

Vulnerabilities in Personal Firewalls Caused by Poor Security Usability

Bander Alfayyadh
James Ponting
Mohammed Alzomai
Information Security Institute
QUT, Australia

Email: {b.alfayyadh, j.ponting, m.alzomai}@student.qut.edu.au

Audun Jøsang
UNIK Graduate Center
University of Oslo
Norway
Email: josang@unik.no

Abstract—Poor usability of IT security present a serious security vulnerability which can be exploited to compromise systems that are otherwise secure. This is of particular concern when considering that the majority of people connecting to the Internet are not experts in IT security. Personal firewalls represent the most important security mechanisms for protecting users against Internet security threats. However, the knowledge and skills required to effectively manage and operate some aspects of a firewall may surpasses the capability of the average user. A set of security usability principles can be used to determined whether a security system has good usability. This paper evaluates the usability of personal firewalls systems by conducting a cognitive walkthrough to identify elements of the design which may violate these usability principles. The paper concludes with recommendations and suggestions for future work in the analysis and design of personal firewalls.

I. INTRODUCTION

The number of Internet and computer users is growing rapidly. More users are online everyday, with notebooks roaming between wireless and wired networks accessing essential services or their private data. Clearly, protecting private data is becoming extremely important. Computer users face more and more threats and they look for tools to protect their data. According to the Computer Crime and Security Survey [1], one of the most popular tools used for such need is a personal firewall. A firewall is defined as "an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system." [2]. Personal firewalls have become an essential part of online security. Typically a firewall controls incoming and outgoing traffic within a network and its role is to prevent some threats in the form of denying access. Generally, if used correctly a personal firewall should provide reasonable security. But as with many other security measures, a sound security system could be compromise by users' misuse or carelessness and this could cause serious security vulnerabilities [3], [4].

Poor usability of a security system can lead to serious consequences as pointed out by several authors. Whitten and Tygar's study [5], [6] on the usability of PGP showed that the security vulnerabilities were a direct result from usability problems. The same could be said about personal firewalls, personal firewalls usually run in the background and alert the

user if needed, the alert can be as clear as a pop-up window or as subtle a color change of a small icon in the system tray. Usability of personal firewalls is especially important and interesting to study because the target consumer for personal firewalls is normal users with little or no knowledge about IT security. And when a normal user has to make critical security decisions while interacting with their personal firewalls it is important that adequate information is given to them to make the correct decision.

A user who is not a security expert, may not have the required level of knowledge to understand the terminology or the consequences of some of the decisions he/she is required to make to manage the firewall properly. A security system that is used improperly could be more harmful than possessing no security system at all. The illusion of safety provided by a misconfigured firewall can result in users behaving as if they are protected, when, in fact they are exposed to the same risks as any other user but with the added vulnerability of a false sense of security.

Jøsang et al. [7] proposed eight usability principles inspired by security principles suggested by Belgian cryptographer Auguste Kerckhoffs [8], [9].

The security usability principles are divided into principles for security action and security conclusion which can be described as follows:

- A *security action* is when users are required to produce information and security tokens, or to trigger some security relevant mechanism. For example, typing and submitting a password is a security action.
- A *security conclusion* is when users observe and assess some security relevant evidence in order to derive the security state of systems.

The eight security usability principles are:

- 1) Security Action Usability Principles
 - a) The users must understand which security actions are required of them.
 - b) The users must have sufficient knowledge and the practical ability to make the correct security action.
 - c) The mental and physical load of a security action

must be tolerable.

- d) The mental and physical load of making repeated security actions for any practical number of transactions must be tolerable.

2) Security Conclusion Usability Principles

- a) The user must understand the security conclusion that is required for making an informed decision. This means that users must understand what is required of them to support a secure transaction.
- b) The system must provide the user with sufficient information for deriving the security conclusion. This means that it must be logically possible to derive the security conclusion from the information provided.
- c) The mental load of deriving the security conclusion must be tolerable.
- d) The mental load of deriving security conclusions for any practical number of service access instances must be tolerable.

This paper describe an analysis of personal firewalls against usability principles outlined above. If any of these principles is violated when the user interacts with the firewall then this will denote a usability problem. Violating any of these principles will not necessarily breach normal usability, (By normal usability we mean that of a non-security software) but breaches security usability which in turn causes security vulnerabilities. Modern firewalls normally have good usability from a traditional HCI (Human Computer Interaction) perspective. However, when tested against these security usability principles, several weaknesses emerge. The difference between normal usability and security usability has been pointed out in the literature [5], and is confirmed by this study.

