Usability and Security of Personal Firewalls

Almut Herzog[1] and Nahid Shahmehri[1]

Dept. of Computer and Information Science, Linköpings universitet,Sweden
{almhe, nahsh}@ida.liu.se

Abstract. Effective security of a personal firewall depends on (1) the rule granularity and the implementation of the rule enforcement and (2) the correctness and granularity of user decisions at the time of an alert. A misconfigured or loosely configured firewall may be more dangerous than no firewall at all because of the user's false sense of security. This study assesses effective security of 13 personal firewalls by comparing possible granularity of rules as well as the usability of rule set-up and its influence on security.
In order to evaluate usability, we have submitted each firewall to use cases that require user decisions and cause rule creation. In order to evaluate the firewalls' security, we analysed the created rules. In addition, we ran a port scan and replaced a legitimate, network-enabled application with another program to assess the firewalls' behaviour in misuse cases. We have conducted a cognitive walkthrough paying special attention to user guidance and user decision support.
We conclude that a stronger emphasis on user guidance, on conveying the design of the personal firewall application, on the principle of least privilege and on implications of default settings would greatly enhance both usability and security of personal firewalls.

1 Introduction

In times where roaming users connect their laptops to a variety of public, private and corporate wireless or wired networks and in times where more and more computers are always online, host-based firewalls implemented in software, called *personal firewalls*, have become an important part of the security armour of a personal computer. Typcially, personal firewalls control both incoming network connections—to defeat unsolicited connection attempts and host explorations—and outgoing network connections—to contain network viruses and spyware and to thwart distributed denial of service attacks by zombie machines.

Most of the time, a personal firewall runs silently in the background, but at times, it alerts its unsuspecting user of ominous, security-critical events and demands instant attention and an instant decision. This is the moment where security and usability meet. If the user, at this moment, does not take in the alert message, the firewall ends up with an ad-hoc configuration that the user will rarely take time to revise and which may be more dangerous than no firewall at all because of the user's false sense of security.

From this anecdotal scenario, one can identify a number of security and usability issues that make personal firewalls special and interesting to study:

Please use the following format when citing this chapter:

Herzog, A. and Shahmehri, N., 2007, in IFIP International Federation for Information Processing, Volume 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., (Boston: Springer), pp. 37–48.

- Personal firewalls target end users that are not security experts, yet
- the effective security of personal firewalls depends to a great extent on the correctness and level of detail of a lay user decision.
- At decision time, the lay user is typically busy with other tasks.
- A wrong decision by the user can compromise the user's privacy and computer.

However, *if* personal firewalls can address these difficult issues successfully, they could potentially serve as guiding examples of how to warn and inform user of security events, and, consequentially, also of how to explain security features to lay users. Therefore we have conducted a usability study of personal firewalls that takes the pulse of applications that must unite security and usability under the rather adverse conditions described above.

We have studied the following 13 personal firewalls for the Windows XP platform: BlackICE PC Protection 3.6, Comodo Personal Firewall 2.0, F-Secure Internet Security 2006 6.13-90, LavaSoft Personal Firewall 1.0, McAfee Personal Firewall Plus 7.0, Microsoft Windows Firewall (SP2), NetVeta Safety.Net 3.61.0002, Norman Personal Firewall 1.42, Norton Personal Firewall 2006, Sunbelt Kerio Personal Firewall 4.3.268.0, Tiny Desktop Firewall 2005 (6.5.126) (gone out of business in autumn 2006) and the free and professional versions of ZoneAlarm 6.1.744.001. According to the firewall portal `firewallguide.com`, these are the most popular personal firewalls for the Windows platform that are either available for free or as time-limited but full-featured evaluation versions.

