Global Information Assurance Certification Paper

Personal Firewall: Pro's and Contra's

Pavel Epifanov
Version 1.0
16 November 2000

Introduction

The firewall market is booming now. There are many articles with reviews and comparison of different firewall products. This article is different. It tries to help you in answering a question: "Do I really need a personal firewall now?" There are also threats and risks analyses inside.

It based on assumption that you already know what the personal firewall is. The best time to read this critical article when you finished with an optimistic firewall review or any firewall product' advertisement.

The article is intended more for beginners than for experts.

Please check the Resources section for the real names of existing products.

Risk Analysis

First, you should be an active Internet user. If all you do is sending and receiving e-mail then you are not exposed to the most of risks below.

Otherwise you should consider following threats:

1) Intrusion on your PC with one or many goals:

a) To steal confidential information
Somebody might want to use the Internet connection you paid for. Program licenses or your access codes to bank accounts could be interesting for certain people. At the end an intruder might want some confidential file like latest business plans which you took home to finish.

b) To use resources of your PC for illegitimate purposes
If you have a permanent IP address then your computer with large harddisk could be used for storing hacking tools, child pornography and other dangerous content. This could be done for intruder' convenience or with the purpose to abuse you.

c) Use your PC as a launch pad for new scans and attacks
As soon as your network connection is perfect and fast you are a very attractive target because your PC can be easy used for hiding the real attacker personality. In fact only most stupid of them will do large scans or attacks from their own PCs. This becomes the most popular reason for break-in.

d) Destroy your data
There is a little chance of it but it could be just a sick person who likes to destroy data.

2) Carry an attack against you with one of the following goals:

a) Test new intrusion or attack techniques
b) Shutdown your PC like a game

3) Use your PC for indirect attacks and scans

There are several complex scan and attack techniques, which require the third party to carry them on. Your PC does not need to be broken in. In this case the unsecured known holes in network protocols are used.

Lets prioritise the risks for the individuals corresponding to these threads:

I. Legal investigation of illegal PC use

To my opinion this is the most serious risk because your name could appear in criminal records or your company may have its image damaged. This is most serious risk but the chance of it is quite low at this moment. I haven't heard about any such attacks yet.

II. Loss of confidential information

It depends on how you are using your PC. If all your passwords are stored in system files you might be affected, especially if some of these passwords are for billing or dealer systems. Oh, I hope you do not store your company' confidential documents on your home PC (or on your laptop) in clear (unencrypted) form? Many successful attempts were registered in the past to steal Internet passwords and access codes. Please be aware of it.

III. Time, money and information losses due to recovering your PC

After the intrusion is noticed, you should recover your PC. This might include the restoration from recent proven backup or complete re-installation of OS from original distribution. If you make backups on regular basis than your losses could be slim. On my experience not many of the Windows home users have a fresh backup. It means that almost all your data including e-mails and Internet bookmarks would be lost unless you know how to save it. This risk is not so dangerous as the first, but very inconvenient and happens much more often.

IV. Unavailability of the PC

If you do have an attack launched against you there is little chance that you can continue using a PC. It would be frozen, restarted of just terribly slow. This is not a problem for most of the Internet users who are experienced with often slow Internet.

V. Use of your PC(s)

Nobody likes it than somebody breaks in his computer and uses it or computer virus infects it. This risk is more about moral losses and fear.

Solutions

There are some standard solutions for securing computers in IT area. Let see how they can be applied for our case.

A. Backup data and system configuration.

This is the best coverage for risk III. You may have to invest some money to install a backup device for your PC or for the home network. To my opinion the backup device should be in the standard home PC configuration when it is not possible to backup the PC to a set of floppies anymore.

B. Install recent patches for your PC

Following this traditional way you could keep an OS and programs on your PC in an up-to-date state. This is a precondition of reasonably secure computer. And there is no replacement for this process, sorry. It is a known fact that most of the breaks even happened are with computer systems, which weren't updated in time. Following this way you will eliminate risk V.

