 Experiment 4 conclusion 70
Chapter 6: Conclusion and future work 72
6. Conclusion and Future Work 72
6.1 Conclusion 72
6.1.1 Research Question One Conclusion 72
6.1.2 Research Question Two Conclusion 74
6.2 Future Work 74
6.2.1 Zoom Feature 74
6.2.2 Add or Remove, Application or Port Nodes 74
6.2.3 Refinement of Icons and Tick, Cross and Prompt Control Buttons . 75
6.2.4 Visualization solution to the application or port list becoming extremely large in numbers 75

6.2.5 Connect the new information visualization personal firewall to the back-end of a personal firewall and see if this functionality affects the visualization choices made 75
6.2.6 Add this new information visualization personal firewall as an added view to personal firewalls. 76
References **77**
Appendix A **80**
Appendix B **82**
Appendix C **83**

List of Figures

Figure 1.1 Novice user's usage of the metaphor leads to understanding of the Personal Firewall Functionality. 5
Figure 2.1 Programs with network access 12
Figure 2.2 Access Settings of the Automatic firewall protection settings. 13
Figure 2.3 Panda Platinum Internet Security (8.05.01) [18]. 14
Figure 2.4 Automatic firewall protection settings. 14
Figure 2.5 View Network Activity [18]. 15
Figure 2.6 ZoneAlarm Pro Firewall Settings [4]. 16
Figure 2.7 Internet Zone Security Settings [4]. 18
Figure 2.8 Norton Internet Security: Program Control [26] 19
Figure 2.9 Windows Firewall Exceptions Settings [17]. 20
Figure 3.1 Likert Rating Scale to be used in the questionnaire for this 26
study. 26
Figure 4.1 The first suggested visualization for the metaphor. 44
Figure 4.2 Agreed visualization choice for the metaphor. 45
Figure 4.3 An example node including controls 47
Figure 5.1 Screenshot 1: Overview First 55
Figure 5.2 Screenshot 2: Selecting the Internet Explorer node by clicking the node itself. 56
Figure 5.3 Screenshot 3: Displaying the port nodes that have an access status for the Internet Explorer application. 57
Figure 5.4 Screenshot 4: Changing the status of the HTTP port node to deny by clicking on the big X of the HTTP port node 58
Figure 5.5 Screenshot 5: Change all port nodes' access to deny status by clicking on the big X of the Internet Explorer node. 59
Figure 5.6 Summary of the results for the repeat of the cyclic conceptual model extraction questions. 65
Figure 5.7 Summary of the successful or unsuccessful results of the task based evaluation experiment. 65

List of Tables

Table 4.1: Panda Platinum Internet Security (version 8.05.01) Functionality 33
Table 4.2: Zone Alarm Pro Functionality 34
Table 4.3: Norton Internet Security 2003 Functionality 35
Table 4.4: Microsoft Windows Firewall (Service Pack 2) Functionality 35
Table 4.5: Different Types of Visualization 36
Table 4.6: Summary of experiment 2 short questionnaire responses. 80

Chapter 1: Introduction

1. Introduction

Access to technology is increasing in leaps and bounds. According to the world Internet usage and population statistics, global Internet usage growth for 2000 – 2007 is 202.9% with substantial growth of 625.8%, 490.1% and 391.3% in Africa, Middle East and Latin America/Caribbean, respectively [11]. Consequently, increasing numbers of people are purchasing or acquiring access to computers hence increasing the number of people who have the opportunity of connecting to the Internet.

The Internet provides users with many convenient and essential services, e.g., banking, online shopping, auctions and email. Conversely, vital information can be compromised if users connect to the Internet without sufficient protection. Insufficient protection makes users, and the information on their computers, vulnerable to an array of attacks from hackers, crackers and spyware.

- "On the 29th of January 2003:

  PSINet Europe purposely built an unprotected server and connected it to the Internet to determine how quickly it would be compromised. Their findings were astonishing:

  - The server was maliciously attacked 467 times in the first 24 hours.
  - Most of the attacks originated in the US or Western Europe.
  - After 3 weeks, a total of 626 attacks were detected against the server.

- On the 1st of February 2003:

  An analysis of the Sapphire/Slammer SQL worm shows:

  - This worm required roughly 10 minutes to spread worldwide making it **by far the fastest worm to date**.
  - In the early stages [the number of compromised hosts] was doubling in size every 8.5 seconds.

- At its peak, achieved approximately 3 minutes after it was released, Sapphire scanned the net at over 55 million IP addresses per second.
- It infected at least 75,000 victims and probably considerably more.

- On the 17th of January 2004:

  - Processing between 50,000 and 60,000 new copies per hour, W32/Mydoom.A has exceeded the infamous SoBig.F virus in terms of copies intercepted, and the number continues to rise.
  - Message Labs collected over 1.2 Million copies of W32/Mydoom.A.
  - At its peak infection rate, about 1 in 12 emails on the Internet were MyDoom Viruses. [22] "

The above statistics are the reason why firewall and security technology has become a top priority within businesses and homes across the globe. They show the damage that viruses and worms can cause and how susceptible an unprotected computer can be. However, the security of a computer is not only provided by anti-virus software alone. "Anti-virus software is designed to stop or eliminate viruses, and/or recover data affected by viruses" [10] – meaning that the virus has already infected the computer and has already breached the security of the computer. The security of a computer is provided by a firewall, which should prevent the computer from becoming infected in the first place. This is why the focus of this thesis is on firewalls and not anti-virus software; firewalls provide the first line of defense.

Firewalls have the sole purpose of protecting stand alone computers or computer networks from security threats all while still providing the computer user with access to the Internet and wide area networks [25].

There are two types of firewalls:

1. Hardware firewall – a computer that protects a larger computer network. This is found in large corporations or universities [27]. In these corporations or universities, these firewalls provide protection of the internal corporate or university network from the external network e.g., the Internet. An example is an IP packet filtering firewall which monitors and examines every packet,

whether it is incoming or outgoing and it decides whether to allow or block the packet [30].

2. Software firewall – a program that runs on a computer that is used to protect a single computer or a small number of computers [27].

In this research, we will be focusing on the second type of system described above, also known as a Personal Firewall. It is our belief that users of Personal Firewalls are more at risk than large corporations, as individuals often lack the expertise to properly configure their own firewalls. The following section will provide a more detailed description of a Personal Firewall.

1.1 What is a personal firewall?

There are numerous definitions of a personal firewall. However, the following two definitions provide a concise meaning of a personal firewall:

- "*Personal Firewalls are software products that act to safeguard an end user's computer on the Internet by monitoring attempts to access or probe his or her system*" [2].
- "*A personal firewall (sometimes called a desktop firewall) is a software application used to protect a single Internet-connected computer from intruders*" [21].

Based on the above definitions, it is safe to conclude that, in essence, a personal firewall is computer software that:

1. at a functional level, monitors and restricts data to and from the computer.
2. from the user perspective provides security against intruders, for computers connected to the Internet.

1.2 Motivation

- "**Juvenile Computer Hacker Cuts Off FAA Tower at regional airport** – First Federal charges brought against a juvenile for computer crime" [20].

- "**Computer Hacker Charged** – 29 year old Matthew Schuster is accused of transmitting a program causing damage to a protected computer and intentionally accessing a protected computer without authorization" [16].
- "**Brazilian hackers attack email bank accounts** – Brazilian police arrest 53 people suspected of stealing close to $30 million through Internet fraud" [28].
- "**MyDoom (virus) continues to cause chaos** – The outbreak caused by MyDoom.m caused the search engines either to intermittently fail, or return results far slower than usual" [29].
- **"Hacker cleans out bank accounts** - Hundreds of thousands of rands stolen via Internet from Absa clients" [14].

The above headlines highlight the need for the security provided by a personal firewall or firewalls in general. These computer crimes are of a serious nature. However, one has to ask the question, if a firewall is supposed to protect a computer from intruders and control the communications to and from a computer, then how do the intruders still manage to gain access to computers and cause major damage?

The configuration of your personal firewall is the important factor that determines how secure your personal firewall is going to be [32]. Research has claimed that more than 90% of all computer security failures are probably caused by errors made during the configuration of the security mechanism [31]. Our hypothesis is that many of the users who install personal firewalls lack the knowledge to properly configure them. We propose that the problem with a personal firewall is that most users do not have the correct conceptual models of interaction between computer, firewall and security in order to configure these personal firewalls correctly.

The protection of a computer does not end with the installation and activation of a personal firewall; the computer is only protected once the personal firewall is correctly configured. The level of protection is entirely dependent on the effective configuration of the personal firewall.

This research is therefore focused on the usage of personal firewalls by novice users (by novice, we mean someone who is proficient in using application software, but has no understanding of the underlying operating system and hardware). We investigate

whether novice users can configure their personal firewalls sufficiently and how they fare when presented with personal firewall information in a different, more visual, form. The following section aims at explaining a different approach to presenting personal firewall information such that novices could configure their personal firewalls.

1.3 Aim

The aim of this research is to use information visualization as a possible solution to the problem of novice users configuring their personal firewalls – information visualization can be used to make explicit the interactions between the firewall, operating system and application software.

Information visualization is "the use of computer-supported, interactive, visual representations of abstract data to amplify cognition" [3, pp 7 - 8]. The aim is to use visualizations of security information to build a familiar, or intuitive, metaphor that the novice users can interpret correctly.

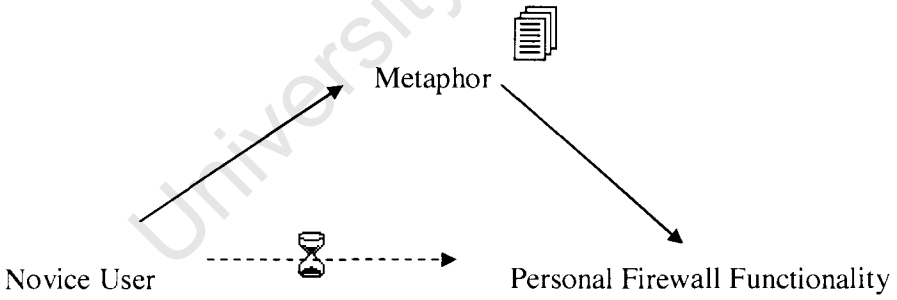

Figure 1.1 - Novice user's usage of the metaphor leads to understanding of the Personal Firewall Functionality.

A metaphor is defined as – "a figure of speech in which a word or phrase literally denoting one kind of object or idea is used in place of another to suggest a likeliness or analogy between them" [8].

Developing the metaphor in this context, it has to be a visual representation as opposed to "a word or phrase" that "denotes one kind of object or idea". This visual representation has to be in place of textual firewall functionality information, thus

building an analogy between the visual representation and the functionality of a firewall. This visual representation will allow users to acquire an accurate understanding of what they are doing whilst configuring or using a firewall. (See Fig. 1.1)

Besides designing a visual metaphor, the user must interact with the visualization. Much work has been done in this area and one of the most reliable guidelines when developing visualizations is Ben Shneiderman's Visual Information-Seeking Mantra: Overview first, zoom and filter, then details-on-demand [23]. This mantra is regarded as a useful starting point when designing an interface and will be used to guide the creation of our visual metaphor [23].

Should the novice users understand the metaphor, they can use the metaphor to understand the functionality of the personal firewall and can therefore configure the personal firewall to provide sufficient protection for the computer (see Figure 1.1).

1.4 Methodologies and techniques

The methods and techniques that will be used for this research are taken broadly from the field of Human-Computer Interaction (HCI). They were chosen as they focus on discovering how users understand concepts in computing, rather than forcing the ideas of the technology (e.g. ports, protocols) onto the user. Specifically, we shall be using:

1.4.1 Evaluation methodologies

- **Conceptual Model Extraction**

  Conceptual Model Extraction is a fairly new HCI method based on conceptual models. A conceptual model is a functional, behavioral and appearance representation of the proposed system based on a set of incorporated ideas and concepts that can be understood by users in the way it should be [19, pp 40]. This method attempts to obtain information from the users' perception and interpretation of the proposed system, meaning the users set of incorporated ideas and concepts of the functions, behavior and appearance of the proposed system.

This method can provide two types of conceptual models. They are an initial conceptual model and a formative conceptual model [15]. An initial conceptual model can demonstrate how the user perceives the proposed system for the first time. A formative conceptual model can demonstrate how the user perceives the proposed system after using it for a while. This method's strengths lie in the fact that it can provide people's understanding of the proposed system before and after they have used the system. It is not the preferred method when attempting to explore system exploration and learning [15].

We expect qualitative data from this method, which is information from the users' perception and interpretation of the proposed system. .This qualitative data can be used to assist the design and development of the new personal firewall information visualization.

- **Artifact Walkthrough**

  Artifact Walkthrough is a structured observation technique, which is used in an exploration process involving the creation and use of artifacts [6]. This technique can be used to gain insight into how users have used a particular piece of software. For example, in this research the artifact is the way in which the personal firewall was configured. The benefits of an artifact walkthrough are that it demonstrates the series of actions performed by a user when performing a task; in our case it will provide an insight into why users configured their firewall the way they did.

  We expect qualitative data from this method, which is insight into how users use their particular software packages. This qualitative data can also be used to assist the design and development of the new personal firewall information visualization.

- **Task-Based Evaluation**

  Task-Based evaluation is based on an evaluation technique known as usability testing or user testing. It involves the performance measurement of typical users on tasks that have been carefully prepared and based on tasks that would

be typical to the system being designed [15]. The task-based tests are done in a controlled environment, involving typical users that are asked to perform carefully prepared tasks [15]. The data collected from these tests are the task completion time, the number of errors made during the task completion time, and the path the user took to navigate through the system in order to complete the task [15]. This data is used to analyze the performance of the user when conducting a set of customization tasks using firewall software.

We expect qualitative and quantitative data from this method. The quantitative data that could be yielded from this method is the success and failure rate of each task e.g. Task 1 had 9 people who successfully completed the task and 1 person who was unsuccessful. This data could assist us in determining whether each task was a success or not. This method also allows us to observe how usable the new personal firewall information visualization is based on the steps the user takes in attempting to successfully complete a task.

1.4.2 Design techniques

- **Paper Prototyping**

This design technique is used in the designing, testing and refinement of user interfaces [24, pp 3, pp 12]. Before and during the 1980s, Paper Prototyping was used by technology companies. It was in the early 1990s that it was regarded as a fringe technique and was used by a usability pioneers. In the mid 1990s, IBM, Digital, Honeywell and Microsoft began experimenting with this design technique [24, pp 3, pp 12].

The benefits of using this technique are receiving user feedback at an early stage, helps provide rapid iterative development and using this technique requires no technical skills [24, pp 3, pp 12]. One weakness that could arise with paper prototyping is that you might miss a few user interface ideas.

This technique should provide us with a paper prototype of what we expect the system to look like and what actions should occur when certain objects on the new personal firewall information visualization are clicked. A high-level prototype can be built based on this artifact.

1.5 Dissertation outline

Chapter 1 establishes that this research involves personal firewalls, the motivation, aim and methodology used for this research.

Chapter 2 provides information on existing personal firewalls and information visualization.

Chapter 3 explains which methodologies were selected and why they were selected for this research.

Chapter 4 explains and discusses experiments completed and experiment results.

Chapter 5 presents the final evaluation of the new information visualization personal firewall and the results.

Chapter 6 presents concluding remarks and recommendations for future work.

Chapter 2: Literature Review

2. Literature review

2.1 Introduction

This research begins by having a closer look at existing personal firewalls or Internet security packages and information visualization techniques.

The aim of exploring existing personal firewalls is: to gain knowledge on what functionality is used in existing personal firewalls; how the interface of existing personal firewalls is structured; and how the security information is structured. The aim of exploring information visualization techniques is to gain insight into what kind of techniques have previously been used and which information visualization techniques are relevant to this research.

2.2 Experiment 1: The study of existing personal firewalls or computer security systems

- **Aim**

  The aim of this study is to gain knowledge of the functionality, interface structure and how the security information is structured within existing personal firewalls.

- **Description of the study**

  This study will involve choosing a representative few, (about four or five,) existing personal firewall or computer security packages. These existing systems will be closely examined with respect to the above criteria, which are checking what functionality is available to the user; how the interfaces of these systems are structured with respect to visualization and the manner in which the security information is structured with respect to usage.

- **Methodology**

  The methodology will be inspection. This involves examining, assessing or scrutinizing each existing system with respect to the above criteria and noting useful information that will possible satisfy the aim of this study.

- **Possible Outcome or Results of the study**

  Possible outcomes or results that could be gained from this study will be a list of core functionality on offer by existing systems and insight into what, and how, existing systems structure their security information with respect to the interface. This list of functionality will be used in a future experiment to observe whether novice users would be familiar with the core functions and which of these functions are of importance to novice users. Information gained from examining interface structure can be used or modified in the future development of the new information visualization personal firewall design.

2.3 Exploration of Existing Personal Firewalls

Four of the more popular personal firewall or Internet security packages were chosen to be explored. They are as follows:

- **Panda Platinum Internet Security**

  The Panda Company was established in Bilbao, Spain [18]. It is privately owned and in 1995 it became a market leader in Spain. It started expanding to the rest of the world in 1996 [18]. They do business with consumers and businesses in over 200 countries [18].