2 Method

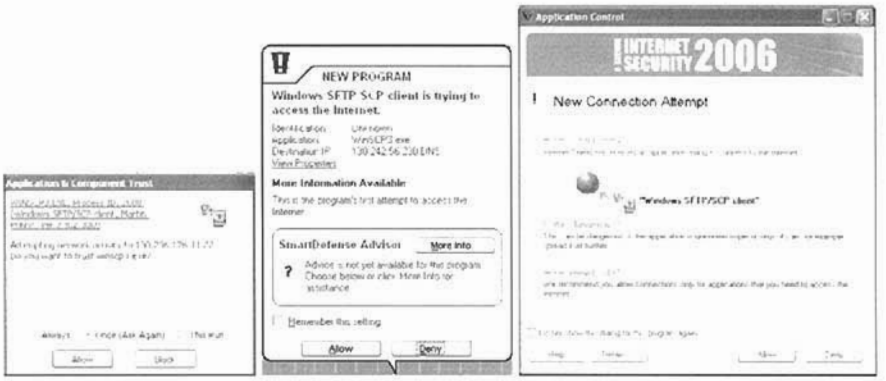
For the evaluation, we have defined two common use cases that typically require user interaction with the firewall, namely (1) setting up an application so that it has access to the Internet and (2) setting up a server on the local host so that it accepts incoming connections from exactly one host. We have also evaluated firewall behaviour for the misuse cases of port scanning and replacing a legitimate, network-allowed application with another application.

The evaluation method is the method of cognitive walkthrough [11]. Cognitive walkthrough means that the evaluator uses the program as prescribed by use and misuse cases and notes usability problems as they arise.

During the cognitive walkthrough, we have paid special attention to user guidance, user help and whether the created firewall rule grants the minimally necessary set of permissions. The firewall design with its default settings and user guidance features are the focus of this work, rather than the meticulous listing of each and every usability problem encountered.

3 Use cases

In this section we describe the findings from performing the tasks of enabling an application to access hosts on the Internet and to set up a server that can receive connections from only one host.



NetVeda Zone Alarm Pro F-Secure

Fig. 1. Alerts for outgoing connections ranging from very technical (left) to non-technical (right), from no help (left) to full help (right).

Detailed results from our study with screenshots and additional information on the firewalls' installation process, help system and log viewing capabilities can be found at `www.ida.liu.se/~iislab/projects/firewall-comparison`.

3.1 Allowing outgoing connections

Setup A personal firewall should only allow trusted applications to access the network. WinSCP (`winscp.net`) is a small application for connecting to SCP (secure copy protocol) or SFTP (secure file transfer protocol) servers. We used WinSCP to connect to a host. If necessary, we responded to the alerts of the firewall. In an alert window, we would follow the path of least resistance, choosing those answers that the interface suggested or, if no default indicated, we would choose the seemingly securest answer.

Findings 9 of 13 firewalls pop up an alert when WinSCP tries to open a network connection to the SCP server to ask the user whether to allow the network connection or not. In the alert—some example alerts are shown in figure 1—, the user can typically choose between allowing and denying the connection and whether to remember this setting for this application i.e. to automatically create a rule for this application (Comodo, F-Secure, ZoneAlarms). Some firewalls offer a greater variety of user choices. Answer alternatives for all examined firewall products are shown in table 1.

However, there are four firewall products (BlackICE, Win XP, Norton, Sunbelt) that by installation default allow any outgoing connection, either silently (BlackICE, Win XP, Sunbelt) or with an unobtrusive float alert informing the user (Norton). By design, the Windows XP firewall does not monitor outgoing connections. However, as all other firewall products do this, one wonders how many users assume that the Windows XP firewall does so, too, and feel protected even though there is no protection.

Table 1. Information available in alerts and default rule created when allowing an outgoing connection. The darker the cell background the less secure or usable is the firewall behaviour.