II. CHARACTERISTICS OF A PERSONAL FIREWALL INTERFACE

Personal firewalls work in the background monitoring traffic and events. But they also communicate with the users either by alerting them that a threat or a condition that require their attention has been detected, or by asking them to configure the firewall to work properly. In most firewalls, users interact with them through the following interface channels.

A. Main Interface

The firewall main interface presents the menu through which the firewall can be controlled. Also, from here a user can check the status of the firewall, recent events, domain and other information.

The main interface is common across firewall vendors, although features may vary. An example of a firewall main interface is shown in Fig.1 which is a screen shot of ZoneAlarm personal firewall's main Interface. It has the following features:

- Firewall "strength" controls. (A simplified control to set firewall rules.)
- Program access/control. (A list of programs with network access.)

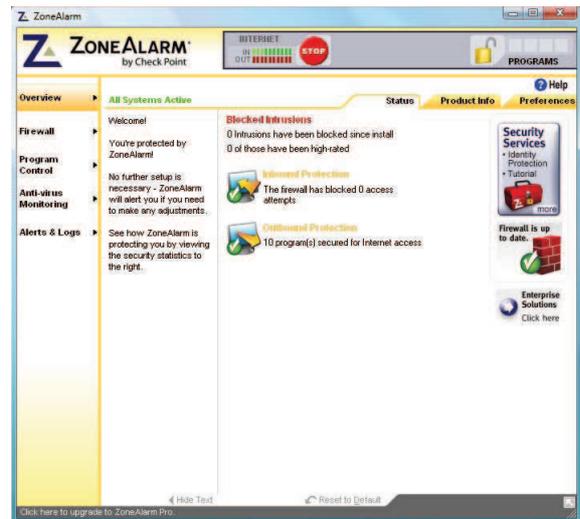


Figure 1. ZoneAlarm Master Interface.



Figure 2. Norton 360 Pop-Up Notification

- Alert logs. (A list of alerts or recent events pertaining to the firewall. This includes user inputs and connection attempts from numerous sources.)
- Network traffic displays. (A graphical representation of the network traffic heading in and out of the firewall.)
- Advanced Filters. (These allow for the creation of certain master rules whereby certain protocols and or ports can be forwarded without the firewall intervening.)

Other firewall vendors use different combinations of the above in various layouts and configurations.

B. Pop Up Notifications

Pop-up notifications are commonly used by the firewall to inform a user of a current event which requires the user's attention. The pop-ups occur when the firewall requires the user to make a decision, or needs to inform the user of a decision or an event.

The pop-up usually provides information regarding the



Figure 3. ZoneAlarm Start-bar Notification Icon (Left-most icon).

application that is trying to access the network, the destination from whence the message came or was meant to go and finally the actions which the user can instruct the firewall to take. The actions are usually to allow or deny and sometimes it also includes setting a new rule for the firewall to follow (i.e. to always allow such action).

In Fig.2 we can see an example of a pop-up notifications in Norton 360. The firewall was trying to alert the user that a program is attempting to access the Internet.

C. System Tray Notifications

Many firewalls display a small icon on the bottom right of the screen near the clock that provides information about the security status as monitored by the firewall. For example, ZoneAlarm provides an icon called a notification represented by the letter Z shown in Fig.3.

These icon provides information pertaining to the security status of the system. The status is shown usually by a change in color. In most cases, the icon remains static, however if a fault, error or intrusion is detected, it will change its colour in order to draw the user's attention to the event.

III. STUDY METHOD

For our evaluation of personal firewalls usability on Windows XP platform, we have chosen four popular firewalls, ESET Nod32 Smart Security, Norton 360 V. 2.0.0.242, ZoneAlarm V. 7.1.248 and Trend Micro Internet Security Version 16.00.1412. According to web portal firewallguide.com those are among the most popular personal firewalls for the windows platform and are generally used by consumers. We had the trial versions which had all the features. We configured four identical machines with similar software operating environment with each having a different firewall installed. We configured each firewall for initial use. Then we initiated network traffic between them and a fifth machine setup as an FTP server to trigger firewall response if any. During this we were evaluating usability and noting any issues. The evaluation method was cognitive walkthrough [10], [11]. Cognitive walkthrough means that we use the firewall per its intended use and take notes of usability problems. Usability problems occur when the usability principles are violated while interacting with the firewall interface.