- **ZoneAlarm Pro**

  Zone Alarm Pro is a product of a company called Check Point. Check Point is regarded as one of the most trusted internet security brands [4]. Check Points products can be found in global enterprises, small businesses and consumers' homes [4].

- **Norton Internet Security**

  Norton Internet Security is a product of a company called Symantec. In this research we will be investigating the 2003 version of Norton Internet Security. Symantec was established in 1982. On 23rd June 1989 it became an IPO. Symantec can be found in more than 40 countries worldwide [26].

- **Microsoft Windows Firewall (Service Pack 2)**

  Microsoft Windows Firewall was released with Windows XP Service Pack 2 (SP2) and as a consequence is automatically installed on almost every personal computer in the world.

The exploration of these personal firewalls or security packages will include inspecting the functionality on offer; and the way the interface and security information is structured with respect to the configuration of a personal firewall from a novice's perspective.

The type of features that we are looking for in each exploration area is as follows:

- **Functionality features:** Access Control, which is program, port, and protocol and PC control. We will compare each of the chosen packages based on the mechanisms they have or do not have in place for access control.

  Interface structure features: Program status interface access, which means having access to the program status of a personal firewall via the interface and being able to add or remove programs. We will compare each of the chosen packages based on the whether they do or do not exhibit a quick indication of program status.
- **Security information structure features:** Security information of programs running on a pc and the level of security terminology used.

2.3.1 Panda Platinum Internet Security

2.3.1.1 Personal Firewall Functionality

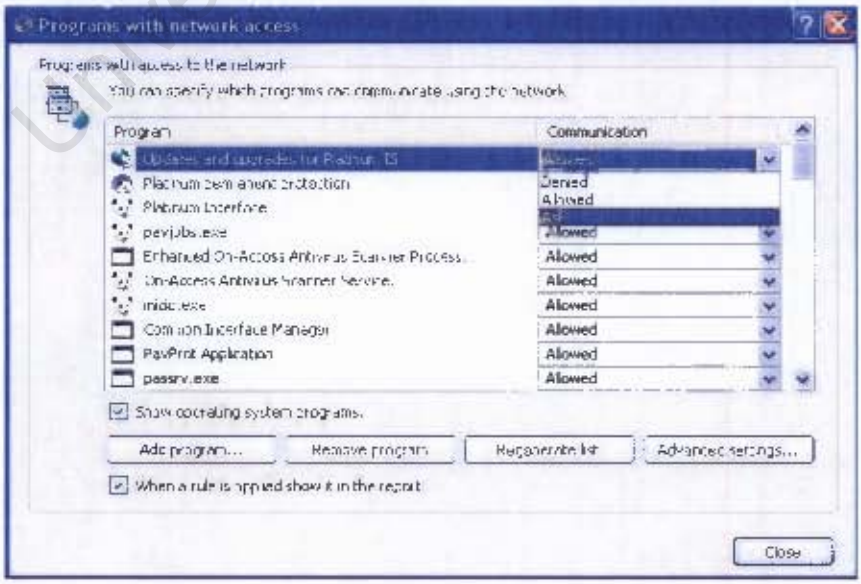

Figure 2.1 Programs with network access.

Panda Platinum's firewall protection functionality includes the following:

- **Program Access**

This function involves the accessibility of programs to the network i.e., the Internet. It also includes the addition and removal of programs. The accessibility of a program is dependent on the status setting, which is either allowed, deny or prompt/ask. (see Figure 2.1)

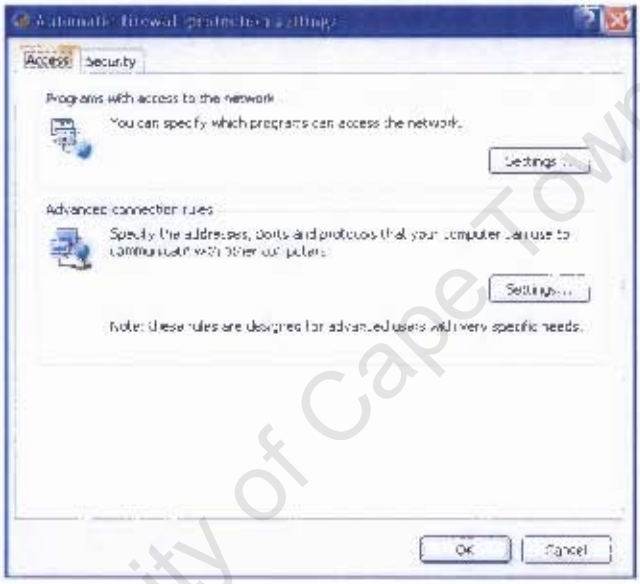

Figure 2.2 Access Settings of the Automatic firewall protection settings.

Port and Protocol Access

This function involves rules for specifying addresses, ports and protocols. These rules are used by your computer to communicate with other computers [18]. (see Figure 2.2)

- **View Network Activity**

This function provides the user with a view of which programs have inbound or outbound connections.

Figure 2.3 Panda Platinum Internet Security (8.05.01) [18].

2.3.1.2 Personal Firewall Interface and Security Information structure

Panda Platinum's firewall protection option (see Figure 2.3) contains possible aspects, involving interface and security information structure, which could hinder the personal firewall configuration process for novice users.

- **Interface Structure**

  There is no quick indication or overview of program status i.e., whether the program is allowed or denied and the inbound and outbound traffic of the computer.

Figure 2.4 Automatic firewall protection settings.

For the user to view program status, they have to click on the settings link for firewall protection, (see Figure 2.3), then click on a settings button, (see Figure 2.4), which takes them to the actual firewall protection settings. Once

they have selected "Settings", users are presented with a two tab menu, one for access and the other labeled security, (see Figure 2.2). Users then have to click on the programs with access to the network "Settings" button, which finally leads to a list of programs that contains the status of each program accessing the network, (see Figure 2.1). The user has to interact with three different interfaces to access program status. The procedure for adding or removing programs is the same as above because the add and remove program buttons are situated on the same interface as the program status. This could possibly be too many levels for a novice to navigate.

There is no indication or overview for firewall traffic. The user has to figure out that this information is accessible by clicking on the "View network activity" link for firewall protection, (see Figure 2.3). This could also be a possible problem for the novice users.

- **Security Information Structure**

Important information such as the list of programs allowed or denied access is hidden three levels down, as in the previous task. This information should be easier to access from a novice user's perspective.

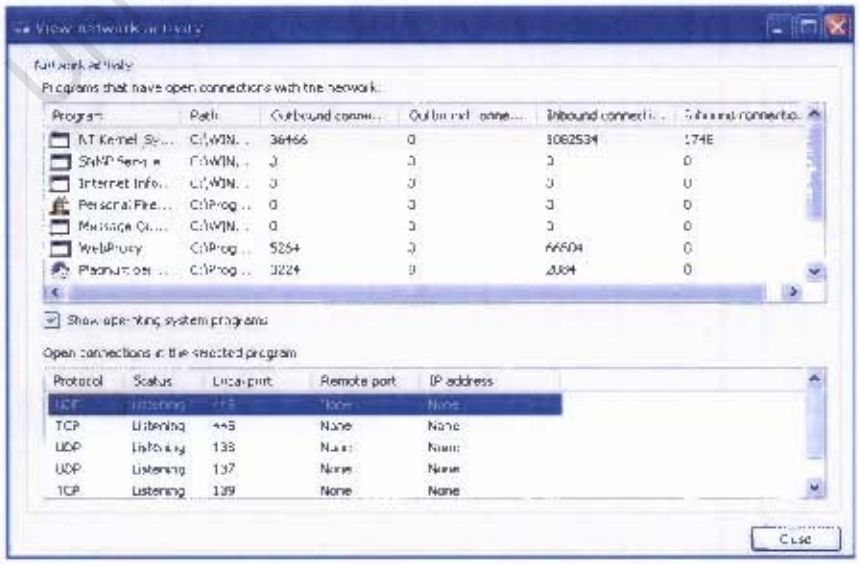

Figure 2.5 View Network Activity [18].

Another cause for concern is that Panda's security information contains technical firewall terminology that novice users would possibly have a problem with understanding: e.g., in Figure 2.5 words such as port, IP address, protocol and the numbers that represent the size of the inbound and outbound connections could be very difficult for a novice user to understand.

2.3.2 ZoneAlarm Pro

2.3.2.1 Personal Firewall Functionality

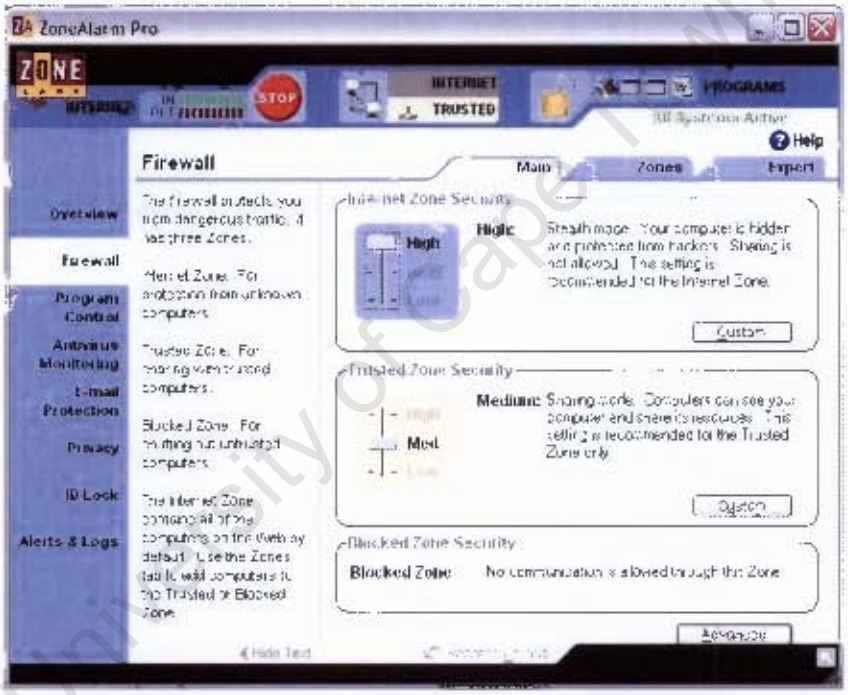

Figure 2.6 ZoneAlarm Pro Firewall Settings [4].

ZoneAlarm Pro's firewall functionality includes the following three zones of security:

- **Internet Zone Security**

  The function of this security zone is to protect your computer from unknown computers while on the internet, (see Figure 2.6) [4]. This function involves allowing and blocking of protocols and ports. This zone has three levels. A High, Medium, Low level, where high is the recommended choice it claims that at this level the computer will be hidden from hackers [4].

- **Trusted Zone Security**

The function of this security zone is to provide a level of protection while sharing resources on your computer with trusted computers, (see Figure 2.6) [4]. This function involves allowing and blocking of protocols and ports. This zone also has three levels, that being High, Medium and Low, where medium is the recommended choice and it claims that your computer is visible by other computers and can share its resources [4].

- **Blocked Zone Security**

  The function of this zone is to block computers that are not trusted by your computer, (see Figure 2.6) [4].

2.3.2.2 Personal Firewall Interface and Security Information structure

ZoneAlarm Pro also has possible aspects, involving interface and security information structure, which could hinder the personal firewall configuration process for novice users.

- **Interface Structure**

  ZoneAlarm pro does have a simple overview of program status and Internet traffic. It uses an open padlock that signifies that the programs are allowed and a stop sign signifying that all Internet access will be blocked, See Figure 2.6. This could cause a few problems because the use of the open pad lock and a stop sign is inconsistent. The inconsistency could confuse novice users because they use two metaphors to signify the same action i.e. open padlock signifies the programs allowed access and stop sign signifying not allowed. To be consistent the open padlock should have been a green go sign.

  It does not have an option to add programs and display their status. This is in a separate option called program control, (see Figure 2.6). This could be a possible problem because users might expect to find this option within the firewall but then have to explore another option to find the 'add programs' option.

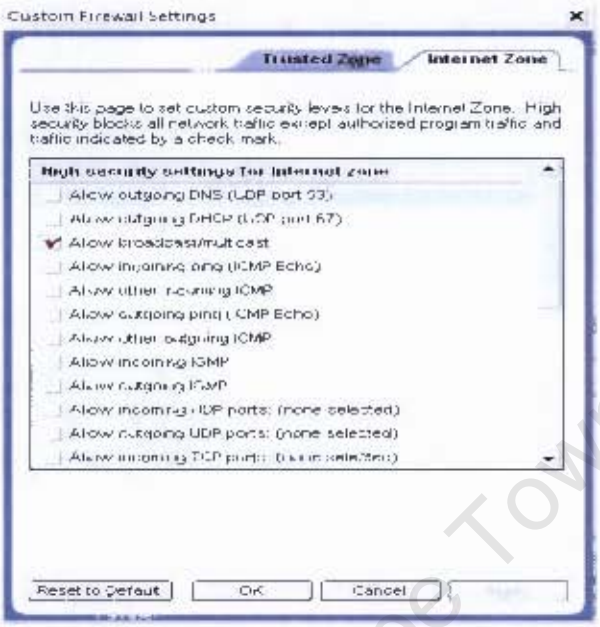

Figure 2.7 Internet Zone Security Settings [4].

Security Information Structure

Once again the security information contains very technical terminology that could be a problem for novice users to understand, (see Figure 2.7).

2.3.3 Norton Internet Security

2.3.3.1 Personal Firewall Functionality

Norton Internet Security's Personal Firewall Functionality includes the following:

- **Program Control**

  This function has two settings, automatic program control and manual program control. Automatic program control's function is configuring the access of Internet programs that are used for the first time. Thus reducing the number of alerts received [26]. Manual program control's function is configuring Internet access for individual programs [26]. It allows users to add, modify or remove a program and has a feature called program scan which allows the user to scan for all Internet-enabled programs.

- **Home Networking**

  This function allows the user to identify computers that are given access to and computers that are blocked from your computer [26]. It has two zones.

the trusted zone, which contains a list of computers that are allowed to access the user's computer, and the restricted zone, which contains a list of computers that are not allowed to access the user's computer. In each of these zones the user can add or remove trusted or restricted computers from their respective lists.

- **Advanced**

  This function contains the general and trojan horse rules. The adjustment of these rules are claimed to be advanced user settings that majority of the users will have no need to change [26].

2.3.3.2 Personal Firewall Interface and Security Information structure

Figure 2.8 Norton Internet Security: Program Control [26].

Norton Internet Security has problems that could hinder the personal firewall configuration process for novice users. These problems are similar to the problems described in the above two personal firewalls. These include:

- No indication of program status or Adding/Modifying/Removing programs option, which is Program Control, (see Figure 2.8). Program status has to be found by exploration of the configuration settings.

- The use of high technical terminology that could be a problem for novice users to understand.

2.3.4 Microsoft Windows firewall

2.3.4.1 Personal Firewall Functionality

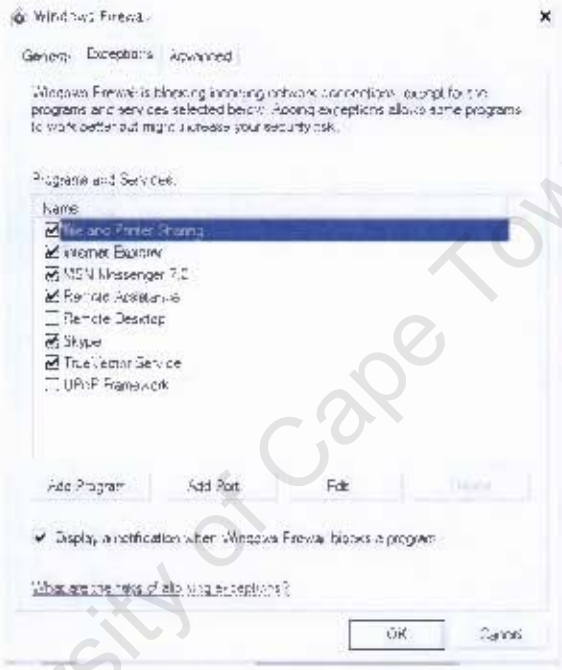

Figure 2.9 Windows Firewall Exceptions Settings [17].

Microsoft Windows Firewall Functionality includes the following:

- **Program Control**

This function allows programs and ports to be added to a list of programs, (see Figure 2.9). These programs are trusted or restricted by ticking a checkbox to trust a program and not ticking a checkbox to restrict a program, (see Figure 2.9). Port access for each program can also be set.

Advanced

These functions are aimed at advanced users, who might want to set specific functions such as Security logging, which creates log files, Network connection settings and Internet Control Message Protocol (IMCP) settings.

2.3.4.2 Personal Firewall Interface and Security Information structure

Windows firewall also exhibits the above mentioned hindrances of the personal firewall configuration process.

Windows Firewall does, however, use the tab labeled "Exceptions" which is the same as "Program Control" in the above personal firewalls, (see Figure 2.9). The use of Exceptions instead of Program Control could lead to a misunderstanding on the role of the Exceptions. For example, novice users could be looking for the list of trusted or blocked programs to check for a particular program's status but instead they have to explore the Exceptions tab window, (see Figure 2.9), to discover that this is the option they are looking for.

