TDDC03 Projects, Spring 2006

# A comparison of the security and usability of personal firewalls

Kristian Köpsén, Malin Nilsson

Supervisor: Almut Herzog

# A comparison of the security and usability of personal firewalls

Kristian Köpsén and Malin Nilsson
Dept. of Computer and Information Science
Linköping University
Linköping, Sweden
{kriko839, malni280}@student.liu.se

## Abstract

*In this study we have evaluated the security and usablity of a number of personal firewalls by installing them on a PC and submitting them to a security and usability test of our design. We have downloaded eleven different personal firewalls, both free and evaluation versions. We have investigated these with respect to 13 different aspects. Our conclusion is that all of the firewalls contain flaws, both in usability and security.*

## 1. Introduction

It has lately become common that home users have personal firewalls. In contrast to classic firewalls, these are completely software based, and are often oriented around applications, rather than ports, packets and hosts. Unfortunately, many of the personal firewalls can be quite difficult to understand and manage. A badly configured firewall can easily be worse than no firewall at all, since users might get a false sense of security. Because of this it is interesting to investigate their usability and its security consequences.

## 2. Method

### 2.1 Firewalls

We have evaluated eleven personal firewalls, that were all available for download in March and April of 2006. They are all product run in Microsoft Windows, and we made this restriction because that is a market with a large number of products available. We don't believe it would have been possible to make a fair comparison if firewalls for different operative systems were included. The firewalls in the study are:

- Sunbelt Kerio Personal Firewall
- Agnitum Outpost Firewall PRO
- Comodo Personal Firewall
- LavaSoft Personal Firewall
- VisNetic Firewall
- Norman Personal Firewall
- Microsoft Windows Firewall
- Norton Personal Firewall
- NetVeta Safety.Net
- ZoneAlarm
- F-secure Internet Security

We have picked these firewalls from those that a number of websites [2] [3] mention as common or popular, and that were available for download. We also added some firewalls that we ourselves recognised, and thought of as interesting enough to include.

### 2.2 How we evaluated

The firewall evaluations were performed on a Dell Inspiron 510m notebook, using the university's netlogon internet access through the built-in 100 MBit network adapter. The computer also had a wireless network adapter, but firewall settings relating to that were not actively evaluated, and are only mentioned in cases where the user is forced to make a related decision. The operative system of the test computer was Windows XP Professional, with Service Pack 2. We used Windows System Restore after each evaluation, to make sure that as few traces of the firewalls as possible remained.

### 2.3 Our evaluation criteria

The evaluation of the firewalls was done with a novice user primarily in focus, but at all times we also had a experienced user in mind.

The security evaluation was done without any formal evaluation model. The field of personal firewalls does not seem to be big or interesting enough for there to be any formal definitions of what a personal firewall is supposed to be able to do. Instead, we have done a comparative evaluation and let the evaluated set of firewalls determine what funcionalities we consider as normal.

We have used Jakob Nielsen's [4] ten general principles for user interface design as guidelines and reference. Since they are not complete in any way, we have not based our evaluation on them but rather used them where applicable. The ten principles are [4]:

1. **Visibility of system status.** The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.

2. **Match between system and the real world.** The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order.

3. **User control and freedom.** Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. Support undo and redo.

4. **Consistency and standards.** Users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform conventions.

5. **Error prevention.** Even better than good error messages is a careful design which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.

6. **Recognition rather than recall.** Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.

7. **Flexibility and efficiency of use.** Accelerators – unseen by the novice user – may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.

8. **Aesthetic and minimalist design.** Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.

9. **Help users recognize, diagnose, and recover from errors.** Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.

10. **Help and documentation.** Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user's task, list concrete steps to be carried out, and not be too large.

## 2.4. What we evaluated

### 2.4.1 Trial or free version

Some of the firewalls that we tested are freely available while others are commercial. In the latter case, we evaluated trial versions.

### 2.4.2 General

Under this heading, we describe and evaluate the general interface of the firewall, and the general feeling of the software. We also discuss general aspects that do not fit under any other heading.

### 2.4.3 Installation

The install process usually gives the users their first impression of the software. This makes it extra important that it is well thought through. Often, the user has to make security critical decisions already during the install, which makes it important to investigate.

### 2.4.4 Stealth

A very basic functionality of a personal firewall is to acheive stealth on unused ports. A proper firewall should have this as a default setting, or at least as a very easily available option. To test how the firewalls reacted to incoming packets we used [1]. For the basic tests we ran sequential port scans on the low port ranges.

### 2.4.5 Allowing outgoing communication

One central functionality of a personal firewall is that it should be configurable to allow a trusted application to access the Internet. To test this, we used the program WinSCP.exe which is a small application for connecting to SCP or SFTP servers. The basic scenario consisted of just starting the program and responding to the alerts and dialog boxes. If that did not succeed, we proceeded by trying to add rules through the interface of the firewall.

### 2.4.6 Allowing software to receive incoming requests

Another category of applications using the network are those that receive incoming connection attempts. We believe that a decent personal firewall should be fairly easy to configure to make such programs work properly. We tested this by running the Cerberus FTP Server, and trying to set up the firewall so that it could accept connections and send files. The basic way we tried was to just start the application and see what happened. In some cases there were alerts that allowed us to configure appropriate rules. In other cases we had to force alerts by attempting to make FTP connections from another computer, while in some cases we had to manually configure rules.