IV. USABILITY OF PERSONAL FIREWALLS

The focus of this study was to observe the usability of the user interface in personal firewalls from the perspective of a normal user. For the purpose of this study we define a

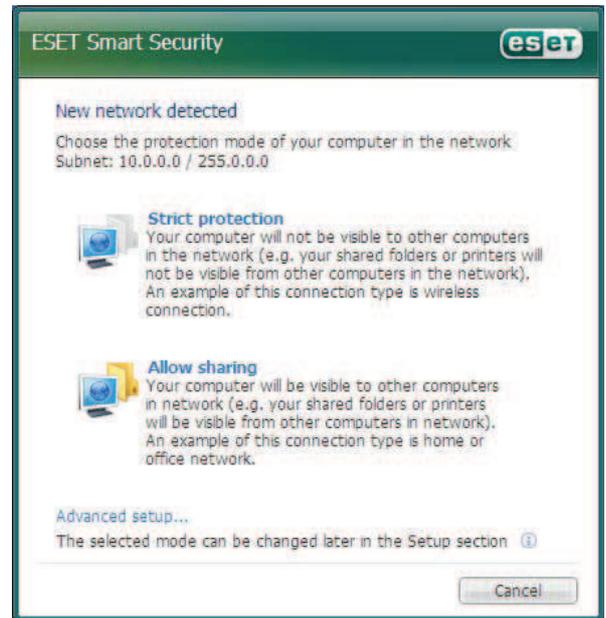


Figure 4. ESET Node32 Installation Pop Up

normal user as someone who uses computers but does not have training or expertise in IT security. It's generally understood that most computer users fall into this category. The personal firewalls we have chosen have fairly reasonable and friendly user interface and setup procedures. They are targeted to be used by normal users, they come in a packaged suites and are usually available where personal software are sold. It took us roughly the same amount of time to install and configure each firewall. In the following sections we discuss observed issues during the entire process.

A. Installation and Configuration

The installation and configuration of the personal firewalls was somewhat short. They all required the user to make security decisions during the setup process to determine how the firewall will operate. We noticed that some of these decisions required a level of knowledge that some inexperienced users may not possess. For example, while installing ESET Nod32, A pop-up window informed us that a network has been detected and asked to choose between two modes of protection while connected to this network (Fig.4). However, It did not provide necessary information like the name of the network or its type. The only information provided was this line: "Chose your protection mode of your computer in the network subnet 10.0.0.0/255.0.0.0" The subnet information does not help the user to make an informed decision compared to informing him/her if the network was secured or at least its name. Further more, the explanations provided for these options could be considered vague and misleading. Users are asked to chose either *Strict Protection* or *Allow Sharing*. They explained *Strict Protection* as *Your computer will be visible to other computers in the network*

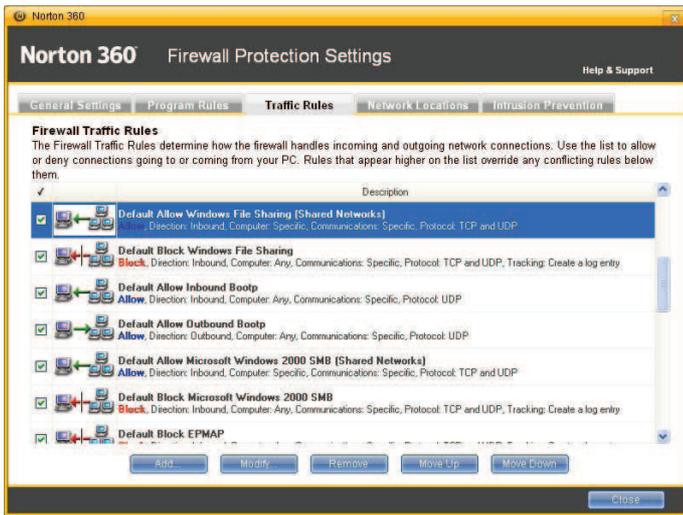


Figure 5. Norton 360 Traffic Rules

(e.g. your shared folders and printers will not be visible from other computers in the network), an example of this is wireless connection. While it's true the computer will be hidden from others, it is somewhat misleading to describe it as "Strict Protection", the computer is still connected to the network sharing resources (Internet, for example) and depending on the security of the network, the user still can be vulnerable.