2.4 Conclusion

By examining these four personal firewalls we have gained knowledge on the core functionality of existing personal firewalls and how the interface and security information is structured. We have identified possible problems that could hinder the configuration process by novice users. Now, we can look at possible solutions in the form of information visualization.

2.5 Information Visualization Origins and Exploration of Its Techniques

2.5.1 Origins of Information Visualization

Information Visualization is formulated from several communities [3, pp 7 - 8]. The first community was data graphics, starting as early as 1786, with Playfair's work on abstract visual properties [3, pp 7 - 8]. His work involved using lines and area to display data in a visual way [3, pp 7 - 8]. The first IEEE Visualization Conference was held in 1990 and various communities participated such as the earth resource scientists that led the conference, physicists and computer scientists in supercomputing [3, pp 7 - 8]. During this period the computer graphics and artificial intelligence communities were interested in the automatic design of visual presentations of data [3, pp 7 - 8]. The user interface community followed next at the advent of a new generation of user interfaces caused by the progress made in graphics hardware [3, pp 7 - 8].

2.5.2 Information Visualization Techniques

According to a research paper titled, The Eyes Have It: A Task by Data Type Taxonomy for Information Visualization written by Ben Schneiderman [23], there are seven tasks and seven data types in visualization. The seven tasks are Overview, Zoom, Filter, Details-on-demand, Relate, History and Extract [23]. The seven data types are 1-dimensional, 2-dimensional, 3-dimensional, Temporal, Multi-dimensional, Tree, Network [23].

The information visualization technique used in our research involves the following four tasks: Overview first, Zoom and Filter, Details-on-demand and the following data type: Network [23]. These four tasks are the components of the Visual Information Seeking Mantra and the one data type: ,

- **Overview:** This is where you get an overview of the entire collection [23].
- **Zoom:** This is where you zoom on the items of interest [23].
- **Filter:** This is where you filter through the item of interests and filter out the uninteresting items [23].
- **Details-on-demand:** This is where you get details-on-demand when you select an item or group [23].
- **Network:** The data used in our research is the same as network data because its data that consists of items. However, these items cannot be suitably represented with a tree structure. Since we acknowledge the usefulness of having items linked to an arbitrary number of other items and a tree structure is not suitable to represent our research data, we have chosen Network data as our data type [23].

We will look at using network visualization to approach the problems of finding a way to represent personal firewall information in a way that can be understood and easily configured. Network visualization is the most appropriate as our problem requires looking at many-to-many data sets. This network visualization will involve the representation of the data used in our research data, which is network data. Our research data involves nodes and links. These nodes correspond to the objects and the links correspond to the

relationships between the objects [7]. Networks have two areas where one can ask interesting questions. The first area involves questions about the network structure and the second area involves questions about the statistics associated with the relationships. Node and link displays are the most common of the techniques for visualizing networks [7]. We will explore these node and link displays to solve our problem of representing our research network data in such a way that it is understandable and usable with respect to personal firewall configuration. We will explore the use of objects to represent the nodes and lines to represent the relationship between the nodes. The lines could be given colour to strengthen the relationship between the nodes. For visualizing a small sparse network that could contain tens to hundreds of nodes, node and link displays as the visualizing technique will be the most effective [7]. We believe that our research network data could be a small sparse network and therefore we will explore node and link displays in conjunction with the visual information seeking mantra to solve our research problem of building a metaphor to make the configuration of personal firewalls more usable and understandable.

Chapter 3: Methodology

3. Methodology

3.1 Introduction

The key to solving this research problem will be the building of the metaphor because the metaphor will assist the novice users in their interpretation and usage of the personal firewall (See Figure 1.1, Chapter 1). We will be using computer graphics to build the metaphor from the security information.

3.2 Metaphor Development and Experiments

The first step in developing the metaphor will be to explore existing personal firewalls and firewall security packages to discover what has previously been done with respect to personal firewall functionality, interface structure and security information structure. This will be followed by an experiment conducted with novices to discover the level of their personal firewall understanding. The results and conclusions from these two stages will allow us to determine which type of visualization is best suited for our metaphor.

Once a decision has been made on the type of visualization for our metaphor, we will build different metaphors based on these ideas. We will extract beneficial ideas from the different metaphors and construct the final metaphor. An experiment will be conducted on the final metaphor to determine whether the visualization choices made for the metaphor are effective. Once the first cycle of this experiment is complete, we will make changes to the visualization and perform a cycle of system design. After this system design cycle, the metaphor will be finalized and the final implementation of the metaphor will be completed.

After the metaphor has been completed we will conduct one final experiment to evaluate the usability of the new information visualization personal firewall. This evaluation will be used to decide whether our chosen metaphor was a viable approach to improving the usage of personal firewalls by novice users.

3.3 Experiments and Methodologies

3.3.1 Experiment 2: The study of novice user's personal firewall or computer security system knowledge

- **Aim**

  The aim of this study is to gain insight into the level of the novice users' personal firewall knowledge. We want to find out the level of novice users' understanding of the functionality and domain of personal firewall software.

- **Description Of The Study**

  This study will involve conducting Semi-Structured Interviews [13] with six novice users. The six individuals who possibly fit the criteria of a personal firewall novice user will be chosen based on a certain criteria. This criteria includes people who are novice computer users and do not have much security knowledge. They will also be selected regardless of their age, gender or race. The semi-structured approach has been selected because we would like to use a few "open-ended questions [13]" which could assist the aim of the experiment. The interviews will therefore take place in context.

  In order to deduce what the users know and do not know, our line of questioning will start out vaguely, e.g., "How often do you use the computer?" or "Are you worried about the security of your computer?", and will progress to more technical security questions, e.g., "What is a firewall?" or "What is antivirus software?" The questions will be structured in this way to observe the level of the user's firewall knowledge and to obverse where the user fails to answer the more technical security questions.

  The more technical security questions will be conducted using **conceptual model extraction** [19] (if they did not have a personal firewall installed on their computer) or **artifact walkthrough** [6] if they had a firewall installed. The conceptual model extraction will be conducted using screenshots of Panda Platinum Internet Security (8.05.01) [18], (see Figure 2.1). After performing the previous experiment, which was inspecting each chosen personal firewall package, we decided that Panda Platinum Internet Security (8.05.01) will be best suited for the line of questioning because of its control panel menu structure,

(see Figure 2.1). We can follow our approach of starting with vague questions and then progressing to more technical security questions.

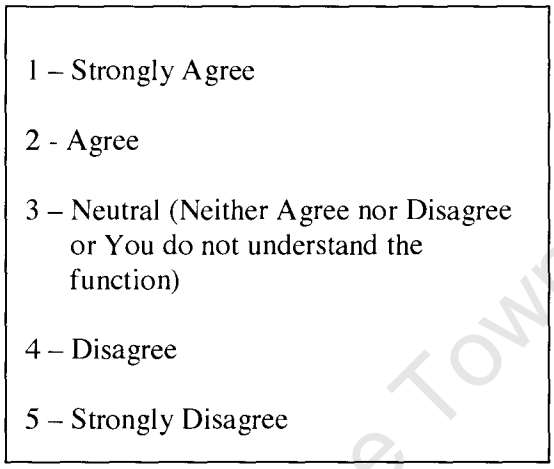

Figure 3.1 Likert Rating Scale to be used in the questionnaire for this study.

After the interview, the interviewee will be required to complete a short questionnaire. The questionnaire will be using a Likert rating scale, (see Figure 3.1), where the interviewee will be asked to rate various statements from 1 to 5.

After inspecting each personal firewall package in experiment 1, we noted that the menu structures of each package were more or less the same. There menus contain a number of main functions. However, these main functions differed across the packages and the reason for the questionnaire will be to deduce which functions the novice users perceive as main functions. These main functions will be on the "overview first [23]" interface of a personal firewall.

- **Methodology**

The methodologies for this study will be conceptual model extraction or artifact walkthrough.

Conceptual Model Extraction involves showing people an interface and obtaining their interpretations. This method will be used to observe the interviewees' understanding of personal firewall icons and interfaces.

Artifact Walkthrough is when you ask people how they will perform tasks or why they chose to perform a task in a particular way, e.g., asking the interviewee, "How did you perform a full scan of your computer?". This method will be used to observe the interviewee's usage of personal firewalls.

- **Possible Outcome or Results Of The Study**

  Possible outcomes or results of this study could be gaining information on the understanding and mental models of personal firewalls by novice users. This study will also provide some insight into how novice users use their personal firewalls. Another result will be gaining insight into how much the novice user knows, or does not know, about firewalls. Knowing what novice users know and do not know will assist by providing a starting point for the development of the new information visualization personal firewall. Information gained from interviewing and observing novice users will be used to choose the design and visualization for the new information visualization personal firewall.

3.3.2 System Design: Brainstorming and paper prototyping

- **Aim**

  The aim of this experiment is to explore an array of visualization ideas and to develop a prototype for the metaphor.

- **Description Of System Design**

  This brainstorming session will involve using the analysis and conclusions obtained from the previous two experiments. The results and information from the previous experiments will be used to explore various visualization ideas. A metaphor brainstorming session will be held with four or five interface, visualization and computing experts. This brainstorming session will involve whiteboard sketches of possible metaphors for the new personal firewall interface. These whiteboard sketches will be hand-drawn to form a paper prototype.

- **Methodology**

  The methodology that will be used in this system design session is user-centered design and the technique used is Paper Prototyping. User centered design is where the design is evaluated with the users or user data as the criteria or where the users are the source for generating design choices [12]. Paper prototyping is

a technique that can be used to brainstorm, design, create, test and communicate user interfaces [24, pp 3, pp 12].

- **Possible Outcome or Results Of System Design**

  This brainstorming session outcome will result in a prototype of the new information visualization personal firewall design. This paper prototype can be used or modified in future experiments.

3.3.3 Experiment 3: Conceptual model extraction and expert evaluation of the new information personal firewall prototype

- **Aim**

  The aim of this experiment is to refine the personal firewall metaphor by presenting the metaphor to potential users to discover whether the design decisions we chose were effective.

- **Description Of The Experiment**

  This experiment will require a high-level prototype created using Microsoft PowerPoint. This prototype will be based on the paper-prototype which resulted from the metaphor brainstorming session during system design. The prototype will be presented to approximately fifteen volunteer interviewees. They will be interviewed about this prototype. The ideal interviewees for this experiment will be people who have had some sort of exposure to firewall technology but are still novices with respect to the usage of personal firewalls, meaning they do have an understanding of the problem domain.

  The interviewees will be required to complete a short questionnaire before the interview is conducted. This questionnaire is aimed at discovering and determining how much firewall usage experience the interviewee has and whether the interviewee is familiar with personal firewall concepts such as protocol and port. The interview will follow immediately after the completion of the questionnaire.

  The interviewee will then be presented with the high-level PowerPoint prototype and informed of a few points, such as which objects are interactive or clickable. Thereafter the interview questions will commence.

The next cycle will be an expert evaluation of the high-level PowerPoint prototype. This cycle will involve displaying the high-level prototype to four or five people with interface, visualization and socially aware computing experience.

- **Methodology**

  The methodologies for this experiment are conceptual model extraction and expert evaluation. Conceptual Model Extraction involves showing people pictures and obtaining their interpretations. In our case the pictures will refer to icons and interfaces. An expert evaluation involves the assessment of the proposed application done by a HCI or usability expert [5].

- **Possible Outcome or Results Of The Study**

  The outcomes of this study will be further information on the understandability and mental models of personal firewalls by novice users. We will obtain feedback on the effectiveness of our design choices by discovering whether the interviewees recognized what each icon represented and whether they thought the icon was a fair depiction of its function. This experiment will provide us with more information on the usage of personal firewalls by novice users through observing how the interviewees respond to usage questions and explanations on how they would perform certain tasks with a personal firewall. We will receive some suggestions from the interviewees with respect to our design choices. These suggestions will be investigated to see whether it is plausible to implement in our metaphor. All the results from this experiment will assist in the refinement of our metaphor before the coding of the final personal firewall metaphor takes place.

3.3.4 Experiment 4: Task-Based evaluation of the new information visualization personal firewall

- **Aim**

  The aim of this experiment is to evaluate the new information visualization personal firewall.

- **Description Of The Study**

  This experiment will involve the interviewee, an evaluator and the new information visualization personal firewall. A number of tasks will be prepared and the interviewee will be required to perform these tasks. The evaluator will

be watching the interviewees perform the tasks but will not interfere with the interviewees whilst they are performing the tasks.

- **Methodology**

  The methodology used in this experiment is user observation and task completion. This involves setting up a number of tasks for the users/interviewees to perform. An example of a task might be, "Can you allow the SMTP port to be accessed from the MSN Messenger application?". The users will be observed while they attempt to complete the task. These observations and success or failure to complete the task will be documented and analyzed.

- **Possible Outcome or Results Of The Study**

  The combination of quantitative results (Likert rating scale results) and qualitative results (the comments of each performed task) will be an indication of how usable the new information visualization personal firewall is.

Chapter 4: Experiments, Results and Discussion

4. Experiments, Result and Discussion

4.1 Introduction

In order to build the metaphor for this research, certain formative experiments have to be completed. The results from these experiments will guide and assist the construction of the metaphor.

Each experiment discussed in this chapter consists of an aim, an explanation of how the experiment was carried out and the results gathered. After each experiment is described, a discussion on each experiment will follow.

4.2 Summary Of The Experiment Structure

The starting point for building the metaphor was to have a look at existing personal firewalls or computer security packages. Hence experiment one was a study of existing relevant software using inspection as the methodology. Experiment two was to gain a feel for the level of security knowledge of novice users. This study was in the form of a semi-structured interview [13] and the methodologies used were conceptual model extraction [19] and artifact walkthrough [6].

The results from the previous two experiments can now be used in the next step, which is the system design. This system design session brainstormed various visualization options for the metaphor. These visualization options were guided by the results of the previous two experiments. The result of the system design session was to build a prototype of the metaphor based on the visualization option chosen. The methodology used for the prototype experiment was conceptual model extraction with the interviewees and expert evaluation and the technique used was paper prototyping [24]. Expert evaluation in this experiment however makes use of HCI experts instead of end users.

The prototype from system design, (see section 3.3.2), was used in the next experiment. This experiment was to test whether the design choices and visualization chosen was plausible. The methodology used in this experiment was a combination of conceptual model extraction [19] and expert evaluation [5]. Once the prototype was

finalized, the visualization metaphor was coded in visual studio.net C# using the Piccolo Toolkit [9].

The final experiment was an evaluation of the visualization metaphor. This experiment used task-based evaluation [15] as the methodology. This experiment was used to test the usability of the visualization metaphor. The results of the final experiment will be presented and discussed in the next chapter.

4.3 Experiments and Results

4.3.1 Experiment 1: The study of existing personal firewalls or computer security systems.

- **Aim**

  The aim of this study was to gain knowledge of the functionality, interface and security information structure of current firewall and security software.

- **Experiment**

  In this study, as described in section 3.3.1, four existing personal firewalls or computer security packages were chosen to be examined - see Chapter 2 for why these packages were selected. Each of the existing personal firewalls was examined with respect to what functionality is available to the user, how the interface is structured with respect to visualization and the manner in which the security information is structured with respect to usage.

  Examining the existing personal firewalls with respect to functionality allowed us to gain insight into what functionality was available in each package and the differences in functionality between the packages. It also allowed us to gain insight into which main functions were common to all the packages. Once we have an idea of what the common main functions are, we can decide which of those functions we wish to explore in our research. The purpose of examining the interface structure is to gain insight into which visualization techniques were used and to pick up on possible visualization trends within each of the packages. Examining security information structure with respect to usage was done to gain insight on whether the information was structured in a sensible manner e.g., if a user wants to access important functions but that particular function is hidden

away in the menu structure and it has to be discovered possibly by exploration of the package.

- **Results**

Table 4.1: Panda Platinum Internet Security (version 8.05.01) Functionality	
Main Function	**Sub Function**
1. Status	**1.1** Protection Level (Low, Medium, High)
	1.2 Self-diagnosis of automatic protection
	1.3 Program Status
2. Full Scan	**2.1** On-Demand Scans
	2.2 Scheduled Scans
3. Automatic Protection	**3.1** Antivirus protection
	3.2 Firewall protection
	3.3 Anti-spyware protection
	3.4 Anti-Dialer protection
	3.5 Anti-Spam protection
	3.6 Web content filtering
4. Quarantine	**4.1** Add file
	4.2 Quarantine Help
5. Services	**5.1** Services
	5.2 Antivirus resource service

Table 4.2: Zone Alarm Pro Functionality	
Main Function	**Sub Function**
1. Overview	**1.1** Inbound Protection
	1.2 Outbound Protection
	1.3 Email Protection
	1.4 Antivirus Monitoring
2. Firewall	**2.1** Internet Zone Security
	2.2 Trusted Zone Security
	2.3 Blocked Zone Security
3. Program Control	**3.1** Program Control
	3.2 Alert Advisor
	3.3 Automatic Lock
4. Antivirus Monitoring	**4.1** Monitoring
	4.2 Status
5. E-mail Protection	**5.1** Inbound MailSafe Protection
	5.2 Outbound MailSafe Protection
6. Privacy	**6.1** Cookie Control
	6.2 Ad Blocking
	6.3 Mobile Code Control
7. ID Lock	**7.1** ID Lock: Identity Data Protection
	7.2 Status
8. Alerts & Logs	**8.1** Alert Events Shown
	8.2 Event Logging
	8.3 Program Logging

Table 4.3: Norton Internet Security 2003 Functionality	
Main Function	**Sub Function**
1. Personal Firewall	**1.1** Custom Level
	1.2 Default Level
2. Program Control	**2.1** Automatic Program Control
	2.2 Manual Program Control
3. Home Networking	**3.1** Trusted Zone
	3.2 Restricted Zone
4. Advanced	**4.1** General Rules
	4.2 Trojan Horse Rules

Table 4.4: Microsoft Windows Firewall (Service Pack 2) Functionality	
	Sub Function
1. General	**1.1** On (recommended)
	1.2 Off (not recommended)
2. Exceptions	**2.1** Add Program
	2.2 Add Port
	2.3 Edit
	2.4 Delete
3. Advanced	**3.1** Network Connection Settings
	3.2 Security Logging
	3.3 ICMP
	3.4 Default Settings

Table 4.1 – Table 4.4 display the functionality of the four existing personal firewalls or computer security packages. Table 4.5 displays the different types of visualizations found in the four existing personal firewalls or computer security packages. The different types of visualizations are categorized into four sections which are alerts (e.g., pop-up warnings), status (e.g., overview of the security activity of the computer), changing settings (e.g., how the settings options are displayed) and menu (e.g., how the menu is structured.)