Product	How dangerous is it?	What shall I do?	Choice in Popup Dialog	Typical Rule When Allowing Outgoing Connection
BlackICE		Not applicable. BlackICE never alerts.		Full out and listen permissions for local applications
Comodo	Signalled by slider	"No advice available" for WinSCP. No help. Open choice.	Allow, Deny–Once, Always	Full in/out permissions. In-permission needed for the return data connection (!).
F-Secure	Generic text, see figure 1	Help and details available. Default: Allow once	Allow, Deny–Once, Always	Full out permissions
LavaSoft	No indication	No advice. No help. Default: Guesses default rules.	Allow all, Stop all, Create custom rules	Guessed custom rule
McAfee	"McAfee does not recognize this application." may be perceived as dangerous.	Help me choose-button as help. Open choice.	Grant Access, Grant Access Once, Block All	Full out and listen permissions.
MS Win XP	*No indication (only incoming)*	*Generic text, link to documentation, open choice (only incoming)*	*Allow, Deny–Ask me later (only incoming)*	Full out permissions.
NetVeda	No indication	No advice, only technical details. No help. Default: Allow once	Allow, Deny–Once, Session, Always	**Full in/out permissions**
Norman	No indication	"Tip: None" for WinSCP. General help available. Default: Allow always	Allow, Deny–Once, Session, Always	Wizard guides to rule for this port and any host.
Norton	Learn: N/A, Manual: "Medium Risk"	Learn: N/A, Manual: Alert assistant, suggested: allow always	Learning mode: no popup but informative float. Manual mode: Allow, Deny, Manual rule–Once, Always.	Notifies user that it has learnt the app with needed permissions or app-specific defaults. In manual mode, suggests full in/out permissions.
Sunbelt	Green background signals harmless to user but is only contrast to red for incoming connections.	No advice. No help. Open choice.	Default: No prompt. After change: Allow, Deny–Once, Always	Full out permissions.
Tiny	Red header signals dangerous, but the header is always red.	Limited and technical help available. Open choice between allow or deny always.	Allow, Deny–Once, Session, Always	Tight rule with host and port
ZoneAlarms	Colourcoding of alerts: yellow—outgoing, violet—listening, orange—changed application	Smart Defense Advisor has no advice for WinSCP. Default: Allow once	Allow, Deny–Once, Always	Full out permissions

The same request and what would seem to be the same user answer may result in the creation of very different rules. Some firewalls, often those aimed at technical users (LavaSoft, Norman, Tiny), create rather tight rules. Other firewalls, often those aimed at lay users, create a rule that gives full permission to the application to initiate (F-Secure, Sunbelt, ZoneAlarms) and sometimes even to listen for socket connections (BlackICE, Comodo, McAfee) and, still worse, to also accept connections (NetVeda, Norton's suggestion in manual mode).

3.2 Allowing software to receive incoming requests

Setup A firewall should not allow any host to connect to a local server. We tested this by running the Cerberus FTP (file transfer protocol) Server, and trying to set up the firewall so that Cerberus could accept connections and FTP commands from only one, named host.

Findings From the overview presented in table 2, one can roughly identify four ways of handling server applications and incoming traffic to them.

1. Some firewalls generate *alerts when applications start listening* for connections. By default, this is done by Comodo, F-Secure, the ZoneAlarms and Norton. In a default installation Norton does not alert but announces with a float that it has learnt that the FTP server is listening.
2. Those firewalls that do alert when an application starts listening, often also *allow any host to connect* as a default behaviour. The user decision to allow an application to listen also implies for these applications the permission to let any host connect. However, NetVeda, without showing a specific listen alert, also allows connection by any host. This comes from the peculiarity of the Cerberus server that it first does a DNS lookup. This lookup is caught by NetVeda and if allowed by the user, who only sees this as a simple outgoing connection, implies full permissions for Cerberus, i.e. not only to connect out, but also to listen for and accept connections from any host.
3. Firewalls that *silently drop incoming connections to open ports* are BlackICE, Comodo, McAfee and Sunbelt. For users that rarely interact with their firewall it may be unclear why clients cannot connect since the firewall usually runs silently in the background. In misuse cases, this is good; but when the user cannot determine why an authorised client cannot connect, the firewall has become a hinder for the user's primary task of setting up an FTP server.
4. The fourth strategy is to *generate an alert for incoming connection attempts.* Norman alerts upon connection attempts to *any* port. If the computer is exposed to port scanning, the user is swamped by alerts. By default, LavaSoft and Tiny alert upon a connection attempt to an open port. From this alert, the user can create a fine-grained rule. The Windows XP firewall normally alerts upon connection attempts to open ports but Cerberus modifies the XP firewall rules so that Cerberus is trusted by the firewall and no alert is caused. That an application can modify firewall rules and grant itself additional permissions renders the firewall useless. However, all Windows applications that run from an administrator account can change firewall rules if only they know where and for which product.