In addition, it could be misleading to describe a wireless connection as an example where this mode is needed, the same could be said for a wired connection as well. The emphasis should have been on the security and encryption of the network not on its being wireless or wired. Users may lean to choose this option hoping for "Strict Protection" but it offers very little added security than *Allow Sharing* therefore losing valuable network service for little gain. This violates principle 1b and 2b and therefore is a usability problem.

There were similar observations when setting up ZoneAlarm firewall. The user was asked to choose between three settings: Maximum protection, Auto-Learn or minimum. But there was very little vague description to what they meant (See Fig.6).

Norton 360 and Trend Micro Internet Security did not give any configuration options during the installation process. The initial setup was configured by their default options and users were expected to go to the setting tab and change the default configuration if they need to. We inspected the setup and configurations menus for all firewalls. We noticed that some of the setup menus were confusing to a normal user. For example, Fig.5 shows the Traffic Rules, which is part of Norton 360 firewall Protection Settings. From there the user can allow or block different types of networks or connections. There were over 25 protocols and connections and by default some were blocked and some were allowed. The terminology and the short explanations were both unlikely to be understood by a normal user. Furthermore, some of the default values set by the firewall seemed a bit confusing, for example, in



Figure 6. ZoneAlarm Security Level Setting

Fig.5 we can see that the default Traffic Rules were to allow *Windows File Sharing (Shared network)* and just in the line underneath it stated that *Windows File Sharing* is blocked. A normal user will probably be confused by this and will consider it a contradiction and no explanation was found to this contradiction. To a lesser extent, this could be said about Trend Micro's "Network Protocol Control" (see Fig.7).

Throughout the installation and configuration, there was not always a direct link to find help, and most of the time it was either written in an overly simplistic manner, or written in a language that requires some network knowledge.

B. Interacting with the Firewalls

After we setup and configured all four firewalls, we setup our FTP server to selectively communicate with each machine. The goal was to trigger firewall response if any. The FTP server was connected in the same manner with all four machines.

We observed a few usability issues either due to poor visibility of alerts or ambiguous information provided. We will show a few examples to illustrate these problems. When we attempted to connect the ESET Nod32 Machine to the FTP server, there was no clear warning that an outside machine is connecting to the computer. We noticed a small icon at the bottom right of the screen that could easily be missed. Furthermore, when we clicked on it, it led us to the main interface window with no mention of this. We had to navigate through a few menus to find that an outside connection was being setup. There were several usability issues of this nature, all had poor visibility of alert or status notification. Some firewalls have a status icon (Usually at the bottom of screen) that would change color to indicate possible threat. This is not sufficient and it may lead the user to continue using the computer even when the environment is not safe.

There were usability issues due to ambiguous or lack of information. An example of this is when a program attempts to connect or receive incoming connections. The firewall intercepts these requests and prompts the user for a decision. However, the requesting program is identified by its process name and not the program name. Although the process name often reflects the name of the program it is running (Internet Explorer's process is named "iexplorer.exe"), there were cases where it would be difficult for a normal user to identify which