According to our hypothesis that users who install personal firewall packages lack the knowledge to properly configure them, we have learnt that we should choose our feature set based on configuration – meaning our feature set would concentrate on the main functions that are involved with access. From the tables above we will have a closer look at automatic protection from Table 4.1, program control from Table 4.2, program control in Table 4.3 and exceptions in Table 4.4 as a starting point for the selection of our feature set.

Table 4.5: Different Types of Visualization	
Panda Platinum Internet Security (version 8.05.01)	
Alerts	Pop-up warnings ascending from the taskbar.
Status	Protection Level Scale (low, medium, high), Self diagnosis of automatic protection (checklist i.e. tick or! - not) and Program status checklist.
Changing Settings	Iconic Metaphor of the setting added to a bolded setting heading which has short description of the setting
Menu	Iconic Metaphors added to the menu option
ZoneAlarm Pro	
Alerts	Pop-up warnings ascending from the taskbar
Status	In and Out Internet Traffic, Programs accessing the Internet, Inbound/Outbound/Email/ Protection & antivirus monitoring
Changing Settings	Frame View of Firewall, Program Control, Antivirus Monitoring, Email Protection, Privacy, ID Lock and Alerts & Logs Settings
Menu	Side Frame Menu and Horizontal Menu

	Tabs
Norton Internet Security 2003	
Alerts	Pop-up warnings boxes pop up on the screen
Status	Security, Personal Firewall, Intrusion Detection, Norton Antivirus, Privacy Control, Ad Blocking, Spam Alert
Changing Settings	Security, Personal Firewall, Intrusion Detection, Norton Antivirus, Privacy Control, Ad Blocking, Spam Alert
Menu	Status & Settings, Alerting Level, Statistics (Log of personal firewall and Recent Online Content Blocking)
Microsoft Windows Firewall (Service Pack 2)	
Alerts	Pop-up warnings that appear on the screen, that descends from the toolbar
Status	No Status Visualization to monitor the firewalling of the computer
Changing Settings	Tab windows for different settings - general, exceptions & advanced settings
Menu	No Real Menu of important functionality

Since the research is based on configuration, we have decided that we will have to concentrate on all four categories in Table 4.5, which are Alerts, Status, Changing Settings and Menu. We will attempt to implement these four categories. These four categories need to be displayed to the user during configuration in our visualization.

- **Discussion**

The results of the study satisfy the aim of the experiment, which was to gain knowledge of the functionality, interface structure and how the security information is structured. Table 4.1 – Table 4.4 display the functionality and how the security information is structured. Table 4.5 displays certain aspects of the

interface with regards visualization. After this experiment we had an idea of what existing personal firewalls or computer security packages offer. The knowledge of what existing personal firewall offer provided us with a guideline and pointed out possible problem areas with respect to usability and understandability of personal firewall functionality and terminology.

4.3.2 Experiment 2: The study of novice users' personal firewall or computer security system knowledge

- **Aim**

  The aim of this study was to gain insight into the level of the novice users' personal firewall knowledge. We want to find out what the novice users possibly know or possibly do not know.

- **Experiment Walkthrough**

  Semi-Structured interviews [13] were conducted in this experiment. We chose six interviewees because it is similar to the three groups of four participants each, chosen in an initial user study of a game called Feeding Yoshi [1]. Since our study is also an initial user study we have randomly selected a group of potential novice users. The six individuals were selected regardless of their age, race or gender.

  The interview began with a vague line of questioning, for examples, (see section 3.3.1 Description of the study). The reason for starting with a vague line of questioning was because we did not want the interviewees to become withdrawn or unresponsive because they could not answer the more specific, technical security questions. Therefore we began with a vague line of questioning to ease the interviewees into the more specific, technical security questions.

  The more specific, technical security questions were conducted using two methodologies, which are conceptual model extraction [19] and artifact walkthrough - see section 1.4 [6]. Conceptual model extraction was used when the interviewee did not have a personal firewall installed or if the interviewee did not have a computer. Artifact walkthrough was used when the interviewee had a personal firewall installed on his or her computer.

The interview was followed by a short questionnaire. Each interviewee was required to complete the questionnaire. The questionnaire made use of a Likert rating scale, (see Figure 3.1). The aim of this questionnaire was to identify which functions could be considered as main functions on the main menu of a personal firewall. Hence the questionnaire asked the interviewee to rate from 1 – 5, 1 being strongly agree and 5 being strongly disagree (see Figure 3.1), which functions they would think should be main functions on a personal firewall's menu. This rating system gave us insight into which functions the interviewees saw as important functions. The data that we expected to receive was a number rating for each function which was converted into a percentage to provide a better view for analysis purposes. The completion of the questionnaire concluded the experiment.

- **Results**

Summarized results and user comments for the Semi-Structure Interviews, (see APPENDIX C), for the questions:

Question 1:

5 of the 6 interviewees i.e., 83.33% used their computers everyday. One of the interviewees was not asked this question because the Semi-Structured Interview Questions were modified. This question was added because we felt that the responses to this question would provide us with a more information about the interviewees' computer usage. The same reasoning goes for question 2 and 3.

Question 2:

5 of the 6 interviewees i.e., 83.33% said "yes" they use Microsoft Office. One of the interviewees was not asked this question because the Semi-Structured Interview Questions were modified.

Question 3:

5 of the 6 interviewees i.e., 83.33% said "yes" they use E-mail. One of the interviewees was not asked this question because the Semi-Structured Interview Questions were modified.

Question 4:

The interviewees used their computers for games, music, pictures, movies, studies, research, faxes and making cards.

Question 5:

5 of the 6 interviewees' computers i.e., 83.33% are connected to the Internet. 1 of the 6 interviewees' computer i.e., 16.67% was not connected to the Internet.

Question 6:

The interviewees used the Internet for studies, research, seeking information, hobbies, job search, e-mail, "surfing" the Internet and Google.

Question 7:

3 of the 6 interviewees said "yes" they are worried about security on their computers.

Comments included by these interviewees were:

- Interviewee 2: "Mainly worried about the corruption of files, by a virus for example, on the computer than the illegal access of files."
- Interviewees 3 and 6: "Worried about viruses."

3 of the 6 interviewees said "no" they are not worried about security on their computers.

Question 8:

4 of the 6 interviewees did not have any software or package/s protecting their computers. The remaining two interviewees had software or package/s protecting their computers but they were not sure which package was installed. Packages that were mentioned here were Norton, Symantec, Error guard and e-virus. The term firewall did not come up in any of the interviews. Two interviewees had never heard of the term firewall, one claims to know what a firewall is, one has heard of firewalls and one was confused about hearing the term firewall.

Summary for each interviewee for this question:

- Interviewee 1: Unfamiliar with the term firewall and what the functionality of a firewall is but thought it had something to do with protecting your computer.
- Interviewee 2: Does not seem to know exactly what a firewall is but thinks it is some sort of Internet protection. Acknowledges that just having Norton antivirus is insufficient protection for a computer.
- Interviewee 3: Has never heard of a firewall and does not know what it is.

- Interviewee 4: May have heard of the term firewall. Thinks a firewall prevents something bad from getting access to the computer.
- Interviewee 5: Claims to know what a firewall is. Thinks a firewall prevents people from accessing your computer.

Interviewee 6: Has heard of firewalls. Thinks firewalls protect your computer against viruses over the Internet.

Question 9:

3 of the 6 interviewees knew exactly what a wizard was. Two interviewees required an explanation to realize that they actually do know what an installation wizard is; they were just unfamiliar with the term "wizard". One of the interviewees reads the information displayed by an installation wizard. The others just click next or look out for the terms of acceptance checkbox before clicking next until the installation is complete.

Question 10:

Only 1 of the 6 interviewees gave a correct explanation of what the status option does. This interviewee said that the status option gives you the status of your computer with respect to security. 4 of the 6 interviewees knew what an icon was. The other two interviewees made reference to pictures when asked if they know what an icon was. These two interviewees were somewhat unfamiliar with the term icon.

Question 11:

Half said "yes" and the other half said "no" to the scale being a useful indicator for the protection level of the computer.

Question 12:

All the interviewees except one understood the functionality of the full scan option. From the five interviewees who understood the full scan functionality, two of them mentioned scanning of hard drives only and two of them mentioned scanning the whole system and one mentioned neither. Half of the interviewees agreed that all the options are necessary when the user wants to do a full scan and the other half disagreed. One of the interviewees said that the necessity of these full scan options is entirely dependent on what the user wants or prefers to use.

Question 13:

- **Automatic Protection** – All the interviewees did not know what the functionality of automatic protection is.
- **Antivirus Protection** – All the interviewees knew what the functionality of antivirus protection is.
- **Firewall Protection** – All the interviewees did not know what the functionality of firewall protection is. The interviewees knew that firewall protection had to do with the protection of the computer but did not know what or how it protects computers.
- **Anti-Spyware Protection** – All the interviewees did not know what the functionality of anti-spyware protection is.
- **Anti-Dialer Protection** – One interviewee knew what anti-dialer protection does and the other five did not know what the functionality of anti-dialer is.
- **Anti-Spam Protection** – Two interviewees knew what anti-spam protection does and the other four did not know what the functionality of anti-spam is.
- **Web Content Filtering** – Four interviewees knew what Web content filtering does and the other two did not know what the functionality of Web content filtering is. Some of the interviewees used a combination of what the words "Web Content Filtering" mean individually and the icon to deduce what the functionality of Web content filtering is.

Question 14:

One of the interviewees did not know what the functionality of quarantine is.

Question 15:

Only one of the interviewees did not trust that the firewall protects a computer properly.

Question 16:

Three interviewees believe that their machines are secure if there are no error messages or abnormal activity with respect to the security of the computer. One interviewee assumes that the computer is secure. Another interviewee believes that you will not know if the computer is secure unless something goes wrong. Interviewee no. 6 looks out for the security package icon on the taskbar to make sure that the computer is secure.

Question 17:

- Pop ups.
- Upgrades for new viruses without updating the security software.

Table 4.6, (see APPENDIX A) is a summary of the responses to the short questionnaire; see Appendix A for the questionnaire results.

- **Discussion**

This experiment assisted us to gauge the level of personal firewall knowledge by novice users. The key to this experiment was the question structure. The aim was to find out what the novice users knew and what they did not know. The aim was achieved by starting with vague questions and progressing to more technical questions. This approach assisted us to see where the novice user was able or unable to answer questions and thus gave us an indication of the level of their personal firewall knowledge. These results are important for the design of the metaphor because being able to gauge the level of knowledge of the target users will assist in the selection of the visualization for the metaphor. The questionnaire was aimed at discovering which functions the target users would choose as main functions. These are the functions that would be displayed on the "overview first [23]" interface of a personal firewall. The results from the questionnaire show that all but one of the functions was selected as main functions (see Table 4.6, APPENDIX A). This result could prove that most of the functions are important or that the interviewees did not understand the functions so they chose most of them as main functions.

4.3.3 System Design: Brainstorming and Paper Prototyping

- **Aim**

The aim of this system design session was to explore a range of visualization ideas and to develop, using one of these ideas, a prototype for the metaphor.

- **Experiment Walkthrough**

The results and information from the previous two experiments were summarized, analyzed and prepared for use in this system design session. The metaphor brainstorming session was held with the five interface, visualization and computing experts. During this session we managed to identify the key

problems the interface needs to address as well as the key set of functionality the interface should allow users to configure. Since our research is concentrated on configuration of personal firewalls and visualization, the key problems the interface needs to address are as follows:

- How to visually represent the applications and ports?
- How to visually represent the highly technical port names?
- How to represent the connection between the applications and ports?
- How to represent the configuration functionality - allow, deny or prompt?
- How to visually represent an actual configuration of an application or port?

The key set of functionality the interface should allow the user to configure is as follows:

- To view the access status of any application or port.
- To change allow, deny or prompt mode of any application or port.

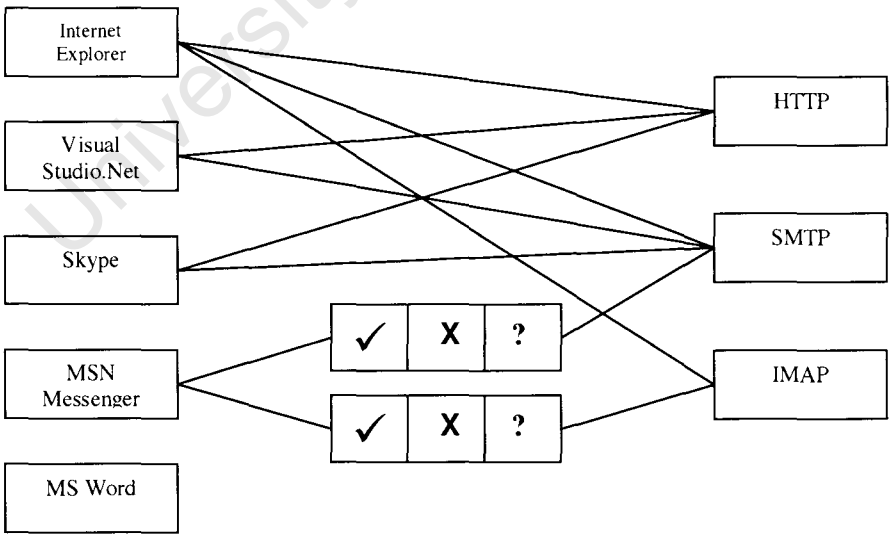

Figure 4.1 The first suggested visualization for the metaphor.

Based on these key interface problems and key set of interface functionality, a suggestion for the metaphor was made, (see Figure 4.1).

In Figure 4.1, the suggested visualization for the metaphor contains boxes on the left, which is to represent the applications and boxes on the right, which represent the ports open on the computer. The lines signify the connections between the applications and the ports or vice versa. The tick, cross and question marks boxes are buttons that can be used to control the access status of the connection between the application and port. The tick signifies allowing an application or port, the cross signifies denying an application or port and the question mark signifies prompt mode, which is where the user is asked whether to allow or deny an application or port.

After this visualization was suggested for the metaphor, in Figure 4.1, follow-up suggestions and discussions were held by the experts. A process of iteration produced a list of possible changes and suggestions to improve this visualization.

- **Results**

The result for this experiment is the suggested changes for the visualization gathered during the brainstorming session with the experts. These changes are discussed in the next subsection.

- **Discussion**

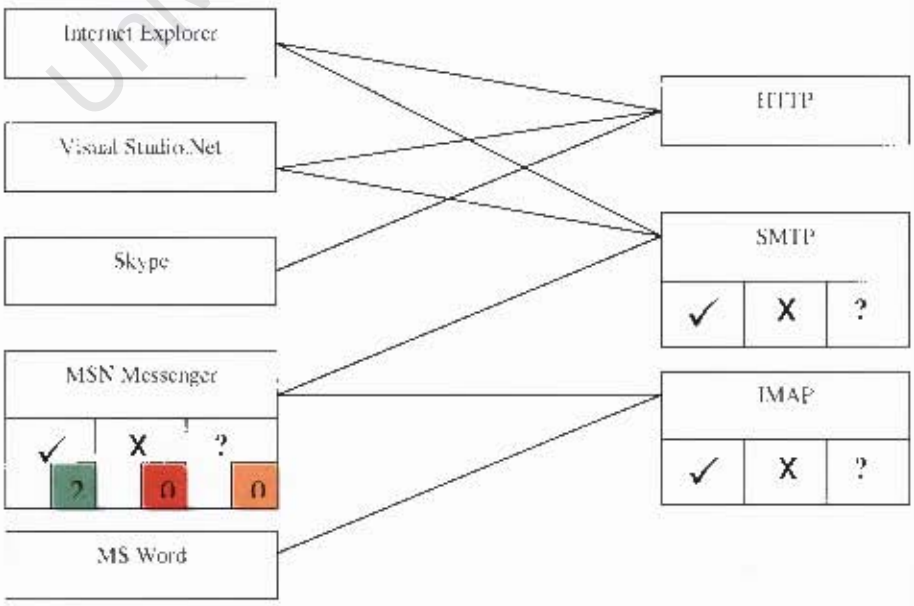

Figure 4.2 Agreed visualization choice for the metaphor.