Application-specific rules that restrict which host can connect on which port can be set up with LavaSoft, Norman, Norton, Sunbelt, Tiny and ZoneAlarm Pro. The other firewalls have coarser rule granularity, the worst case being to

Table 2. Personal firewall default behaviour when trying to set up an FTP server that should allow only one host to connect to it. The darker the cell shading the less secure or usable is the firewall.

Product	Type	Listen Alert	Default Behaviour (if Listening Allowed)	How to allow only one host to connect	User Guidance
BlackICE	3	N	Silently blocks all incoming traffic also to open ports	Manually open port for host.	None
Comodo	1, 3	Y	Silently blocks all incoming traffic also to open ports	Manually open port for host.	None
F-Secure	1, 2	Y	Any host can connect.	Manually open port for host and deny for others. App-based rules should be possible but did not work for us.	None
LavaSoft	4	N	Alerts upon connection attempt to open port.	From alert, open port for host to app.	Alert guides through creation but by default uses ephemeral port in rule.
McAfee	3	N	Silently blocks all incoming traffic also to open ports	Either manually open port (for any host) or trust host (with any connection).	Last event hint in main interface.
MS Win XP	4	N	Creates alert upon connection attempt to an open port.	Either manually open port for host or open app for host.	None
NetVeda	2	N	If outgoing connection is allowed, also incoming is silently allowed and any host can connect (!).	Not possible. Interface is prepared for setting up finer-grained rules but the choices are so limited that our case could not be set up.	None
Norman	4	N	Alerts upon connection attempt to *any* port.	From alert, open port for host.	Wizard guides through rule creation from alert.
Norton	1, 2	*y*	*Learns* and informs (not alerts) with float that server is listening. Any host can connect.	Open port for host to app.	None
Sunbelt	3	N	Silently blocks all incoming traffic also to open ports.	Open port for host to app from alert after changing the default for this app, so that incoming connections cause an alert.	By default: None; after default change: From alert
Tiny	4	N	Alerts upon connection attempt to open port.	Restriction to one host is default behaviour.	None
Free Zone-Alarm	1, 2	Y	Any host can connect	Not possible	None
Zone-Alarm Pro	1, 2	Y	Any host can connect	Manually open port for host to app and deny for others.	None

either fully trust or distrust an application (free ZoneAlarm). Table 3 contains the details of the possible rule granularities.

We found that the most usable and most secure way to achieve the goal of setting up an FTP server and letting only one host connect to it, is presented by LavaSoft, Norman, Sunbelt and Tiny. These firewalls display an alert if an FTP client tries to connect, and from this alert, it is possible to directly create a fine-grained rule. Of these four firewalls, Tiny creates the tightest rule with the least amount of user interaction.

User guidance for this task was nonexistent in many firewall products. By 'nonexistent' we mean that to find out how to allow the connection and only from one host, one had to either resort to exploring the firewall interface or to reading the documentation—all this under the assumption that the user would understand that it was the firewall that caused the problem! However, all firewalls that prompted for an incoming connection attempt showed good guidance by allowing the set-up of fine-grained rules from the alert.

4 Information in alerts

When the user is confronted with an alert from the firewall, there is often a surprising lack of information and guidance from the software. The user typically needs to know how dangerous the current situation is and what he or she should do.

Of the 9 firewalls that show an alert, the alerts of two firewalls (NetVeda and Tiny) do not contain the product name or the word 'firewall', thus leaving the user clueless as to which application caused the message.

Firewalls spend little effort on classifying and explaining the severity of an alert. Of those 12 firewalls that can be made to raise alerts, only three (Comodo, F-Secure, Norton in manual mode) attempt to classify the severity. Comodo shows a slider, F-Secure some generic text under the heading "Is this dangerous?" (see figure 1); Norton classifies the risk as low, medium and high. The other firewalls identify whether it is an incoming or outgoing connection by way of colour coding, symbols or text in the window but do not indicate whether this particular connection attempt is dangerous.

Astonishingly, no firewall attempts to explain the port number to the user other than possibly translating the port number into a—for many people—equally cryptic service name such as '22' to 'ssh' and '80' to 'http', but with no explanation whether 'ssh' or 'http' are potentially dangerous services or are to be expected from an application. Only Norton in manual mode makes a distinction in response alternatives if the outgoing connection is a DNS connection for resolving host names.