C. Tuning OS configuration in a secure manner

Many security professionals and organisations are spending a lot of time to develop recommendations "how to secure <something>". Such papers are freely available on Internet Web sites and in books. You just need to find a proper one and do it. For Windows 9x it is the only several small steps to do. Every computer user can follow recommendations. The risk of intrusion (V) and corresponding risks would be reduced greatly if you do it. This is really the best action to do! Only a very small set of Operating Systems comes with reasonable secure configuration out-of-the-box.

D. Legal advice

If you have a high position in a society or you do have very powerful competitors so you might afraid of intrusion into especially your PC with the goal to abuse you or your company. Then you have to visit your lawyer to discuss your legal risk (I). You might need to invest some money into secured and reliable network solution or just decide that you are going to have no home Internet connection at all.

E. Keep your PC off the Internet.

Please consider the PC connected to Internet as a half-opened door. If you close it then you would have no risk at all. Now the situation on Internet is quite dangerous. Should you keep your door closed when you don't really need it if you are not sure about how good your protection is?

F. Integrity audit.

Unix users for a long time are enjoying integrity checkers. Not many solutions are available for Windows platform. You also have to carry on with a regular complex job to review all changes on your computer systems. This is the best way to ensure about successful intrusion or virus attempts.

G. Special protection tools

Only here we come to tools like firewall. There are many of the hardware and software solutions available. They are both not very cheap on a long run. They also do not provide a guarantee about level of protection. Having them installed you will feel at least protected. Please check the next section (Use of personal firewall) for the detail analysis.

H. Don't install malicious or untrusted software

This is the point, which most of the people forget. Why should somebody to spend a lot of time and effort to break into your computer and install a Trojan program? It is usually enough to send you a "Love email" with Trojan inside or an email with "recent security patch". After you believe to him and execute an attachment his goal is reached in a much simple way and you have installed the backdoor or virus on your computer by your own hands! You'll better be paranoid enough about any program or email attachment you receive without special request. No one antivirus program could protect you against rare or new virus, or Trojan program, especially in case that it was modified for you only. It is much easy just to purge such e-mail or program without a long check.

J. Isolate the Internet PC

The standalone PC for Internet only (and for games too) might be a proper solution. You would eliminate the risk related to confidential information loses and the recovery process for such PCs would be faster and easy. Many large organisations today follow this way of protection. If you are not able to install a separate PC then the installation of several copies of an OS on a single computer could be a solution. A program called "boot manager" will help you to load either "Internet OS" or "Banking OS". This is not the complete protection but it would reduce risks with information losses and PC recovering.

Use Personal Firewall as a solution

The producers of personal firewall solutions are often promising a "total" solution. Let look what their products are offering and what the major downsides are.

= Block incoming connections and "hide" your PC from Internet.

Most of the products can do so. The first problem is a configuration, which is quite complex for a user. The second problem is that many of them come in combination with Intrusion Detection System (IDS). It means that most products are going to notify you about ***each*** scan attempt. This is very annoying indeed.

= Block outgoing connections from your PC to Internet.

Depending on a product this feature can be more or less advanced. It is

really hard to configure this feature in a proper way (to keep existing applications running well). But the only case you really need to do it is when you are infected by virus or Trojan. It could be also useful for analysing the network traffic by advanced users but we are talking about regular people. This feature usually creates many notifications from all applications on your PC and should be taught first. In my opinion the connections created by known viruses and Trojans should be filtered out without any user' intervention.

= Provide proxy services

An advanced firewall is often includes a proxy server for better protection. This feature also makes a personal firewall a more complex program and requires a faster PC to run it. It is positive unless you have to pay too much and buy new PC.

= Sweeping the mails and Web pages from scripts and viruses

These are not unique features of Personal Firewall again. "E-mail sweepers" and antivirus programs are specialised in this activity and should do it better.

