Firewall or FireFolly – An initial investigation into the effectiveness of Personal Firewalls in securing personal computers from attack.

Jeshua Yee

School of Computer and Information Science
Edith Cowan University
E-mail: jyee@student.ecu.edu.au;

ABSTRACT

With the increase in the use of Personal Computer (PC) firewall, this study looks at the security features provided by eight PC firewall; they are BlackICE, Deerfield, Kirio, MacAfee, Outpost, Sygate, Tiny and Zonealarm. The Nessus network scanner was used to probe these systems in a variety of configurations. The paper discusses the results and their implications for users of this new range of software.

Keywords: Personal Computer firewall, Nessus network scanner, firewall security features

INTRODUCTION

Today, with the advent of Personal Computer (PC), a PC no longer acts as a mere word processor or for calculating simple spreadsheets. It has now become an important tool for communications, program organisation and business processes in traditional places of commerce and enterprise. In addition, many of the company's personnel work regularly by logging on the company's network remotely (Yasin, 2000). Therefore, a malicious attack on a home PC could have a detrimental effect on the user's daily routine, business and financial well-being (Hulme, 2002). This problem is further compounded with the increasing deployment of affordable broadband in the form of cable and ADSL services. These services provide reliable 24-hour high bandwidth connectivity to the Internet (Fleishman, 2001; Goldsborough, 2002; Janss, 2000; Radcliff, 2001).

With the increase in hacking incidences (Ravendran, 2002), small and large organisations alike are moving to protect their PCs and the valuable data they contain (Clark, 2001; Goldsborough, 2000a; Schwartz, *et. al.*, 2001). This has created a lucrative market niche for personalised PC firewall products with a resultant surge in the production of PC firewall software as a result (Clark, 2001; Gani, 2002; Goldman, 2002; Harrison, 2000). These products may consist of just a simple system to filter any incoming traffic, to bundled tools that include a firewall, virus scanning, parental content control, privacy control, intrusion detection and encryption (Andress, 2001; Hummel, 2000; Yasin, 2000). Some differences between an enterprise firewall and a PC firewall are shown in Table 1.

While PC firewalls may not have the sophisticated configurations that an enterprise firewall product has, they are purported to provide strong security features that a commercial product provides (Beach, 2001). However, many PC firewall users would debate this claim (Beckman, 2001; Crouch and Captain, 2001; Dalton, 2001; Goldsborough, 2000b; Radcliff, 2001).

	Enterprise Firewall	PC Firewall
Cost	High	Low
Maintenance cost	High	Low
Skill required to operate	High to very high	Low
Size	Medium to large	Small
Host software	Minimalist Configuration	Often contains other third parties software and services

Table 1: The differences between an enterprise firewall and a PC firewall
(adapted from Whitmore (2002) and Framingham (2001))

This project aims at examining and testing the security features of a selection of PC firewall software.

METHOD

The firewalls are downloaded from the Internet and are listed in Table 2. Each is installed on a PC with Microsoft Windows 98 Second Edition Operating system. It is tested using a network security scanner, Nessus. Nessus was installed on a Redhat 7.2 Linux machine.

Product Name	Company name
BlackIce Defender 2.5 (BlackIce)	Internet Security System
Deerfield Personal Firewall 1.0.1.0 (Deerfield)	Deerfield.Com
Kerio Personal Firewall 2.1 (Kerio)	Kerio Technologies
McAfee Firewall 3.0 (Mcafee)	McAfee Security
Outpost Firewall 1.0 (Outpost)	Agnitum
Sygate Personal Firewall Pro 5 (Sygate)	Sygate Technology
Tiny Personal Firewall v 2 (Tiny)	Kerio Technologies
ZoneAlarm 2.6 (ZoneAlarm)	Zone Labs

Table 2: Firewalls tested in this study

Nessus is a free software written by Renaud Deraison and Jordan Hrycaj of Nessus Consulting SARL in France (Danielyan, 2001). This software is chosen for its robustness and it is a true client and server application. It has a neat graphical interface that provides an easy-to-use and convenient front-end to the system. Its modular design allows Nessus to be updated easily on a daily basis. In addition, Nessus has a special scripting language, called the Nessus Attack Scripting Language (NASL), which is used to describe vulnerabilities and effects of attacks. (Danielyan, 2001, Daraison, 2000). The program also works in conjunction with NMAP (Fyodor, 1998) using operating system TCP/IP fingerprints to identify systems and whilst providing ping and scan support.