Also the host *name* is not readily available in alerts that display that information, even though we entered the host name for the SSH connection using a name, not an IP address. This makes it practically impossible for a user to verify whether the application is connecting to the desired host or not.

The firewalls Comodo, LavaSoft, NetVeda and Sunbelt do not provide access to any help from the alert (Tiny provides some limited help). If details are given in the alert, these are often technical such as paths, IP addresses, protocols

and/or ports. Other firewalls keep technical details deliberately away from users (F-Secure, McAfee, Win XP for incoming, Norton in learning mode). User guidance is usually available in the form of online help and context-sensitive help (not in NetVeda, Comodo only partially, Tiny accesses online help over the Internet and has limited context-sensitive help). Some firewalls (BlackICE, especially McAfee) use guiding or explanatory texts in windows and alerts so that the user finds the necessary information without consulting the help system.

5 Misuse cases

We created two misuse cases to test the default reaction of the firewall. It was not our purpose to seriously test the security solution of the firewall, but to see the firewall's presentation of the situation to the user. In-depth security testing of personal firewalls with tools such as `grc.com` is documented on e.g. `firewallguide.com` and we refer to that site for more details on possible security flaws in the blocking behaviour of firewalls.

5.1 Stealth

Setup: A personal firewall should block connection attempts to all ports unless stated otherwise by a firewall rule. To test how the firewalls reacted to incoming packets, we used Netcat (`netcat.sourceforge.net`). For the basic tests we ran sequential port scans on the low port ranges. In this test, we were interested in the default behaviour for unsolicited incoming connection attempts.

Findings By default, 12 of the 13 firewall products block all closed ports. Of the 12, only Norman shows prompts on every connection attempt. With Norman, this behaviour is difficult to change. One is either prompted for everything or for nothing, or one must create rules. Other firewalls can be configured to alert on certain types of incoming traffic. Upon port scanning, LavaSoft and Sunbelt blocked our attacking host. Tiny is the only firewall that failed to block incoming connection attempts by default because it had automatically put all network interface cards (NIC) in its so-called "safe zone", where port blocking is not default behaviour. Had it correctly placed the NICs in the Internet zone, port blocking would have been the default.

5.2 Fooling the firewall

Setup: Firewalls that base their security rules on trusted software are vulnerable to malicious programs that masquerade as trusted software. We replaced a legitimate firefox.exe with a renamed version of winscp.exe, making sure that no firewall rules for WinSCP existed and that Firefox was allowed to connect to the Internet.

Findings Only the Sunbelt Kerio firewall was fooled by this simple masquerading attempt. Norton and Tiny show the spoofed Firefox as a new application, thus they do not recognise (or verbalise clearly) that they have a rule for the genuine Firefox application. The remaining 10 firewalls detect that Firefox

has changed and show a special alert saying that a program which has changed is trying to access the network.

User guidance in this issue is very difficult and not handled satisfactorily. Users of Norton and Tiny could easily believe that the Firefox rules had somehow gone amiss and must be reset. Users of other firewalls are faced with an alert that announces the change but still could easily believe that Firefox was updated and that the rule must be reconfirmed.

6 Summary and recommendations

In this section, we highlight findings, suggest products for certain user groups as shown in table 3 and present recommendations that would render firewalls more usable and secure.

Some firewalls—Comodo, LavaSoft, NetVeda, Norman, Sunbelt—target technical users that are not deterred by IP and port numbers in alert windows. Of these firewalls, Tiny is the one that guides the technical user to the strictest rule with least overhead and also allows additional, advanced application monitoring.

Some firewalls—F-Secure, McAfee, Norton, ZoneAlarm—are part of a product suite and specifically target users with little or no knowledge about network security. Their drawback is that they do not always support the possibility of fine-grained rules and may only be partially of interest for risk-taking Internet users.

This evaluation has shown that there are many different design alternatives and default settings for personal firewalls. One clean design is shown by the LavaSoft and Tiny firewalls. They alert on outgoing connections as well as on incoming connection attempts to open ports. They do not alert when a service starts listening as this is not security-critical in their design. From an alert, they guide the user through the creation of a fine-grained rule (LavaSoft) or create a tight rule by default (Tiny) and thus achieve tight security.