The experts agreed that this is a satisfactory choice for the visualization of the metaphor. They did however suggest a few changes and posed a few new ideas. The first change that was suggested was to move the tick, cross and question mark buttons from in between the lines connecting the application and port, (see Figure 4.1), to below each application or port, (see Figure 4.2). This is a valid change because the buttons may signify a break in connection between the application and port.

The second suggested change was to possibly use colour for the tick, cross and question mark buttons. Suggested colours were: the tick button to be green to signify allow; the cross button to be red to signify deny and orange to signify prompt mode. The expert users then posed a new idea. If possible, when an application or a port is selected the rest will grey out to signify deselection and could possibly go smaller or zoom out to give the effect that the deselected applications and ports move to the back when another application or port is selected. The next new idea was to make the line width increase or decrease. By doing this it will allow us to see the amount of traffic being generated between an application and port e.g., if the width of the line was extremely thick then it could signify that there is a problem or an attack on that connection. The next idea was the bracketed number next to each application or port label to signify how many connections that application or port had. The final suggestion was to give the user the option of allowing, denying or prompting all the applications or ports at once and allowing, denying or prompting applications or ports one by one. This was solved by the suggestion of adding smaller number labeled buttons on top of the bigger tick, cross and question mark buttons, (see figure 4.2). These smaller number labeled buttons would give the user the option of singling out which applications or ports are in allow, deny or prompt mode and then allowing, denying or prompting these applications or ports one by one. The bigger tick, cross and question mark buttons were then used to allow, deny or prompt all the applications or ports.

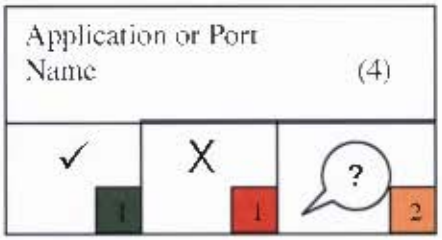

Figure 4.3 An example node including controls. The tick, cross and prompt button, are used to represent an application or port in the new information visualization personal firewall.

Figure 4.3, represents the structure of a node and its control buttons. In Figure 4.3, the application, or port node, consists of two parts. These two parts are the top box and the bottom panel of buttons. The bottom panel of buttons consists of three big buttons and three smaller buttons labeled with a number.

The top box consists of a label, which is a name of either an application or port, and a bracketed number e.g., (4). This bracketed number has two meanings depending on whether the top box is an application or a port. If the node is an application, meaning that the top box is labeled as an application name, then the bracketed number signifies the number of ports the application has access to. If the node is a port, meaning that the top box is labeled as a port name, then the bracketed number signifies the number of applications that are accessing that port.

The bottom panel consists of six buttons, three big buttons and three smaller number labeled buttons. These buttons are the controls for the application or port it is attached to. The tick button allows access to all the applications or ports connected to that application or port node. When clicked the tick button changes colour from white to green. The X button denies access to all the applications or ports connected to that application or port node. When clicked the X button changes colour from white to red. The speech bubble question mark button places an application or port node in prompt mode. When clicked the speech bubble button changes colour from white to orange. Prompt mode is

when the computer prompts the user to ask whether they will allow or deny access to an application or port.

The three smaller buttons with number labels allow the user to view which application/s or port/s are either in allowed, denied or prompt mode. This button will also allow the user to first display the access status and then change the access status of that specific application or port by clicking on the tick, X or speech bubble question mark button of the corresponding application or port. If one of these smaller buttons was clicked from an application node then the three big tick, cross and prompt buttons of the corresponding port node/s will appear. The user can then change the access status of the corresponding port node/s by clicking on one of the three big tick, cross or prompt buttons and vice versa, if one of these smaller buttons was clicked from a port node. These suggestions were noted as ideas and suggestions for the prototype and final implementation of the new information visualization personal firewall.

4.3.4 Experiment 3: Conceptual model extraction and expert evaluation of the new information personal firewall prototype

- **Aim**

The aim of this experiment was to refine the personal firewall metaphor by presenting the metaphor to people to discover whether the chosen design decisions were effective.

- **Experiment Walkthrough**

The experiment consists of two sections. The first section is a questionnaire and the other section is conceptual model extraction using the Microsoft PowerPoint prototype. Fifteen people were recruited for the experiment. The majority of the interviewees were third year computer science students. The third year students were chosen because they had been briefly exposed to firewall technology as part of their course. We understand that these users are not representative of the target user group; they were chosen as we were specifically interested in evaluating how well the interface represented the underlying firewall concepts. If we had used subjects from the target user group at this point we would not know if any confusion arose from a poorly constructed interface or a conceptual misunderstanding. By using the third year students, at the end of this cycle we

will have removed the interface problems so that, when we test with the novice users, any problems reported will be with the metaphor's concept rather than its rendition.

The questionnaire was set up to check whether the third year students do have an understanding of firewall technology or not. The questions were set up in such a way that from the responses one could determine: whether or not the interviewee has used a firewall before; has a firewall installed on their computers; how often they use a firewall; whether they understand some terminology such as protocol and port, and whether or not they understand the concept of a firewall.

- **Results**

1. Summary of the questionnaire responses by the interviewees:

Question 1: Have you used a firewall before?

8 of the 15 interviewees claim to have used a firewall before. The remaining 7 interviewees have not used a firewall.

Question 2: Do you have a firewall installed on your computer?

7 of the interviewees have a firewall installed - the remaining 8 have no firewall installed.

Question 3: How often do you use your firewall?

7 of the interviewees use their firewalls: 1 always, 1 almost always and 5 rarely/not too often. 3 interviewees responded with N/A and 4 interviewees do not use their firewalls.

Question 4: Do you know what a protocol is? If Yes, Specify.

(**Definition of protocol:** A protocol is a set of technical rules about how information should be transmitted and received using computers.)

Only 1 interviewee said "no". 14 interviewees said "yes" and 10 of the interviewees definitions of protocol were more or less the same as the above definition. 4 of the definitions were incorrect.

Question 5: Do you know what a port is? If Yes, Specify.

13 interviewees said "yes" but the majority of them, based on their definition of a port, does not know or have a poor idea of what a port is. 2 thought that is a physical port on a computer. 2 said "no" and didn't know at all.

Question 6: Do you understand the concept of a firewall? If Yes, Specify.

3 interviewees said "no" and 12 said "yes" - these explanations were more or less correct. Most of them understood that a firewall "protects", "prevents", "blocks" or "restricts" access.

2. Summary of the responses by the interviewees to the questions of the conceptual model extraction:

Question 1: What do you think the boxes on the left represent?

6 of the interviewees recognized the boxes as applications. 2 interviewees said that they were browsers, 4 interviewees didn't have a clue, 1 interviewee said "Tools that a user will be logged onto....", 1 interviewee said "different software" and 1 interviewee said "different Internet programs."

Question 2: What do you think the boxes on the right represent?

7 of the interviewees recognized the boxes as protocols. 4 interviewees said that the boxes were servers and 4 interviewees didn't have a clue.

Question 3: What do you think the bracketed number in each box e.g., (6) represents?

4 of the interviewees understood and recognized that the number indicates the number of connections from that application or protocol. 11 interviewee's did not pick up that the number in the box is related to the number of lines and hence the number of connections from that application or protocol. A few interviewees only recognized the relation between the number and the lines after being asked if they think there is a connection between the number and the lines. Responses from the 11 interviewees who thought the number meant something else other than the number of lines or connections include:

- Level of complexity.
- Size.
- How many applications you can open e.g., (4) in the Internet Explorer box means you have 4 Internet Explorer browsers open.
- Category they could be placed into.
- Number of attacks on that application or protocol.
- Number represents strength.
- The number of options for each application or protocol.
- Applications of the same kind have the same number.

Question 4: What do you think the lines represent?

Only 1 interviewee had no idea what the lines represented. The rest of the interviewees understood the purpose of using the lines.

Question 5: If you wanted to select any of the boxes, how would you go about doing it?

All the interviewees said that they would click or right click. The majority of the interviewees thought I was asking them some complex question. They did not realize the simplicity of the question and that made them hesitate.

Question 6: What do you think would happen if you clicked any box, left or right?

6 of the interviewees were able to correctly predict what was going to happen when you click on any of the boxes. Other interviewees expected things like:

- Pop ups.
- Documentation.
- Background on the boxes.
- List of browsers when clicking Internet Explorer.

Question 7: What do you think  **represents?**

9 of the 15 interviewees said that the icon represents the Internet. One interesting response was it represents a web browser emailing.

Question 8: What do you think  **represents?**

13 of the 15 interviewees said that the icon represents e-mail.

Question 9: What do you think the tick represents?

10 of the 15 interviewees identified the tick as "allows or accepts or activates or enables access." One interviewee matched the colour green to the tick. 2 interviewees only recognized what the tick was for after being told that they were controls, in other words buttons.

Question 10: What do you think the cross represents?

12 of the 15 interviewees identified the cross as "doesn't allow or doesn't protect or reject or deactivate or disable access."

Question 11: What do you think the question mark represents?

Only one interviewee identified that the question mark represents the user prompt feature which is to prompt the user to specify allow or deny. Most of the interviewees thought it represented a help function.

Question 12: How would you allow, deny or ask any application/protocol?

11 of the 15 interviewees knew how to allow or deny or both. A few of the 11 interviewee's also said that when clicking the X to deny it will change to red, clicking the tick will change the colour to green. Most of them did not mention what would happen if you clicked the question mark.

- **Discussion**

The main results from the questionnaire were that 12 of the 15 interviewee's i.e., 80%, understood that a firewall "protects", "prevents", "blocks" or "restricts" access and 10 of the 15 interviewee's understood more or less what a protocol is.

What could have affected this questionnaire was the fact that there is a difference between firewall and personal firewall. The questionnaire used the word firewall which could have been misinterpreted as the hardware firewall therefore the interviewees could have been answering the questions thinking that the firewall referred to is a hardware firewall and not a personal firewall. This could have had an effect on the results of the questionnaire. An interesting finding of the questionnaire was that two of the interviewees thought that the port was a physical port of the computer.

The main result from the conceptual model extraction was that the boxes, lines, icons, tick and cross were recognized relatively well. The @ sign and the arrow from the @ sign to the computer sign, (see question 7 Table 4.9), of the http icon caused some confusion because it might have signified emailing as well. The box questions, (questions 1 and 2, Table 4.9), were difficult to ask because most of the interviewees did not understand what type of answer was expected of them. The questions for the boxes could have been rephrased to make the interviewee understand what type of response is expected of them. The question mark icon was totally misinterpreted. Most of the interviewees thought it was a help function and not a "prompt the user" function. This clearly exposed the fact that most of the interviewees did not know what prompt mode was.

Possible changes for the visualization are: the removal of the @ sign and arrow from the Internet icon, to clear up any confusion that the http icon may signify email; changing the question mark to another representation of prompt mode; and when a connection between an application and port is in deny status, change the line to a dotted red line to signify the break in connection. These are a few changes that will be made before final implementation.

Chapter 5: Evaluation of the new information personal firewall visualization

5. Evaluation of the new information personal firewall visualization

5.1 Introduction

Since the metaphor was selected, it has been refined with a combination of conceptual model extraction [19] and expert evaluation [5] and then developed in Visual studio.Net C# using the Piccolo toolkit [9]. Piccolo is a 2D toolkit that allows you to create programs that require 2D structured graphics, particularly Zoomable User Interfaces (ZUIs) [9]. What is a ZUI? A ZUI is a new kind of interface that allows the use of a canvas to present information on a computer screen [9]. This is done by allowing the user to zoom in and focus on more detailed information, and allowing the user to zoom out thereby giving the user an overview of the information. Piccolo is built on a lower level graphics API and is available in three versions which are Piccolo.Java, Piccolo.Net and PocketPiccolo.Net [9]. The version used in this research was Piccolo.Net. The next step would be to test whether the design choices and ideas that were chosen and programmed for the metaphor were indeed implementable. We will use task-based evaluation to evaluate the usability of the implemented metaphor, (see methodologies section 1.4.1).

Task-Based Evaluation involves the performance measurement of typical users on tasks that have been carefully prepared and based on tasks that would be typical to the system being designed [15].

5.2 Screenshots of the visualization and how it works

The screenshots shown in the figures below are of the new information visualization personal firewall. The first screenshot displays the overview, which includes the application nodes on the left, the port nodes on the right and the lines which signify which applications are connected to which ports and vice versa. Three of the port node functionalities are signified by their respective iconic representations.

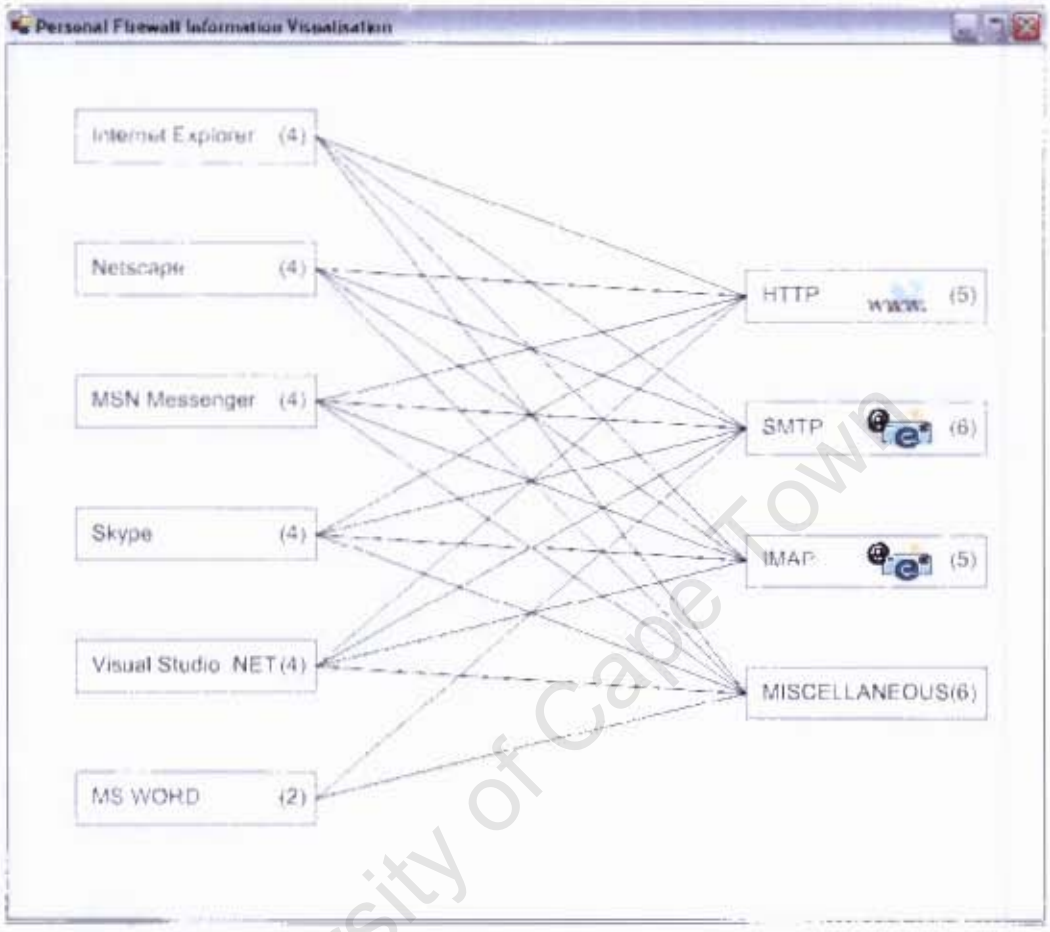

Figure 5.1 Screenshot 1: Overview First

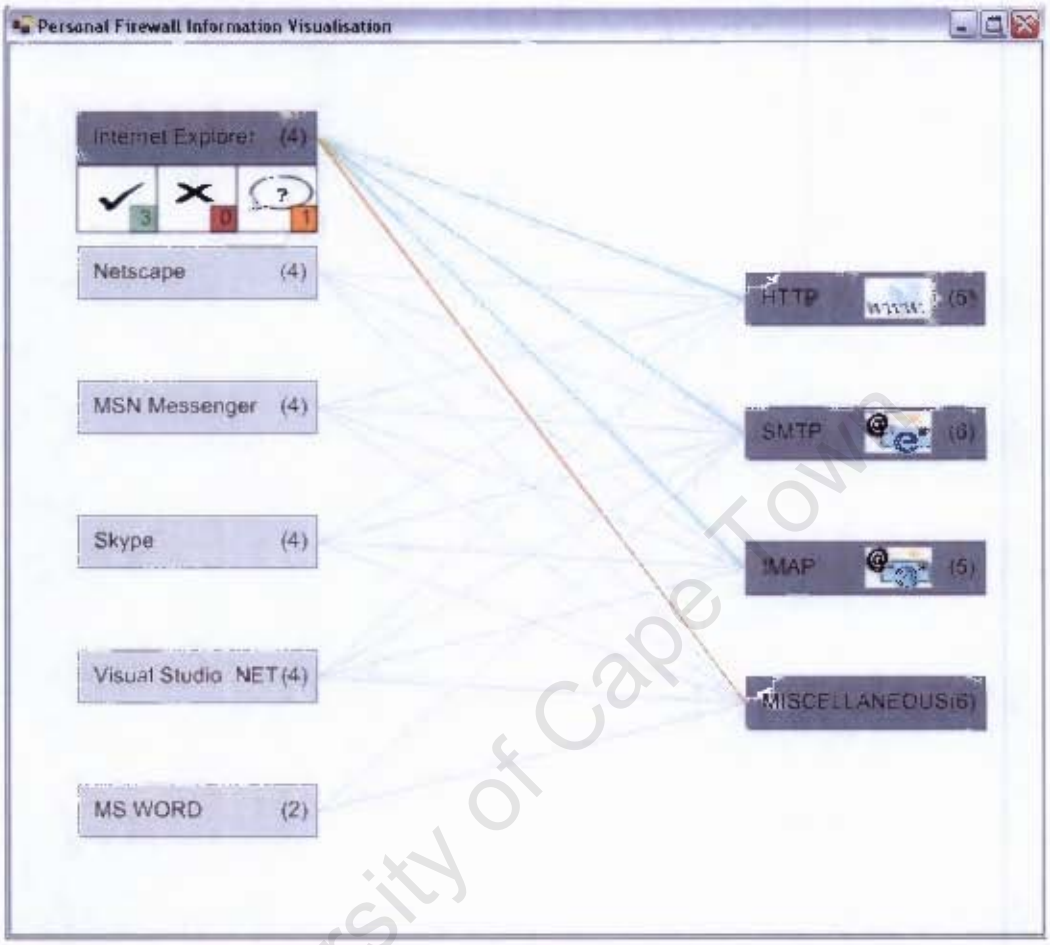

Figure 5.2 Screenshot 2: Selecting the Internet Explorer node by clicking the node itself.