These firewalls were tested on their default settings, minimum settings and maximum settings. Finally, in their default settings, these firewalls are then tested with a popular instant communication software, ICQ, and point-to-point software Bearshare.

RESULTS

Nessus ranks each security weaknesses according to the following Table 3 (Note: Nessus has another risk category also called *Security hole* with "Serious" risk factor. It is more critical than the "high" risk factor. However, this risk category is not included in Table 3 because none of firewall products reached this level):

Risk Category	Risk Factor
Security hole	High: there is security weakness and a hacker is able to breach the security barrier
Security warning	Medium: there is security weakness, however, a hacker would need to use more sophisticated skills to breach the security barrier
Security notes	Low: A difficult attack to implement or low real threat

After each complete scan, Nessus would list out the number of risk category as well as itemise each risk or vulnerability found. Where possible it provides suggestions or directs the user to URLs that contain counter measures and fixes. With only the Windows 98 Second Edition Operating System installed, the number of risk category for each firewall is listed in Figure 1. Figure 2 shows the number of risk category with ICQ or Bearshare installed

Figure 1 reveals that at minimum settings, all firewalls have security flaws that are equivalent to a PC that has no firewall installed. When the security level is set to maximum, all firewalls, except Kirio, successfully protects the PC from an intruder's probe. At default settings, Deerfield does not show any difference from the baseline. Outpost, Sygate and Zonealarm does not have any detected security flaws. McAfee Personal Firewall receives a security note. Kirio and Tiny does not fix the security hole. In addition, when compared with the baseline, Tiny scores high for security warnings. At default settings, Kirio produces the same security weakness as when its security level is set to maximum (Note Outpost has only one setting).

Figure 2 shows that, apart from the Outpost, Sygate and Zonealarm systems, installing ICQ or Bearshare does not affect the security performances of the firewall when their security levels are set at default. With ICQ installed, Outpost and Sygate receive a security note. Installing Bearshare affects some of the firewall security features; Sygate produces a security note; Zonealarm produces the same number of security holes and warnings as a PC not installed with any firewalls.

DISCUSSION

With the exception of Kirio, none of the firewalls revealed any security weaknesses when it is installed, at maximum settings, along with the operating system. This suggests that with the operating systems alone, the firewall is providing adequate protection from an intruder trying to hack in through the Internet. At default level however, Deerfield, Kirio and Tiny does not eliminate the security holes, but did cause a reduction in the security warnings. Predictably, these security weaknesses are present even after installing ICQ or Bearshare. The detected security holes and security warnings expose the PC to possible attack from the Internet.

Installing ICQ or Bearshare have measurable negative impacts on McAfee, Outpost, Sygate and Zonealarm firewall. This suggests that the installation of third-party softwares can compromise the security integrity provided by the PC firewalls. Furthermore, the adverse impact Bearshare has on Zonealarm firewall suggests that installing the wrong software can in fact, nullify the security provided by the firewall.