There are a number of guidelines, e.g. [8, 4, 16], which deal with security and usability. Also more traditional usability guidelines such as [11, 13, 10] must be considered. For the firewall domain we could identify the following specific issues that should be addressed for increased usability and security.

- *Firewalls must make themselves more visible.* This can be achieved through the animation of their logo in the system tray (as shown by Sunbelt and ZoneAlarm). But it may also mean showing small informative floating windows close to the system tray indicating certain actions of the firewall that did not trigger user interaction and displaying the firewall name and logo in every alert that it creates.
- *Encourage learning.* Firewalls spend very little effort in teaching users about network security. All firewalls could be made to show IP address and port; some translate the port number into a service name. But no firewall tries to explain the specific service or shows the host name together with the IP address.
- *Give the user a chance to revise a hasty decision later.* Users that are busy with a primary task take security chances to get the primary task done. However, they may need a reminder, maybe by using a floating window or bubble, of their security settings.

Table 3. Summary of the firewalls including the supported granularity of rules, suitable user group and a concluding comment. The darker the cell shading the less secure or appealing is the firewall.

Product	Product Type	Granularity	User Group	Comment
BlackICE	Commercial	Coarse–medium	Tech user that wants a network monitor rather than a firewall	After installation, scans for and adds all applications on the local host with Allow-permissions to its rule base.
Comodo	Free	Medium	Tech user that wants an appealing user interface	Needs permission for back connection on high ports, prompts for all Windows default applications.
F-Secure	Commercial, part of suite	Medium-fine	Lay user	Tidy alert window with few choices. Application-based rules difficult.
LavaSoft	Commercial	Fine	Tech user with time to set up fine-grained rules	Guesses application type from connection attempt. Ephemeral port numbers in suggested rules.
McAfee	Part of suite	Medium	Playful lay or tech user	High fun factor with tracing events, good informational text in windows.
MS Win XP	Built-in	Medium(in), None (out)	Better than nothing but not good enough	Allows only user control for incoming traffic, not outgoing.
NetVeda	Free	Coarse–medium	Tech user	Fine-grained rules do not work satisfyingly yet. Yes to outgoing implies that the application can listen and respond to incoming events.
Norman	Commercial	Fine	Tech user with a lot of time	Longish wizard is default for all connection attempts.
Norton	Commercial, part of suite	Fine	Lay user or tech user with patience to explore interface	Difficult to access and modify rules.
Sunbelt	Commercial	Fine	User that can change default setting	Default after installation allows all local applications to access the network, fooled by replaced legitimate application.
Tiny	Commercial	Fine	Tech user that wants to learn more about applications	Allows also fine-grained monitoring of other security-critical actions. Alert info very technical, little help.
Free ZoneAlarm	Free, part of suite	Coarse	Lay, low-risk user	Simple user interface, good as a first contact.
ZoneAlarm Pro	Commercial, part of suite	Fine	Lay or tech user	Fine-grained rules not possible from alert: User must remember to refine rule later.

- *Prefer handling security decisions at once.* In order to set up tight rules or set up the Cerberus server, some firewalls require their users to access the firewall main interface. This is a burden to the workflow of the user and should be avoided if possible.
- *Enforce least privilege* wherever possible. The firewalls of Tiny and LavaSoft show that fine-grained rule set-up is feasible without much user burden.
- *Indicate severity, indicate what to do and show the created rule.* In an alert, users need to know how dangerous the attempted action is, what they can and should do, and receive feedback as to which rule was actually created by the firewall.

7 Related work

While usability evaluations of security applications abound—e-mail software with encryption [14, 5], Internet banking [6, 12], Internet Explorer [1], Outlook Express [3], setting up security policies for Java applications [7]— the evaluations that fit best into our context are two previous evaluations of firewalls. Johnston and others [8] have evaluated the first version of the Windows XP firewall and arrive at specific usability issues that may deter users from building trust in the firewall. The authors believed that the following version, roughly the version that we had in our test, would remedy many of the problems they had identified, but the XP firewall still does not rate high on our evaluation. Professional firewall products for network administrators also exhibit usability problems [15]. Technical terms are not explained and terms such as 'inbound' and 'outbound' can be used in confusing ways—we found such a mix-up in Comodo and Norman. In fact, if the target user is a security professional, usability issues may be even more neglected by designers than if the target user is a security novice [2].