The second screenshot displays what would happen if the Internet Explorer application node were selected, (see Figure 5.2). When the Internet Explorer node is clicked, the controls or bottom panel of buttons appears below the Internet Explorer node, the port nodes as well as the Internet Explorer node changes from white to dark grey to signify that it and its connecting port nodes have been selected and the lines connecting the nodes change colour to signify the status of the connection between the Internet Explorer node and its port nodes. A line colour of green, red or orange respectively means that the connection is in access, deny or prompt mode. The rest of the nodes that have no connection to the Internet Explorer node fade to light grey.

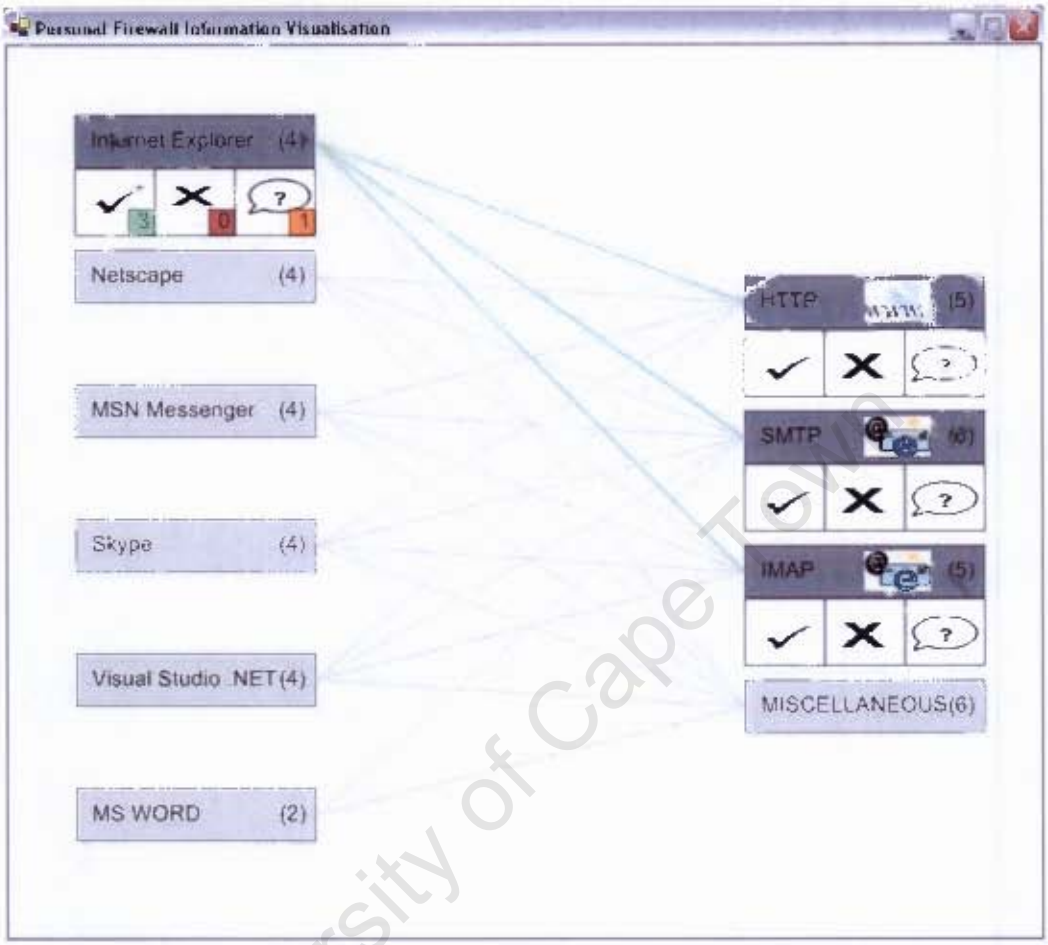

Figure 5.3 Screenshot 3: Displaying the port nodes that have an access status for the Internet Explorer application.

The third screenshot displays what would happen if the smaller green button with the number 3 label were clicked. When this smaller button is clicked, it displays the three port nodes that are allowed access from the Internet Explorer application. The controls for each port node appears at the bottom of each port node and the miscellaneous port node fades to light grey – meaning that it does not have allow access from Internet Explorer. The miscellaneous port node does however have a prompt access status which is signified by the number "1" label in the smaller orange button on the controls of the Internet Explorer application node, (see Figure 5.3).

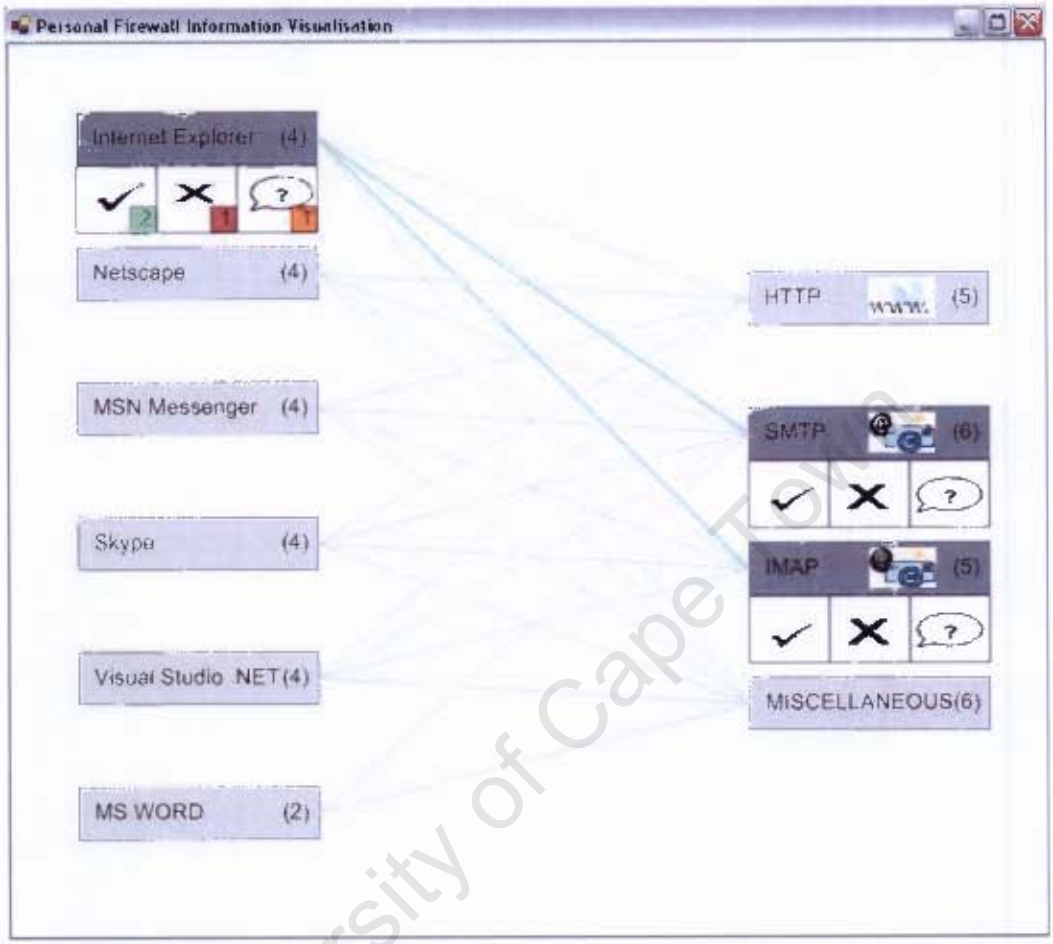

Figure 5.4 Screenshot 4: Changing the status of the HTTP port node to deny by clicking on the big X of the HTTP port node.

The fourth screenshot displays what would happen if the HTTP port was denied access by clicking on the X button of the controls for HTTP, (see Figure 5.3). Once this X button is clicked the HTTP port and line changes to light grey, signifying that the status has changed. In Figure 5.4, the small green button's number changes to 2 and the small red button changes from 0 to 1 - this signifies the change in status of the HTTP port connection with Internet Explorer from allow to deny.

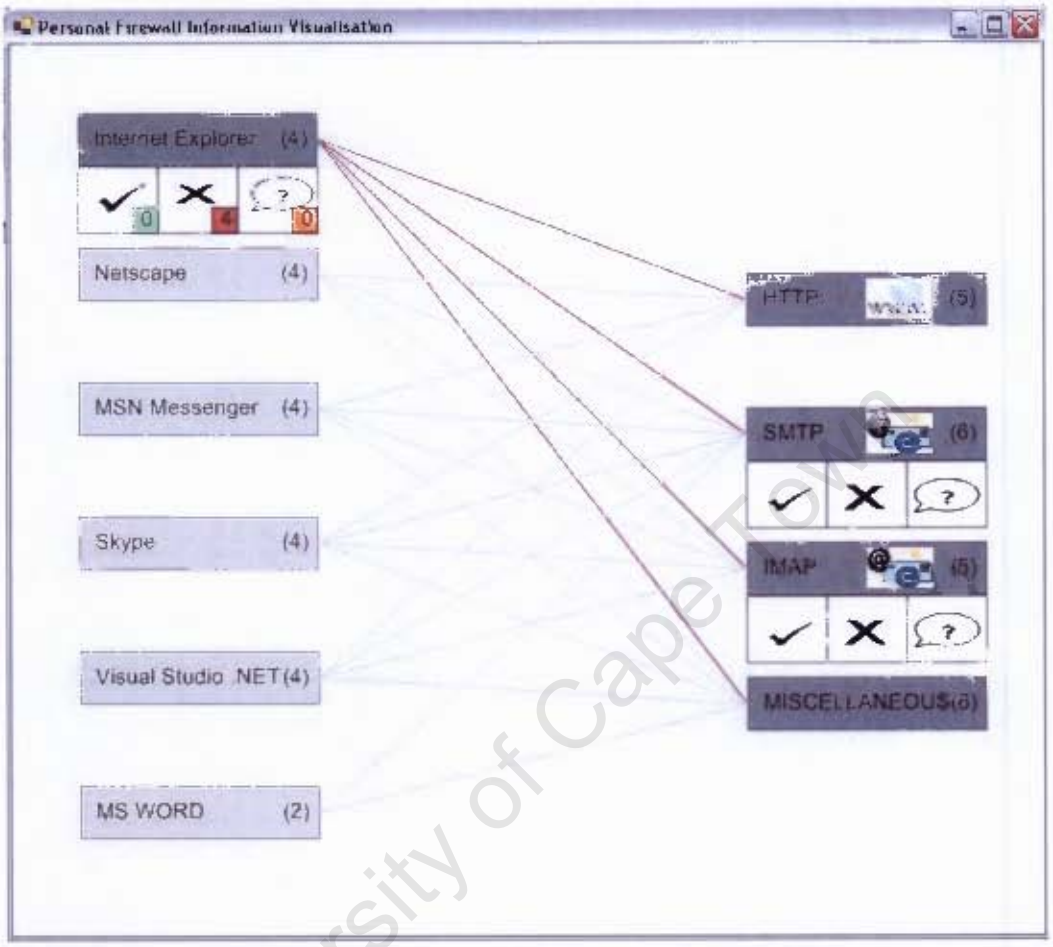

Figure 5.5 Screenshot 5: Change all port nodes' access to deny status by clicking on the big X of the Internet Explorer node.

The fifth screenshot displays how one can deny all ports at the same time, (see Figure 5.5). This is done by clicking the X button of the Internet Explorer application node. Once this is done, the small green button changes to 0, the small orange button changes to 0 and the small red button changes to 4 which signifies that all ports are blocked from the Internet Explorer application node.

Can you deny Internet explorer's access to HTTP port? One starts at the "overview [23]", in Figure 5.1, then "zooming and filtering [23]" in on Internet Explorer's port connections by clicking on the Internet Explorer application node. This will show Internet explorer's port connections and their status, which is the "details-on-demand [23]", (See Figure 5.2). To change the HTTP port connection status from allow to deny, one has to click on the small green button, which then shows the three port's in

allow status and displays each ports control buttons, (see Figure 5.3). Clicking the X button of the HTTP port node will change the status to deny and the line will change colour to light grey to signify that the change has been made. Another way to see that the change has been made is to check the numbers on the small colour buttons, (see Figure 5.4). The numbers change from 3 allow, 0 deny and 1 prompt to 2 allow, 1 deny and 1 prompt, see Internet explorer application node in figure 5.4. Once this has been done the task is successfully completed.

5.3 Experiment 4: Task-Based evaluation of the new information personal firewall visualization

- **Aim**

  The aim of this experiment was to evaluate the new information visualization personal firewall.

- **Experiment Walkthrough**

  This experiment involved twenty voluntary subjects. Of this twenty, four were female and the rest male. The age interval ranges from 14 to 55 years, with the average age of 25 years. The experiment consisted of twelve questions that were reiterated from the cyclic conceptual model extraction experiment, (see Section 4.3.4, Results: Responses to the conceptual model extraction questions), and the twelve tasks, (see APPENDIX B).

  The structure of these interviews was as follows:

  - Communication of the instructions.
  - Reiteration of the twelve cyclic conceptual model extraction questions about the new personal firewall and its elements.
  - Commencement and completion of the Task-Based evaluation tasks.

  The first step of this experiment was to provide the interviewee with instructions for the interview. These include instructions on the structure of the interview and a short explanation of certain aspects about the new information visualization personal firewall e.g., which elements of the new information visualization personal firewall were clickable and which elements were not clickable. The aim for providing the interviewee with instructions for the interview structure was to

give an idea of what is to be expected throughout the interview. The aim of providing a short explanation of certain aspects of the new information visualization personal firewall was to avoid spending time on explaining, for example, the click abilities of each element.

The next step was to reiterate questions from experiment 3, which was conceptual model extraction, about the new personal firewall. This is done to check whether the interviewees are familiar with the elements and icons of the new information visualization personal firewall. If the interviewees were not familiar with the elements and icons, an explanation was provided where required. The reiteration was followed by the task-based questions. This is where the interviewee was asked to perform a task. The path of the interviewee's clicks for each task was recorded on paper. The task-based evaluation was completed once the success or failure of an interviewee's tasks was noted.

For a task to be successfully completed, the interviewee had to satisfy the following requirements for each task:

Task 1:

How many ports (e.g., HTTP, SMTP) are connected to the application Explorer?

This task did not require any clicking or exploration. It can have been answered by observing the bracketed numbered of the Internet Explorer application box that indicates that Internet Explorer is connected to four ports.

Task 2:

How many of the ports connected to Internet Explorer are: Allowed? Denied? Prompt?

Similar to task 1, it can be answered by observing the number on the button of the tick, cross or prompt button. The answer was, the number of allowed ports is 3, the number of denied ports is 0 and the number of prompt ports is 1, the sum of which is equal to the 4 ports connected to Internet Explorer. This is indicated by the bracketed number.

Task 3:

Can you allow the SMTP port to be accessed from MSN Messenger application?

This task required the interviewee to click on the SMTP port node or the MSN Messenger application node. This would have allowed the interviewee to make the desired change to satisfy the task requirements. This task can be done in two ways. Firstly, the allowable access, where access status is allowed, denied or prompt, could have been changed from the port side and, secondly, the allowable access could have been changed from the application side.

One the port side, the user clicks the SMTP port node, which activates the bottom panel, (see Figure 4.3). Once the bottom panel is visible, the user should observe the access status of each big tick, cross and prompt button, which is indicated by the number on the smaller button attached to the bigger tick, cross or prompt button, (see Figure 4.3). Clicking these smaller buttons, which are attached to the bigger coloured buttons, will display the access status for the applications connected to the SMTP port. The user has to observe the colour of the line connecting SMTP and MSN Messenger. This line colour will determine which small number labeled button the user will click to change the access status between SMTP and MSN Messenger.