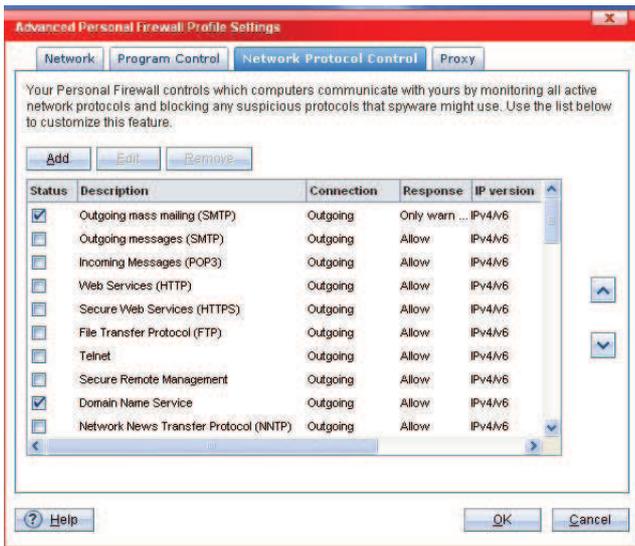


Figure 7. Trend Micro Network Protocol Configuration

program is making the request based upon the process name alone. Adobe's document reader Acrobat is commonly used to open documents from the Internet. In many cases, the Internet browser will pass the address of the file to Acrobat and Acrobat will be the program which attempts to connect and access this file. The firewall will intercept such connection request and prompt the user for a decision on whether to allow or deny. However, the information provided to the user is that "AcrRd32.exe" (Acrobat's process name) is making the request. While an experienced user will recognize the name as Acrobat Reader and make an informed decision, an inexperienced user may be confused. Nothing about Acrobat reader suggests that the "32" should be present, also it may elude some users to recognize that "AcrRd" stands for Acrobat Reader. This is a usability issue because it violates usability principles 1b and 2a.

Another example is the external destination of the connection is represented by an IP address. If Internet explorer, for instance, attempts to connect to www.google.com, it will be intercepted by the firewall and a pop-up will inform the user that IExplorer is attempting to connect to "64.233.187.99" (see Fig.8). This IP address does not provide useful information to make a decision, the user probably will not know that that IP address corresponds to google.com. This is a usability issue and it violates usability principles 1b, 2a and 2b.

The addressing method also presented a usability concern. There was not enough information about ports and protocols. For example, DNS (Domain Name Server) requests are for the most part relatively harmless. They merely turn the namespace www.google.com into its associated IP address; most users do not know that certain protocols and ports can represent larger risks than others. In the operation of the firewalls, there was no such distinction and that information was not used to aid the user when he/she needs to make a decision.



Figure 8. ZoneAlarm Pop-Up Notification.

V. SUMMARY AND RECOMMENDATION

In this section, we provide a summary of our study and present our findings. We also present some suggestions for personal firewalls usability.

The firewalls we reviewed will generally provide good security if configured and used properly. However, we noticed that all of them show some weakness when trying to provide the user with security information. During the installation process we observed some small usability issues resulting from lack of information. The user may not have the level of skills or knowledge about network security to make the required correct decisions and choices, and in some cases, the information provided did not help much. While configuring the firewalls we observed several usability problems. Most of the configurations required at least some IT security knowledge that most personal firewall users do not have.

The usability issues that we noticed lay in two main categories. Firstly, there was either vague information, or lack of information provided to the users when they need to make a security decision. Secondly, there was often poor visibility of alerts or status changes. Firewall designers could improve the quality of information provided by doing more usability testing with normal users. Also, usability experts could be asked to be involved earlier in the design process.

Security software designer's first and main concern is strong security, not great usability. However, we think by improving usability, security could be improved as a result. There is a delicate balance between security and usability that can be achieved with proper design and by including usability in the development process. There are several usability guidelines for security design [12], [13] that could be considered. Also general usability guidelines that are widely available from CHI [14], [10] can help to improve usability if considered during the design process.

VI. RELATED WORK

Usability evaluations of security tools often demonstrate serious security vulnerabilities, such as Whitten and Tygars seminal security usability study of PGP usability [5] which showed that the majority of users were unable to use it correctly for sending encrypted emails, so that the security was

compromised. Similar experimentation study on the usability of sms authorization in online banking showed that poor usability can highlight an otherwise hidden vulnerabilities [15].

The usability of firewalls has been examined to some extent in several studies. The Usability study of Windows XP Internet connection firewall (ICF) conducted by Johnston, et al. has shown some vulnerabilities due to poor usability. They suggest that following HCI-S criteria can lead to improving security by ensuring usability is developed into the security interface [13]. Kamara et al. Described a methodology for vulnerability testing in firewalls [16]. Many computer magazines and website provide analysis of firewalls (Like firewallguide.com) but usually they are short reviews.

VII. CONCLUSION

In this paper we evaluated the usability of four personal firewalls that normally target users with little or no knowledge about IT security. The evaluation method was cognitive walk-through. We setup four computers to have exact conditions and software under Windows XP platform. The evaluation included installation, configuration and normal operation. To trigger firewall responses to possible threats we created a connection between the four machines and a fifth one that acted as an FTP server, we initiated connections both inbound and outbound.