Plenty of firewall reviews can be found online, e.g. through the portal `firewallguide.com`. However, many of these are only short reviews, test the firewall for security only using the e.g. web-based firewall tests like ShieldsUp (`grc.com`) or other automated tools or ask their audience for ratings. A vulnerability test for firewalls is described in [9].

8 Conclusion

In this article, we have presented the evaluation of 13 free and commercial personal firewall products. We have evaluated the products by means of a cognitive walkthrough of the use cases of allowing a local application to access the network and setting up a local server and allowing it to receive connections from only one host. Two misuse cases—port scanning and replacing a legitimate version of an application with a faked one—showed how the firewalls react to potential attack situations.

A winning firewall could not be identified; all firewalls had one or more shortcomings. Personal firewalls are generally good at protecting ports of the local host from unsolicited connection attempts from the Internet. However, they are generally poor at informing users and creating security awareness.

More than half of the evaluated firewalls do not support the set-up of truly fine-grained rules.

If a user switches between firewall products, she cannot anticipate what the default behaviour and its security implications will be. User guidance could remedy this but firewalls spend little effort on conveying their design, default settings or concepts of network security to their users. We conclude that this failure is a notable obstacle to usable and secure personal firewalls.

References

1. S. M. Furnell. Using security: easier said than done. *Computer Fraud & Security*, 2004(4):6–10, April 2004.
2. S. M. Furnell and S. Bolakis. Helping us to help ourselves: Assessing administrators' use of security analysis tools. *Network Security*, 2004(2):7–12, February 2004.
3. S. M. Furnell, A. Jusoh, and D. Katsabas. The challenges of understanding and using security: A survey of end users. *Computers & Security*, 25:27–35, 2006.
4. S. L. Garfinkel. *Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable.* PhD thesis, Massachusetts Institute of Technology, May 2005.
5. D. Gerd tom Markotten. *Benutzbare Sicherheit in informationstechnischen Systemen.* Rhombos Verlag, Berlin, 2004. ISBN 3-937231-06-4.
6. M. Hertzum, N. Jørgensen, and M. Nørgaard. Usable security and e-banking: Ease of use vis-à-vis security. In *Proceedings of the Annual Conference of CHISIG (OZCHI'04).* `http://webhotel.ruc.dk/nielsj/research/papers/eBanking-ajis.pdf` (visited 3-Aug-2005), November 2004.
7. A. Herzog and N. Shahmehri. A usability study of security policy managment. In S. Fischer-Hübner, K. Rannenberg, and S. L. Louise Yngström, editors, *Security and Privacy in Dynamic Environments, Proceedings of the 21st International Information Security Conference (IFIP TC-11) (SEC'06)*, pages 296–306. Springer-Verlag, May 2006.
8. J. Johnston, J. H. P. Eloff, and L. Labuschagne. Security and human computer interfaces. *Computers & Security*, 22(8):675–684, December 2003.
9. S. Kamara, S. Fahmy, E. E. Schultz, F. Kerschbaum, and M. Frantzen. Analysis of vulnerabilities in Internet firewalls. *Computers & Security*, 22(3):214–232, April 2003.
10. N. Leveson. *Safeware: System Safety and Computers.* Addison Wesley, 1995.
11. J. Nielsen. *Usability Engineering.* Morgan Kaufmann Publishers, Inc, 1993.
12. M. Nilsson, A. Adams, and S. Herd. Building security and trust in online banking. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI'05)*, pages 1701–1704. ACM Press, April 2005.
13. B. Shneiderman and C. Plaisant. *Designing the User Interface.* Addison Wesley, 4th edition, 2004.
14. A. Whitten and J. D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium (Security'99).* Usenix, August 1999.
15. A. Wool. The use and usability of direction-based filtering in firewalls. *Computers & Security*, 23(6):459–468, September 2004.
16. K.-P. Yee. User interaction design for secure systems. In *Proceedings of the International Conference on Information and Communications Security (ICICS'02)*, pages 278–290. Springer-Verlag, December 2002.