On the application side, the user clicks the MSN Messenger application node, which activates the bottom panel, (see Figure 4.3). The same procedure, as explained above, may be followed on the application side as well.

Task 4:

Can you show me which ports have allowed access to the application Internet Explorer?

This task required the interviewee to click on the Internet Explorer application node, to show which ports the application has access to. The task can be done in two ways. Firstly, by clicking on Internet Explorer application node, thus activating the bottom panel of buttons, (see Figure 4.3). To display which ports have allow status the user has to click on the small number labeled button attached to the big green tick button. This will only display the ports that have an allow status with the application Internet Explorer. The other way the user could have

completed the task was to perform the same clicks as above but the clicks would have to be performed for every port node, which would display the allow ports to Internet Explorer one by one.

Task 5:

Can you show me which applications are denied access to the HTTP port?

The task required the user to click on the HTTP port node, to show which applications are denied HTTP port access.

The task can be done in two ways. These two ways are similar to those described in task 4 but the difference is that this task involves the HTTP port and the denied status not the allow status needs to be shown.

Task 6:

Can you show me which applications have prompt access to the IMAP port?

The task can be done in two ways. These two ways are also similar to those described in task 4 but the difference is that this task involves the IMAP port and the prompt status not the allow status needs to be shown.

Task 7:

Can you deny Internet Explorer's access to the SMTP port?

The task can be completed in two ways. Firstly, the denied access can be done from the application side or, secondly, on the port side.

On the application side, the top box of the Internet Explorer application node needs to be clicked to activate the bottom panel of six buttons, (see Figure 4.3). The user will have to observe the colour of the line connecting the Internet Explorer application to the SMTP port. The colour of the line will determine which smaller number labeled button to click. If the line is green or orange, then the smaller number labeled button attached to the big tick allow button or the big orange prompt button must be clicked. This will show the access status of Internet Explorer to the SMTP port and it can then be changed by clicking on the big X button on the SMTP port.

On the port side, the process is the same, which is clicking the top box of SMTP port node and vice versa for the rest of the process.

Task 8:

Can you allow Visual Studio.Net access to the HTTP port?

The task can be completed in two ways. These two ways are similar to those described in task 7 but the difference is that the task requires the user to allow access and it involves Visual.Studio.Net and HTTP port, not Internet Explorer and SMTP.

Task 9:

Can you set MS Words' access to SMTP to prompt access?

The task can be completed in two ways. These two ways are similar to those described in task 7 but the difference is that the task requires the user to change the access to prompt mode and it involves MS Word and SMTP port, not Internet Explorer and SMTP.

Task 10:

Can you allow Skype to access all ports?

The task can be done in two ways. Firstly, allowing Skype to have allowed access to all ports can be done with one click of the green tick button or, secondly, Skype can be allowed access to all ports by changing the access status of each port connected to Skype, one by one, to allow.

Task 11:

Can you deny HTTP to all its applications?

The task can be done in two ways. These two ways are similar to those described in task 10 but the difference is the task requires the user to deny HTTP To all applications, not to allow Skype to all ports.

Task 12:

Can you set all the MISCELLANEOUS port connections to prompt access?

The task can be done in two ways. These two ways are similar to those described in task 10 but the difference is the task requires the user to change the access of the MISCELLANEOUS port to prompt mode, not to allow Skype to all ports.

- **Results**

The results of the repeat of the cyclic conceptual model questions represented for each question in Appendix B and the results for tasks completed by the interviewee is summarized below.

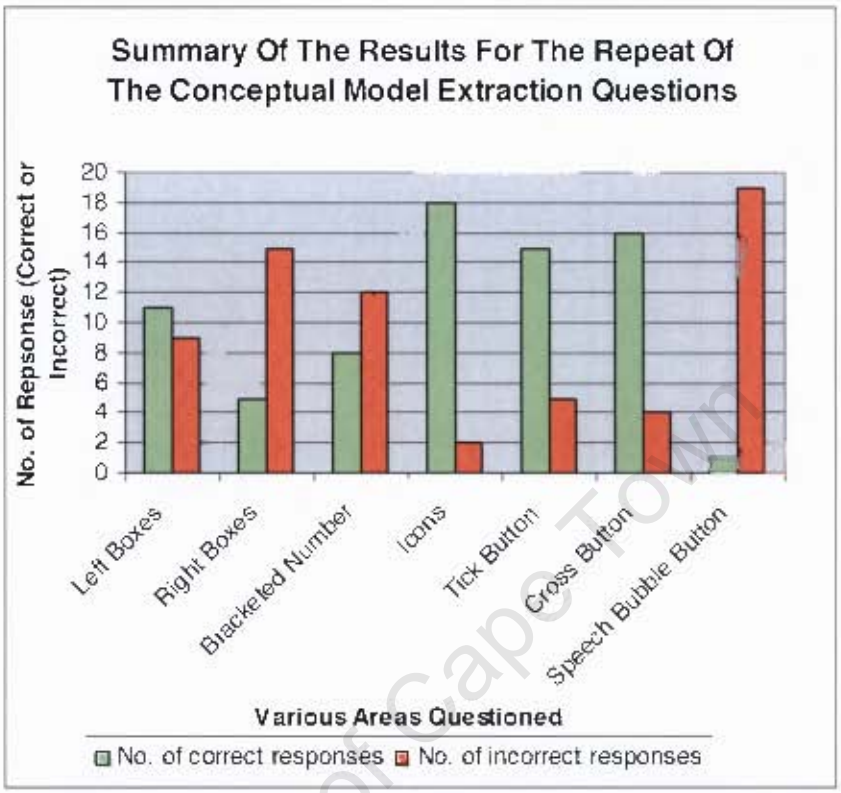

Figure 5.6 Summary of the results for the repeat of the cyclic conceptual model extraction questions. The various areas of questioning are derived from questions in Appendix B. e.g., Icons represents questions 5, 6 and 7 from Appendix B.

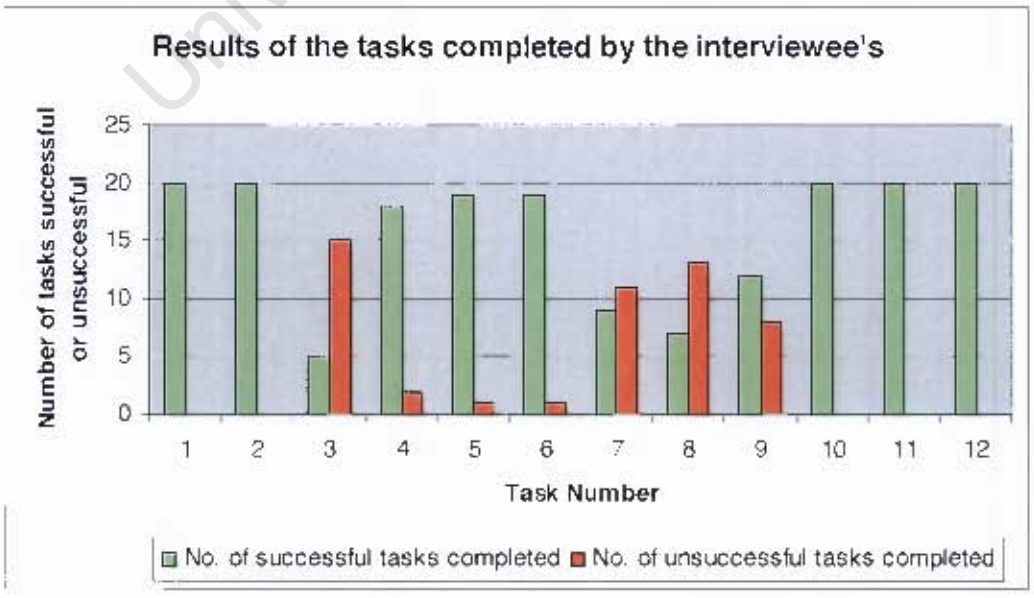

Figure 5.7 Summary of the successful or unsuccessful results of the task based evaluation experiment.

- **Discussion of the experiment, results, methodology and interesting findings**

1. **Discussion of the reiteration of the conceptual model extraction questions and its results**

   Reiterating the conceptual model extraction questions was a success because it provided us with valuable information with respect to what the interviewees were or were not familiar with. Areas of concern were the responses to the left and right boxes, bracketed number and speech bubble button questions, (see Figure 5.6). Nine interviewees did not know, or were unsure of, what the left boxes represented and an explanation had to be provided to those interviewees. Applications or Programs were the two common responses given by those interviewees who were correct. 75%, which is 15 interviewees, did not know what the right boxes represented. All of them had to be provided with an explanation of what a port is. A basic analogy of a brick wall was used to explain what a port and its functionality is.

   The basic brick wall analogy was explained as follows:

   - The interviewees were asked to visualize a brick wall as the protection of their computer. The brick wall is their personal firewall, protecting everything on their computers from everything on the other side of the brick wall.
   - The interviewees were then asked this question, "What would you need to do to the brick wall to allow access to your computer from the other side of the wall?"
   - Most of the interviewees did not respond - then an explanation was given to them. They were told that a brick would need to be knocked out of the wall to create a hole with the functionality of allowing or denying access to the computer. We explained that the hole in the brick wall represents the port and the functionality of a hole is similar to the functionality of a port.

   It would seem that the majority of the interviewees now had some understanding of what a port and what the functionality of a port is. The few interviewees who thought they knew referred to the port as protocols.

In Figure 5.6, 12 of the interviewee's, i.e., 60%, did not know what the bracketed number represents, (see Figure 4.3). What was interesting was that all twelve interviewees only saw that the bracketed number signifying the number of connections between an application and a port or vice versa when they were asked "Do you think there is a link between the lines and the number?" Once this question was asked they recognized the link between the bracketed number and the number of connections to an application or port.

In Figure 5.6, the chart shows that 95% of the interviewees did not know what the speech bubble button represented. About 6 of this 19 thought that the functionality of this button was for help because of the question mark. One interviewee even said that he was expecting a mouse roll over to assist him in answering these questions. The speech bubble button is to be used as prompt mode. Explanations of prompt mode was provided and in some cases this example was used: when you try to access a webpage, it requires ActiveX and when you select install ActiveX your personal firewall will prompt you with a pop-up box to ask the user to decide to allow or deny the installation of ActiveX. The result for this question is a clear indication that the selection of a speech bubble with a question mark as a visual representation of the functionality was insufficient.

2. Discussion on the methodology with regards to the structure and significance of each task

The next step of this evaluation experiment was, of course, the task based evaluation. The task-based evaluation consisted of twelve tasks, (see Appendix B).

The first two tasks required very little clicking or exploration - observation was key to successfully completing these tasks. These two tasks were aimed at easing the interviewee into the task-based evaluation. The aim of the first task was to accomplish an understanding by the interviewees that the applications are connected to a number of ports and vice versa. The aim of the second task was to get the interviewees to acknowledge and understand the significance of the colour of the lines and more importantly the number on each small button

which was connected to a tick, X or prompt meaning allow, deny and either allow or deny respectively, (see Figure 4.3). This could have been accomplished by either observing the number of green, red or orange lines or by observing the number on the small button and relating it to the tick, cross or prompt icons or clicking the number labeled button to see the number of connections. The third task was asked at this stage because we wanted to see if the interviewees could perform the main task, which was to change an application or port's access status.

The aim of the next three tasks was to accomplish an understanding by the interviewees that if you click the small button on either the tick, X or prompt button it would display the allowed, denied or prompt applications or ports as well as the bottom panel of buttons, (see Figure 4.3), of the corresponding application or port node. This bottom panel of buttons of the corresponding application or port should be an indication that the access statuses can be changed by clicking one of the buttons of the bottom panel of the corresponding application or port. Acknowledgment of the bottom panel of buttons of the corresponding application or port would lead the interviewee into the next three tasks.

The next three tasks were aimed at observing whether the interviewees could change an application or port's access status. These three tasks were the main tasks of this task-based evaluation because the results of this ties into whether or not the design and visualization choices for the metaphor were plausible. The last three tasks were aimed at getting the interviewees to discover the functionality of the big tick, X and prompt buttons.

3. Discussion on the results and interesting findings of the task based evaluation

Of the twelve tasks to be attempted, Task 3, 7, 8 and 9, had an unsatisfactory success rate. Task number 3 had a 75% unsuccessful task completion rate, (see Figure 5.7). The unsuccessful task rate is a clear indication that the interviewees had not grasped enough information from the previous two tasks to successfully complete this task. An interesting outcome of this task was that

the majority of the interviewees clicked on the tick button, which changes the access status of ALL the ports or applications connected to that application or port to allow. The majority of the interviewees thought that by clicking the tick button it would only change the status of the one connection between the MSN Messenger application and the SMTP port. Therefore most of them failed to successfully complete this task. This however did expose the functionality of the tick button, which is that it changes all the connections to allow, to the interviewees.

Task numbers 7, 8 and 9 had a 55%, 65% and 40% unsuccessful task completion rate respectively, (see Figure 5.7). The unsuccessful task rate is a clear indication that there must be a number of things that the interviewees misunderstood or were confused with. Reasons for this rate of failure compared to the other tasks could be the following:

- Interviewees did not seem to acknowledge the functionality of a button when they made a mistake. They did not remember that previously the tick button changed the access status of all the corresponding applications or ports.
- The bottom panel of buttons of the corresponding applications or ports was not seen by the interviewee when displaying the number of allowed, denied or prompt applications or ports during Tasks 4, 5 and 6.
- The confusion of having two buttons with different functionality on top of each other but the one button relates to the functionality of the other button. In this case, the small number labeled button relates to the functionality of big tick, X or speech bubble button.

Interesting findings were as follows:

- When trying to do task three, one interviewee was in a loop whilst trying to change the access status of the Visual Studio.Net to HTTP connection to allow. The interviewee clicked the top box; (see Figure 4.3), of the Visual Studio.Net application to change the access status of the HTTP port but also remembers that clicking the tick button will change all the

ports to allow. Remembering this then made the interviewee click on the HTTP port and realized that the situation is the same from the port side. This raised the following question by the interviewee, after going around in a loop from Visual Studio.Net to HTTP, "If I click the tick it changes all of them, if I click in the small one it selects none of them because it's in deny, so I cant select it." This clearly indicates that the interviewee did not see that the change could be made from the bottom panel of buttons that appears on the corresponding HTTP node. It also indicates that the interviewee might not know that you have to select the connection between Visual Studio.Net and HTTP first and then change it.

- When attempting the last three tasks, some interviewees changed those access statuses one by one, using the technique that was suppose to be used in tasks 7, 8 and 9, instead of just clicking on the tick, X or prompt buttons to change all the applications or ports.
- Some interviewees were overeager to explore so before, or in some cases during, a task they were already clicking on some of the objects of the new information visualization personal firewall. This exploration however did afford them the opportunity to discover what happens when clicking on various options.
- The majority of the interviewees learnt the functionality of the tick button by mistake. This is when they were attempting to do task three but by clicking the tick button they discovered that it changes all the ports to allow. What was interesting was that even though the interviewees had learnt this functionality this mistake was continued in tasks 7, 8 and 9.

5.4 Experiment 4 Conclusion

This experiment allowed us to gauge the success of our design and visualization choices, as well as how usable the new information visualization personal firewall was. Based on the results, interesting findings and the discussion above we think that the high success rate of 8 of the 12 tasks and the fairly successful rate of the latter 4 tasks counts well for the new information visualization personal firewall. There were a few areas that influenced the usability of the new information visualization personal firewall. These included that design choices made for the bottom panel of buttons

were not intuitive and somewhat confusing because it was shown that to allow, deny or prompt an application or port the interviewees chose to click on the bigger tick, deny or prompt buttons. There was also reliance on interviewees noticing certain things whilst attempting to perform a task - the interviewees did not notice that an application or port can be changed using the corresponding bottom panel of buttons of the application or port. Design solutions for these problems will be discussed in the next chapter.

Chapter 6: Conclusion and future work

6. Conclusion and Future Work

6.1 Conclusion

There are a few questions that initiated the train of thought for this research. They are as follows, "If security software such as a personal firewall is installed to protect computers, why do these computers still get infected with viruses, worms and intrusion attacks by hackers, crackers etc.? Could the problem be that the person who installs the personal firewall lacks the knowledge and know how when configuring the personal firewall? Could it be that the terminology used on personal firewall software is not easily understandable by novice users?

In Chapter 1, we proposed that the problem with a personal firewall is that most users do not have the correct conceptual models of interaction between computer, firewall, and security in order to configure these personal firewalls correctly. From this proposition, the research problem that we attempted to solve is to design and develop a new personal firewall interface that will intuitively develop the user's conceptual models of interaction between computer, firewall and security. We used information visualization to build a metaphor, which was to be the solution to this research problem.

The research questions that were raised at the beginning of this research were as follows:

- Does the use of visualization improve the usage and adoption of modern network firewalls by novice users?
- Is visualization the answer to improving usage of firewalls by novice users?

6.1.1 Research Question One Conclusion

"Does the use of visualization improve the usage and adoption of modern network firewalls by novice users?"