### 2.4.7 Fooling the firewall

Firewalls that base their security rules on trusted software can have a weakness. If it is possible for a malicious program to masquerade as a trusted program, it might be able to bypass the firewall. In order to try if it was possible to fool the firewall through changing the name and path of a malicious application to match that of a trusted one, we performed the following steps.

1. Make a rule to allow the web browser Firefox to access the internet (on port 80 if applicable).
2. Make sure there are no rules relating to WinSCP.exe
3. Rename firefox.exe to something else.
4. Copy WinSCP.exe into the firefox directory and rename it firefox.exe
5. Run the fake firefox.exe, and ask it to connect to the internet on port 80.
6. See how the firewall reacts.
7. If the firewall detected the changed application, tells us about it in an understandable way, and offers to block it, we will.
8. Replace the fake software with the real Firefox, and try to get online.
9. See how the firewall reacts.

### 2.4.8 Pop-ups and error messages

Once the firewall is installed and configured, users usually do not want it to bother them any more. We have investigated the ways that the personal firewalls announce themselves to the user, and the ways to control such behaviour. We have also evaluated the pop ups from a usability perspective.

### 2.4.9 Activation/deactivation

Sometimes it is necessary to temporarily deactivate the firewall. Also, many firewalls have "panic buttons" that stop all network traffic. We have looked at how this is done in the different firewalls.

### 2.4.10 Help and documentation

Having a working and useable help system is vital for any application. In security applications, such as personal firewalls, this is extra important, because of the potential risks with a bad configuration. We believe that a help system should be context sensitive, easy to navigate and obviously provide correct and understandable information.

### 2.4.11 Log

The firewall log might not be of much interest for inexperienced users. However, once a user gains a bit more knowledge, or has a specific problem they want to fix, a log can be a good help or even a necessity. A log file can usually grow large very fast, and because of this, we believe that there should be ways to sort and filter it.

### 2.4.12 System resources

Since personal firewalls are intended to run in the background while the user is working, it is interesting to know how much of the computer's system resources they use. During the evaluation we concluded that a memory usage of up to 25 MB was quite normal, and that most firewalls rarely used more than ten percent of the CPU.

### 2.4.13 Trusted zone

Personal firewalls can be used in many different network environments. In for example a home environment, the user may want to exclude certain hosts or subnets from the protection of the firewall, or make special rules for these hosts. In this section, we investigate whether such tasks are possible, and if the settings are easy enough to understand.

#### 2.4.14 Advanced filtering

In this section we investigate firewall functionalities beyond host and port based filtering. We have seen that most personal firewalls make their rules based on the hosts and/or ports that packets arrive from (or are addressed to). However, many hardware firewalls and other professional security systems use other methods to determine whether connections should be allowed or not, such as inspecting packet contents as if they were operating on a higher level of the network stack. For each firewall, we investigate if they claim to have this, or any other similar, feature.

## 3. Results

The results from our study can be found at http://www.ida.liu.se/˜almhe/firewall-comparison/

## 4. Conclusions

All the firewalls in this study have at least one rather serious flaw. This is rather sad, since it means that a lot of people are using software that they don't understand, or that does strange things.

For example, there are cases where it is very unclear when changes actually apply. Most of the firewalls are also rather bad at explaining the extent of its rules, e.g. when a user adds a rule, what premissions do the application get? Another common flaw is that the help system uses different terminology than the interface, and that there are mismatches in structure. Also, the logs in most of the firewalls do not quite meet our standards. In most of them, you can not control what is logged, and many of them lack filtering and sorting functionalities. Because logs are mostly used by advanced users, we believe this to be less serious.

We can definitely say that we have not found any personal firewall that we would recommend without reservations. However, a number of the firewalls would be acceptable, since their flaws and problems are of the kind that users can learn to live with, as long as they are aware of them.

Of the free firewalls, Comodo Personal Firewall is the one that we can consider recommending. The users have to learn that it is actually necessary to open specific ports in addition to the application rules, when setting up a server, but once they are aware of the need for this, it is not very difficult.

The commercial firewalls were generally not better than the free ones at all. We do not see any clear advantage with using any of these, since they contain the same types of omissions, errors, bad design and quirks as the freely available firewalls.

## References

[1] Giacobbi, G., *The GNU Netcat Project*, February 27, 2004. http://netcat.sourceforge.net/. Accessed on April 20, 2006.

[2] Langa, F., *Langa Letter: Readers Rate Desktop Firewalls*, November 7, 2005. http://www.informationweek.com/story/showArticle.jhtml?articleID=173402915. Accessed on April 28, 2006.

[3] Markus, S.H., *Personal Firewall Reviews*, April 05, 2006. http://www.firewallguide.com/software.htm. Accessed on April 28, 2006.

[4] Nielsen, J., *Ten Usability Heuristics*, 1994. http://www.useit.com/papers/heuristic/heuristic_list.html. Accessed on March 22, 2006