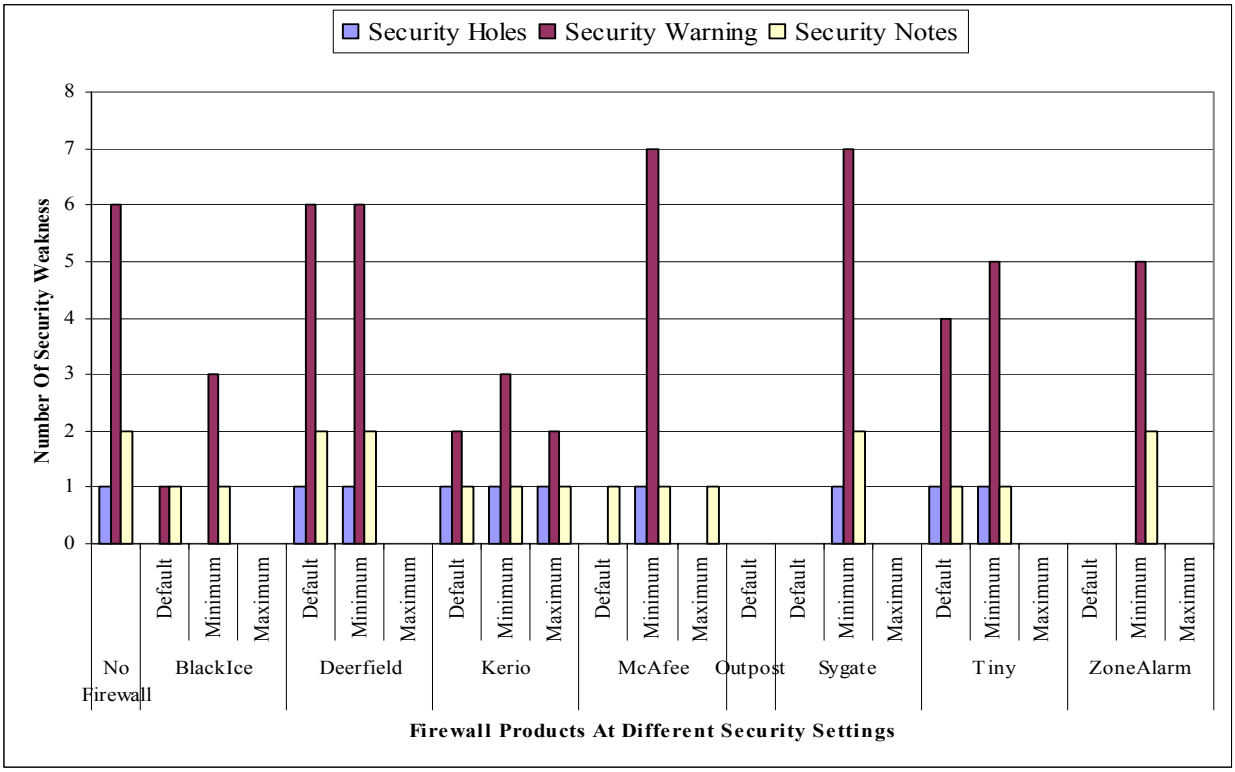

Figure 1: Result of scanning with only base operating system installed

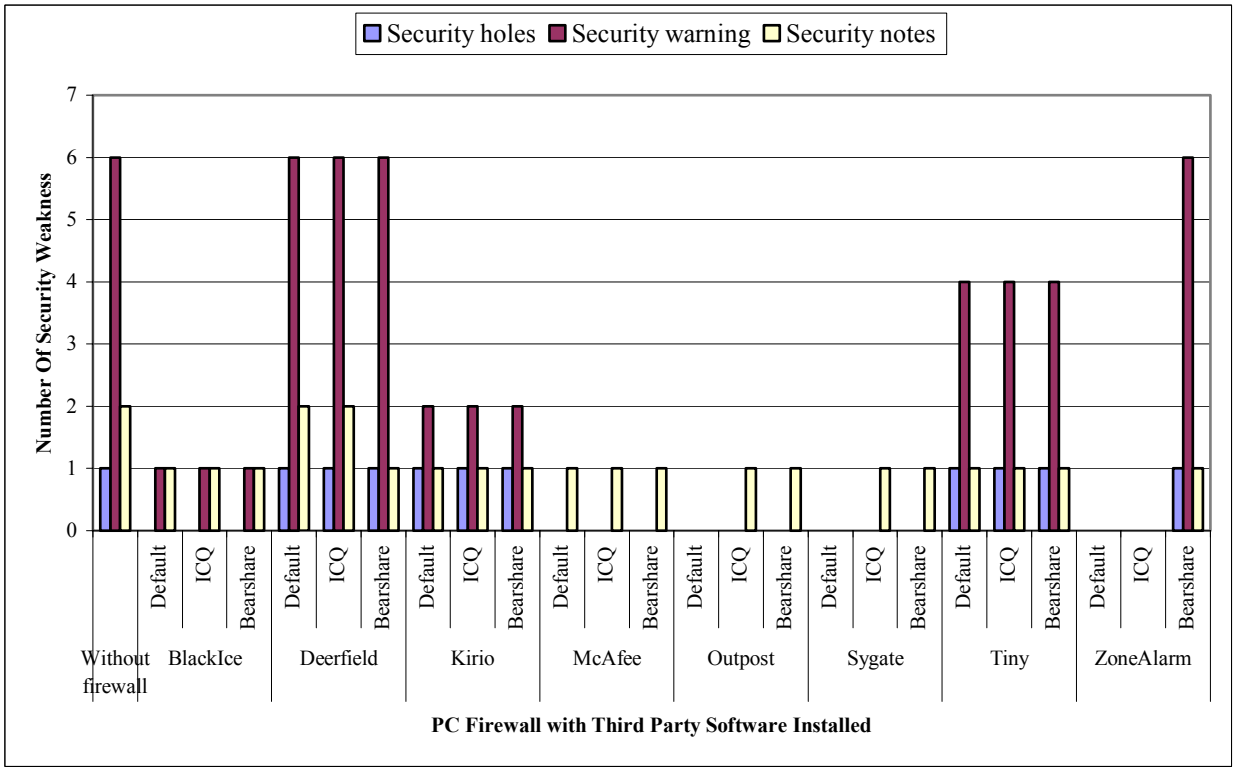

Figure 2: Result of scanning with ICQ or Bearshare installed

The findings in this report indicate that the securities of the PC firewalls need further research. Some questions that needed answers include:

1. Would installing a third party software compromise the security integrity provided by the PC firewall, even when its security level is set to maximum?
2. Would installing two or more third party packages have a compounding and negative impact on the security of the firewall?

These questions warrant further investigations because this current study indicates that, at default settings, third party softwares have negative impacts on the security integrity of the PC firewall. A PC may often contain many third party packages. In addition, setting the firewall to maximum may imply to the user that they are fully protected. However, this study has gone some way to suggesting that this may in fact be misleading and may give the PC-user a false sense of security and safety while they are using the Internet when in fact they are open and vulnerable to attack.

REFERENCES

Andress, M., (2001). Building a better virus trap. *InfoWorld*, 23(47), 54

Danielyan, E., (2001). Introducing Nessus network security scanner. *Inside Solaris,* 7(6), 3-5.

Beach, B., (2001). Cyberarmor personal firewall interoperates with contivity. *Computer Security Update*, 2(7), 1.

Beckman, M., (2001). Norton personal firewall 1.0. *Macworld*, 18(5), 70.

Clark, E., (2001). Special reports: Securing the new perimeter. *Network Magazine*, 16(6), 41.

Crouch, C., and Captain, S., (2001). Is your PC safe from the enemy within? Updates plug firewall leaks. *PC World*, 19(4), 56