From a task success rate and iconic representation perspective the answer is "yes" to the success of the adoption of modern network firewalls by novice users. This is

proven by results of the cyclic conceptual model extraction experiment and the task-based evaluation.

In the cyclic conceptual model extraction experiment the users understood the iconic representations, which are the http icon, email icons, tick, cross, lines, etc, (see Section 4.3.4, Results: Responses to the conceptual model extraction questions), with the exception of the prompt user icon. The prompt user icon was not recognised due to poor iconic design choices to represent prompt user mode. The question mark within a speech bubble was supposed to signify a question being asked to the users but the interviewees did not understand the significance of the speech bubble in the context of personal firewall technology.

In the task-based evaluation, we would claim that the usability of these novice users' exhibit the signs of improved usage because 8 of the 12 tasks had a success rate of 90% and above, (see Chapter 5, Figure 5.3).

From a task success rate perspective in this particular research solution the result was less encouraging in terms of improving the usage of modern network firewalls by novice users. This is proven by the results of a few tasks of the task-based evaluation.

In the task-based evaluation, tasks 3, 7, 8 and 9 had an unsuccessful task rate of 75%, 55%, 65% and 40% respectively. These tasks were usage tasks e.g., Task 7: Can you deny Internet Explorer's access to the SMTP port? For there to be a success for the usage of these tasks, they should display a similar high percentage level as the other tasks, which is 90% and above success rate but the success rates for tasks 3, 7, 8 and 9 are 25%, 45%, 35% and 60% respectively.

The reason for the unsuccessful rate for tasks 3, 7, 8 and 9 is a poor design choice for the bottom panel of control buttons. The idea of having a smaller button placed on top of a bigger button and the fact that these buttons had two different functions was not a logical choice. This situation caused a reasonable amount of confusion for the interviewee's during the task-based evaluation experiment. Task 7 was denying Internet Explorer access to only the SMTP port. When the interviewee's attempted this task the most recurrent action was the interviewees denying all ports to Internet

Explorer by clicking the bigger X button which they thought would deny Internet Explorer access to only the SMTP port. The layout of the bottom panel of control buttons was not effective enough and detrimental to the usage of the new personal firewall information visualization by the interviewees and this is the reason for the unsuccessful rate of 75%.

6.1.2 Research Question Two Conclusion

"Is visualization the answer to improving usage of firewalls by novice users?"

We believe that visualization can be the answer to improving usage of firewalls by novice users. However, in this research, the attempt at improving the usage was not convincing but we believe that with a few more design and test iterations, long term trial and testing of the visualization it is possible to increase the effectiveness of the visualization.

6.2 Future Work

6.2.1 Zoom Feature

- **Feature Description**

  A zoom feature can be added to the nodes. The zoom feature is when an application or port node is selected, this node, along with the nodes connected to it, will zoom forward and the unselected nodes will turn grey in colour, get smaller and zoom to the back, thus creating a selection/deselection effect.

- **Feature Benefits**

  Benefits include allowing one to clearly see the selected node and its children connected to it because the other nodes get smaller, turn grey and zoom to the back and emphasizes the "Zoom and Filter [23]" part of the visual seeking mantra.

6.2.2 Add or Remove, Application or Port Nodes

- **Feature Description**

  This feature will allow the user to add or remove nodes to either the application or port side of the visualization.

- **Feature Benefits**

  One benefit is that it allows one to add and remove ports on-the-fly.

6.2.3 Refinement of Icons and Tick, Cross and Prompt Control Buttons

- **Feature Description**

  The icons can be evaluated and refined to see how effective they are with respect to icon functionality. An alternate or completely new solution to the tick, cross and prompt buttons can be researched.

- **Feature Benefits**

  The refinement of the icons and the tick, cross and prompt buttons can improve the adoption of modern network firewalls by novice users.

6.2.4 Visualization solution to the application or port list becoming extremely large in numbers

- **Feature Description**

  The visualization solution could involve hiding the application or port nodes under a group name via a drop list. This would mean that there would be more information to "zoom and filter [23]" while looking for an application or port and its connecting applications or ports.

- **Feature Benefits**

  The benefit of this is that the visualization will be able to cope with large numbers of applications and ports all running at once and all requiring to be visible on the visualization.

6.2.5 Connect the new information visualization personal firewall to the back-end of a personal firewall and see if this functionality affects the visualization choices made

- **Feature Description**

  Connect the new information visualization personal firewall front end to the back-end of a personal firewall. This will allow us to see how the front end will behave when connected to a back-end.

- **Feature Benefits**

  A benefit is that new problems may present themselves as a result of connecting the front end to a back-end. These new problems may have an effect on the visualization. This effect may be negative, thus making the visualization more inefficient than when it was just a front end or the effect may be positive in that

the visualization will become more efficient as a result of being connected to a back-end of a personal firewall.

6.2.6 Add this new information visualization personal firewall as an added view to personal firewalls.

- **Feature Description**

  This involves adding this new information visualization personal firewall to an existing package like Panda Platinum Internet Security, for example.

- **Feature Benefits**

  A benefit of doing this could be to observe how well it meshes into the structure of an existing personal firewall package and to observe how often users use it and what they use it for.

References

[1] Bell, M. Chalmers, M. Barkhuus, L. Hall, M. Sherwood, S. Tennent, P. Brown, B. Roland, D. Benford, S. Hampshire, A. Capra, M. 2006 *Interweaving Mobile Games With Everyday Life*. ACM CHI 2006, April 21-28.

[2] Canavan, J.E. (2001). *Fundamentals of Network Security*. Artech House Publishers, Boston.

[3] Card, S.K., Mackinlay, J.D., and Shneiderman, B. (1999). *Readings in Information Visualization: Using vision to think*. Morgan Kaufmann Publishers, Inc., San Francisco, California.

[4] Check Point Software Technologies Ltd. 2003 – 2007. *ZoneAlarm Pro*, [online] Available: http://www.zonelabs.com

[5] Dillon, A. (2001) *The evaluation of software usability*. In: W. Karwowski (ed). Encyclopedia of Human Factors and Ergonomics. London: Taylor and Francis.

[6] Dray, S.M, 2003. *Tutorial Presented at CHI 2003 Ft. Lauderdale, FL, April 2003. Understanding users' work in context: Practical observation skills.* Dray & Associates, Inc. Minneapolis, Minnesota, USA [April, 2003]

[7] Eick, S.G. 1996. *Aspects of Network Visualization* Computer Graphics and Applications, Vol. 16, No. 2, pages 69 – 72, March 1996. [March, 1996]

[8] Encyclopedia Britannica Concise Edition, 2005. *Metaphor Dictionary Definition*. 2005.

[9] Human-Computer Interaction Lab, University of Maryland. *Piccolo Toolkit: A structured 2D Graphics Framework*. [online] Available: http://www.cs.umd.edu/hcil/jazz/

[10] Infosec, 2007. *Anti-Virus Software Definition* [online] Available: www.infosec.gov.hk/english/general/glossary.htm [January, 2007]

[11] Internet world statistics: usage and population statistics, 2007. *World Internet users and population statistics: usage growth 2000 - 2007*. [online] Available: http://www.internetworldstats.com/stats.htm [January 11, 2007]

[12] Karat, J. Atwood, M.E. Dray, S.M. Rantzer, M. Wixon, D.R. 1996. *User Centered Design: Quality or Quackery?* CHI 96 Panels, 161 – 162, April 13 – 18, 1996 [13 – 18 April, 1996]

[13] Leech, B.L. 2002. *Asking Questions: Techniques for semi-structured interviews.* PS: Political science and politics, American Political Science Association. Vol. 35, No. 4 (Dec., 2002), 665-668. [December, 2002]

[14] Lombard, E, 2006. HouseCall: First Aid for you PC, Trend Micro. *Hacker cleans out bank accounts - Hundreds of thousands of rands stolen via Internet from Absa clients.* [online] Available: http://www.housecall.com.sg/PDFs/Hackerscleansoutbankaccounts.pdf [January 15, 2006]

[15] Marsden G, 2005. *Interaction Design* [Course Notes] Cape Town: University of Cape Town. [February, 2005]

[16] McPartlin, C. 2000 – 2007. WSAW: News Channel 7. *News Headlines: Computer Hacker Charged.* [online] Available: http://www.wsaw.com/home/headlines/1157736.html

[17] Microsoft Corporation, 2007. *Windows Firewall: Windows XP Service Pack 2 (SP2)* [online] Available: http://www.microsoft.com

[18] Panda Software, 2007. *Panda Platinum Internet Security (8.05.01)* [online] Available: http://www.pandasoftware.com

[19] Preece, Rogers, Sharp, (2002). *Interaction Design beyond human-computer interaction*, John Wiley & Sons, Inc, 2002 [January 2002]

[20] Rindskopf, A. 1998. U.S. Department of Justice. *Press Release: Juvenile Computer Hacker cuts off FAA tower at regional airport – first federal charges brought against a juvenile for computer crime.* [online] Available: http://www.cybercrime.gov/juvenilepld.htm [March 18, 1998]

[21] SearchSecurity.com, TechTarget, 2000 – 2007. *Information Security Definitions – Personal firewall* [online] Available: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci331881,00.html

[22] SecurityStats.com, 2000 - 2004. *Most Requested Statistics* SecurityStats.com, Inc., 2000 [online] Available: http://www.securitystats.com

[23] Shneiderman, B. 1996. *"The Eyes Have It: A Task by Data Type Taxonomy for Information Visualizations"* Department of Computer Science, Human-Computer Interaction Lab, and Institute for Systems Research, University of Maryland, College Park, Maryland 20742 USA. [September, 1996]

[24] Snyder, C. (2003). *Paper Prototyping* Morgan Kaufmann Publishers, Inc., San Francisco, California.

[25] Stallings, W. (2003). *Network Security Essentials: Applications and standards.* Pearson: Prentice Hall.

[26] Symantec. *Norton Internet Security 2003* [online] Available: http://www.symantec.com

[27] United States of America. New York University Information Technology Services. (2006). *Personal Firewalls: NYU Security Awareness Month 2006.* [online] Available: http://www.nyu.edu/its/pubs/pdfs/personal_firewalls.pdf

[28] Viruslist.com: all about Internet security, Kaspersky Lab. 1996-2004. *News: Brazilian hackers attack email bank accounts.* [online] Available: http://www.viruslist.com/en/news?id=154001879 [October 23, 2004]

[29] Viruslist.com: all about Internet security, Kaspersky Lab. 1996-2004. *News: MyDoom continues to cause chaos.* [online] Available: http://www.viruslist.com/en/news?id=1931854 [July 27, 2004]

[30] Geng, W, Flinn, S, Dedeourek, J. 2005. *"Usable Firewall Configuration"* Proceedings of the 3rd Annual Conference on Privacy, Security and Trust (PST 05). [October 2005]

[31] Whitten, A, Tygar, J.D. 1999. *"Why Johnny Can't Encrypt: A Usability Case Study of PGP 5.0"* Proceedings of the 8th USENIX Security Symposium. [August 1999]

[32] Wool, A. 2004. *"The use and usability of direction-based filtering in firewalls"* Computers & Security. Vol. 23, Issue 6. Pages: 459-468. Elsevier Science B.V. [September 2004]

Appendix A

Key for Table 4.6:

Int. - Interviewee

V P – Virus Protection

S P – Spyware Protection

ADP – Anti-Dialer Protection

SmP – Spam Protection

WCF – Web Content Filtering

QS – Quarantine Services

PC – Program Control

Alert Ad – Alert Advisor

Email – Email Protection

MAC – Machine Access Control

DNU – Do Not Understand.

Table 4.6: Summary of experiment 2 short questionnaire responses.

	VP	SP	ADP	SmP	WCF	QS	PC	AlertAd	Email	MAC
Int. 1	1	1	2	4	4	2	3	3	2	3
Int. 2	1	1	2	2	4	1	3	3	1	3
Int. 3	1	1	1	3	2	2	3DNU	1	2	2
Int. 4	1	1	2	1	2	1	2	1	1	2
Int. 5	1	1	1	1	1	1	3	1	1	1
Int. 6	1	1	1	1	1	1	3	1	1	1
No. of 1's	6	6	3	3	2	4	0	4	4	2
No. of 2's	0	0	3	1	2	2	1	0	2	2
No. of 3's	0	0	0	1	0	0	5	2	0	2
No. of 4's	0	0	0	1	2	0	0	0	0	0
No. of 5's	0	0	0	0	0	0	0	0	0	0

One can clearly see that the functions agreed on are:

- Virus Protection (V P) with six 1's which is 100% agreement.
- Spyware Protection (S P) with six 1's which is 100% agreement.
- Quarantine Services (Q S) with four 1's and two 2's which is 100% agreement.
- Email Protection (Email) with four 1's and two 2's which is 100% agreement.
- Anti-Dialer Protection (ADP) with three 1's and three 2's which is 100% agreement.
- Alert Advisor (Alert Ad) with four 1's which is 66,67% agreement.
- Spam Protection (SmP) with three 1's and one 2's which is 66.67% agreement.
- Web Content filtering with two 1's and two 2's, which is 66.67% agreement.
- Machine Access Control with two 1's and two 2's which is 66.67% agreement.

The only function that is not agreed on is:

- Program Control (PC) with one 2's i.e. 33.33% agreement.

Appendix B

Experiment 3: Reiterated a few questions from the cyclic conceptual model extraction experiment

1. What do you think the boxes on the left represent?
2. What do you think the boxes on the right represent?
3. What do you think the bracketed number in each box e.g. (6) represents?
4. What do you think the lines represent?
5. What do you think  represents?
6. What do you think  represents?
7. What do you think would happen if the tick was clicked?
8. What do you think would happen if the cross was clicked?
9. What do you think would happen if the question mark in a speech bubble was clicked?

Tasks to be performed:

Task 1:

How many ports (e.g., HTTP, SMTP) are connected to the application Explorer?

Task 2:

How many of the ports connected to Internet Explorer are: Allowed? Denied? Prompt?

Task 3:

Can you allow the SMTP port to be accessed from MSN Messenger application?

Task 4:

Can you show me which ports have allowed access to the application Internet Explorer?

Task 5: Can you show me which applications are denied access to the HTTP port?

Task 6: Can you show me which applications have prompt access to the IMAP port?

Task 7: Can you deny Internet Explorer's access to the SMTP port?

Task 8: Can you allow Visual Studio.Net access to the HTTP port?

Task 9: Can you set MS Words' access to SMTP to prompt access?

Task 10: Can you allow Skype to access all ports?

Task 11: Can you deny HTTP to all its applications?

Task 12: Can you set all the MISCELLANEOUS port connections to prompt access?

Appendix C

Experiment 2's, Semi-Structured Interview Questions:

1. How often do you use your computer?
2. Do you use Microsoft Office e.g. Ms word, Excel, Powerpoint, Access?
3. Do you use Email?
4. What other things do you use your computer for?
5. Is your computer connected to the Internet?
6. Can you tell me what you use the Internet for?
7. Are you worried about the security of your computer, whether it is on or off the Internet?
8.

8.1 Do you currently have any software or package/s protecting your computer?

8.2 If firewall does not come up, have you heard of firewalls?

8.3 What do you think a firewall is?

8.4 If firewall does come up, what do you think a firewall is?

9.

9.1 Do you know what an installation wizard is?

9.2 Do you trust that the wizard is setting up your security such that your computer is secure?

9.3 Do you read the information the wizard is displaying or do you just click next to get the installation done?

10.

10.1 What do you think the status option does?

10.2 Do you know what an icon is?

10.3 Do you think the icon choice for status is good enough to represent status?

11.

11.1 Do you think the scale indicating the protection level of your computer is useful?

11.2 Is there anything you like, dislike or want to comment on?

12.

12.1 What do you think the full scan option does?

12.2 Do you think the icon for full scan is good enough to represent status?

12.3 Do you think all the options e.g., Scan local disk, Scan cd rom, Scan my documents is necessary?

12.4 Is there anything you like, dislike or want to comment on?

13.

13.1 What do you think automatic protection does?

13.2 What do you think antivirus protection does?

13.3 Do you think the icon for antivirus protection is a good choice to represent antivirus protection?

13.4 What do you think enabled means?

13.5 What do you think firewall protection does?

13.6 Do you think the icon for firewall protection is a good choice to represent firewall protection?

13.7 What do you think the view network activity option does?

13.8 What do you think anti-spyware protection does?

13.9 What do you think spyware is?

13.10 Do you think the icon for anti-spyware protection is a good choice to represent anti-spyware protection?

13.11 What do you think anti-dialer does?

13.12 Do you think the icon for anti-dialer protection is a good choice to represent anti-dialer protection?

13.13 What do you think anti-spam protection does?

13.14 What do you think spyware is?

13.15 Do you think the icon for anti-spam protection is a good choice to represent anti-spam protection?

13.16 What do you think Web content filtering does?

13.17 Do you think the icon for Web content filtering is a good choice to represent Web content filtering?

13.18 Is there anything you like, dislike or want to comment on?

14.

14.1 What do you think quarantine does?

14.2 Do you think the icon for quarantine is a good choice to represent quarantine?

14.3 Is the anything you like, dislike or want to comment on?

15. Do you trust that the firewall protecting your computer works properly?

16. How do you or would you know if your computer is secure, once you have installed the software?
17. What sort of things do you think firewalls should control?