= Help you to catch an intruder

Do you really believe that an inexperienced home user could catch a "bad guy" who is breaking into several computers each day? You can catch a schoolboy who does "script kiddie scans" for fun or an innocent owner of an infected computer. The result you can get is to disconnect a person from his Internet provider. Even to reach this goal you have to follow special procedure published on SANS ([OWCN]) Website and spend at least an hour per each case to create proper documented request.

= Educate users about Internet and its danger

If this is your primary goal, you will definitely need Intrusion Detection System built into a product. Many people including myself use Personal Firewall primary for self-education.

Common problems with a Personal Firewall

The first and most important problem with any firewall solution is in its basis: the firewalling principles are complex for technicians and very complex to understand for a regular user. A lot of work should be done to hide these principles under a user interface.

The second problem is a user interface itself. We know that it is very hard to create one solution, which suits experts and beginners. Still it could be (and should) done. The biggest complaint is about high level of user annoyance from the built-in Intrusion Detection module. Should it be then a separate module which user could always switch off? There is a tendency to add such setting into firewall configuration.

Security is a very dynamic area. You can see it for example with antivirus products. Indeed, there is a great sense to buy not just an antivirus program but a long subscription for a product. This is absolutely necessary to keep the antivirus database on your computer up-to-date. Otherwise there is not much reason to have it at all. This subscription should be for every personal firewall product. To this moment I saw only one product ([NIS2]) with a reasonable upgrade policy.

The level of assistance from the help system is a very low now. Such complex area requires a huge help system to be delivered with every product to answer almost any user' question. There is plenty of information available in Internet. It should be collected and compiled to one "search and answer" system like famous Windows installation or search Wizards. Otherwise, in practice, a user will never get an answer for his question and his choice of sensitive system configuration will be intuitive.

Testing and Validation of the installed firewall is a complex operation. Every major change in firewall configuration should be followed, in theory, by good test to ensure that there are no new holes. There is no complete

solution for this problem so far. As simple and incomplete solution you can check Web sites, which are offering a security validation of your PC protection (Scans).

Price considerations are important as well. Everybody wants a cheap (or even a free) product. A good product could be hardly free because high level of support needed (the same as for antivirus products). A product should be upgraded quite often as new scans or attack principles are appearing. Now the price of a personal firewall solution is below 60 USD (except of PGP7 suite), which is not expensive. I don't expect it to go down because new features are added with each new version.

Conclusion

This new product called "Personal Firewall" is very promising. The need for it is growing every week but it is only useful for experts now. For a regular user is more a toy to explore the firewalling principles.

Please note that a single solution never gives you the 100% protection. The combined solution (for instance: backup + upgrades + firewall + standalone PC) should be used for the best protection.

Resources

General

1.[WEBO] internet.com Corp. "firewall - Webopedia Definition and Links". 29 May 1997. URL: http://webopedia.internet.com/TERM/f/firewall.html 10 Nov 2000
= Definition of the term "firewall"
= This page describes the term 'firewall' and lists other pages on the Web where you can find additional information.

2.[SPFW] Boran, Sean. "Personal Firewall/Intrusion detection Systems". 14 Nov 2000. URL: http://www.securityportal.com/articles/pf_main20001023.html 14 Nov 2000
= A current review of many personal firewalls

3.[SCIN] secinf.net "Network Security Information: Firewalls". Nov 2000. URL: http://secinf.net/ifwe.html 10 Nov 2000
= Huge number of variable links
= Network Security Library - Information about network security, (in)security: UNIX, Windows, NetWare, WWW, Firewalls, Intrusion Detection, Security Policy,

4.[BEYS] Beyond Security Ltd. "SecuriTeam.com Security Reviews". Security Reviews. 14 Oct 2000 URL: http://www.securiteam.com/securityreviews/ 10 Nov 2000
= Review "BlackICE Defender - A personal Firewall for the novice user"
= Review "Norton Internet Security 2000 - complete personal security"
= Company: = Beyond Security will help you expose your security holes and will show you what the bad guys already know about your hosts and network. Use our Automated Scanning service to perform a full security audit of your site, and find the latest security news and tools on Beyond Security's SecuriTeam web site.