Dariason., (2000). Nessus. [Internet]. Available from: <http://www.nessus.org/intro.html>[Accessed 18th March, 2002]

Dalton, C., (2001). Getting personal with firewalls. *Network Magazine*, 16(1), 100-106

Fleishman, G., (2001). Broadband security at home. *Fortune*, 143(10), 278.

Framingham, M., (2001). Firewall for the frugal. *InforWorld*, 23(21), 86

Fyodor. (1998). Remote OS detection via TCP/IP stack fingerprinting. [Internet]. Available from: <http://www.insecure.org/nmap/nmap-fingerprinting-article.txt>[Accessed 20th March, 2002]

Gani, H. M., (2002). Considering home networking. *Computime Malaysia*, 1.

Goldsborough, R., (2000a). Personal computing: Keeping hackers away with personal firewall. *Commercial Law Bulletin*, 15(3), 36-37

Goldsborough, R., (2000b). Firewalls are becoming essential. *Computer Dealer News*, 16(19), 21.

Goldsborough, R., (2002). Protecting yourself against cyberterrorism. *Link-up*, 19(1), 1.

Goldman, Lee, (2002). A fortune in firewalls. *Forbes*, 169(6), 102-108.

Harrison, A., (2000). Corporate security begins at home. *Computerworld*, 34(10), 14

Hulme, G., (2002). Help to combat the next big blended threat. *Informationweek*, 882, 18

Hummel, R., (2000). How it works: Personal firewalls. *PC World.Com*, 1-3

Janss, S., (2000). Frontier defence: Personal firewall software. *Network World*, 17(32), 42-46
Radcliff, D., (2001). Firewalls reach out. *Computerworld*, 3(13), 64-65

Ravendran, A., (2002). Dealing with security threats. *Computimes Malaysia*, 1.

Schwartz, E., Fonseca, B., Neel, D., Lee, S. and McCarthy, J., (2001). Security concerns top agenda. *InfoWorld*, 23(46), 17-19.

Whitmore, S., (2001). Asiaweek: Security: Keeping hackers at bay; Home firewall can protect your PC from attack. *Asiaweek*, 19, 1.

Yasin, R., (2000). Telecommuters on security alert – Specialised firewalls, intrusion systems fortify always – on connections. *Internetweek*, 812, 43-46.