We have shown that generally personal firewalls suffer from poor usability which in turn may cause security vulnerabilities. The usability issues were either that the information provided by the firewalls (whether it was during installation, configuration or interaction) was vague or misleading. Some usability issues were noted due to poor visibility of alerts.

Personal firewalls, generally, have friendly user interface and provide good security in protecting ports from harmful connection threats from the Internet. However they display poor usability when it comes to informing the user of a possible threat and prompting for a decision. Security decisions that will affect the performance of the firewall had to be made by a user who is either un-informed or mis-informed. The level of knowledge that is required to understand some of the concepts or information provided in configuration menus or warning pop-ups often surpasses that of a normal user with little or no expertise in IT security.

VIII. FUTURE WORK

As an extension to this study, we intend to conduct further investigation into usability of personal firewalls. the investigation will include more personal firewalls and will involve actual users interacting with the interface of the firewalls. We will investigate the installation and configuration process as well as interacting with the firewall.

We will ask the users to record the instances when they were asked to make a decision and if they understood all the information provided by the firewall. The machines will be identical and the users will be normal users with little or no knowledge about network security.

REFERENCES

- [1] R. Richardson, "Csi/fbi computer crime and security survey," Computer Security Institute, San Francisco, USA, San Francisco, USA, Tech. Rep., 2003.
- [2] O. Dictionary, "<http://www.dictionary.com>," Last accessed: Feb-2008, 2008.
- [3] M. Sasse, "Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery," in *Proceedings of the Conference on Human Factors in Computing Systems (CHI2003)*, (Workshop on Human-Computer Interaction and Security Systems), 2003.
- [4] M. A. Sasse and I. Flechais, "Usable security: What is it? How do we get it?" in *Security and Usability: Designing Secure Systems that People Can Use*, L. Cranor and S. Garfinkel, Eds. Sebastapol, CA, USA: O'Reilly, 2005.
- [5] A. Whitten and J. Tygar, "Why johnny can't encrypt: a usability evaluation of pgp 5.0;" in *Proceedings of the 8th USENIX Security Symposium (Security'99)*, 1999.
- [6] Whitten, A. and Tygar, J.D., "Usability of Security: A Case Study," Carnegie Mellon University, Computer Science Technical Report CMU-CS-98-155, 1998.
- [7] A. Jøsang, B. AlFayyadh, , T. Grandison, M. AlZomai, and J. McNamara, "Security Usability Principles for Vulnerability Analysis and Risk Assessment," in *proceedings of ACSAC 2007 - Annual Computer Security Applications Conference*, Dec 2007.
- [8] A. Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires*, vol. Vol. IX, no. 38, pp. 5–38 (January) and 161–191 (February), 1883, translation available at F. Petitcola's Website: <http://www.cl.cam.ac.uk/~fapp2/kerckhoffs/>.
- [9] P. Gutmann and I. Grigg, "Security Usability," *IEEE Security and Privacy*, vol. 3, no. 4, pp. 56–58, 2005.
- [10] J. Nielsen, *Usability Engineering*. San Francisco, United States: Morgan Kaufman Publishing Inc., 1993.
- [11] P. Polson, C. Lewis, J. Rieman, and C. Wharton, "Cognitive walk-throughs: a method for theory-based evaluation of user interfaces," *International Journal on Man-Machine Studies*, vol. 36, no. 5, pp. 741–773, 1992.
- [12] K. Yee, "User interaction design for secure systems," in *Proceedings of the 4th International conference on Information and Communications Security, ICICS 2002*, 2002.
- [13] Johnston, J. and Eloff, H. P. and Labuschagne, L., "Security and human computer interfaces," *Computers And Security*, vol. 22, no. 8, pp. 675–684, 2003.
- [14] R. Kumar, *Research methodology : a step-by step guide for beginners*. Melbourne, Australia: Longman, 1996.
- [15] M. AlZomai, B. AlFayyadh, A. Jøsang, and A. McCullagh, "An Experimental Investigation of the Usability of Transaction Authorization in Online Bank Security Systems," in *proceedings of AISC 2008 - Australian Information Security Conference*, Jan 2008.
- [16] Kamara, S. and Fahmy, S. and Schultz, E. and Kerschbaum, F. and Frantzen, M., "Analysis of vulnerabilities in Internet firewalls," *Computers And Security*, vol. 22, no. 3, pp. 214–232, 2003.