5.[SANR] The SANS Institute. "Information Security Reading Room". 10 Nov 2000. URL: http://www.sans.org/infosecFAQ/index.htm 10 Nov 2000
= A collection of security papers and reviews

6.[AUDF] Spitzner, Lance. "Auditing Your Firewall" 9 Sep 2000 URL: http://www.enteract.com/~lspitz/audit.html 10 Nov 2000
= A technical article about testing your firewalls
= Tools and methods used by most common black hat threat on the Internet,

the Script Kiddies

7.[ZTFW] Zych, Tina. "Personal Firewalls: What are they, how do they work?". 22 Aug 2000 URL: http://www.sans.org/infosecFAQ/personal_fw.htm 10 Nov 2000
= A technical comparison of personal firewalls

8.[OWCN] McLachlan, Donald and the GIAC Community. "GIAC: Special Notice - Contacting Host Owners". v2.0 from 8 Apr 2000. URL: http://www.sans.org/y2k/contacting.htm 10 Nov 2000
= Right procedure of complaining about scan/attack

Linux

9.[FWHW] Grennan, Mark. "Firewall and Proxy Server HOWTO". 26 Feb 2000. URL: http://www.ibiblio.org/mdw/HOWTO/Firewall-HOWTO.html 10 Nov 2000
= Linux standard document about firewalls

10.[LNXF] Access/Interactive, Inc. "Linux Firewall Package". Nov 2000 URL: http://www.systime.com/access/firewall.htm 10 Nov 2000
= A short about Linux firewall solution

11.[FWLX] About.com, Inc. "Linux Firewall links on NTSECURITY". Nov 2000. URL: http://netsecurity.about.com/compute/netsecurity/cs/linuxfirewalls/index.htm 10 Nov 2000
= Unix Firewalls, intrusion detection, proxies and access control software.

12.[LNHO] Jewett, Sean. "RIMBoy's Firewall Config". 6 mar 1999. URL: http://www.rimboy.com/firewall/ 10 Nov 2000
= HOWTO about configuration of Linux firewall for @Home cable provider

Windows

13.[FWNT] About.com, Inc. "NT Firewall links on NTSECURITY". Nov 2000. URL: http://netsecurity.about.com/compute/netsecurity/cs/ntfirewalls/index.htm 10 Nov 2000
= NT Firewalls, intrusion detection, proxies and access control software.

14.[FWW9] About.com, Inc. "Windows 95/98 Firewall links on NTSECURITY". Nov 2000. URL: http://netsecurity.about.com/compute/netsecurity/cs/windowsfirewalls/index.htm 10 Nov 2000
= Personal firewall and intrusion detection software for your desktop computer.

15.[FXWT] Zeichick, Alan. "Firewalls: Use 'Em or Lose 'Em". 22 Dec 1999. URL: http://www.webtools.com/story/printableArticle?doc_id=TLS19991222S0001 10 Nov 2000
= Protect your web-development network with a firewall.

Commercial

16.[COFW] Thegild Corp. "Commercial Firewalls and Related FW Products". 12 Sep 2000. URL: http://www.thegild.com/firewall/ 10 Nov 2000
= Many commercial firewall solutions with short description

17.[SEFW] Markus, Stephen. "Personal Firewall Software". 10 Nov 2000. URL: http://www.firewallguide.com/software.htm 10 Nov 2000
= web site dedicated to reviews and sells of firewalls

18.[ZAPF] Zone Labs Inc. "ZoneAlarm Personal". 07 Nov 2000. URL: http://www.zonelabs.com/products.htm#zap 10 Nov 2000
= Zone Labs is a software technology company dedicated to providing leading Internet products enabling safe and productive use of the Internet.

19.[NIS2] Semantec Inc. "Norton Internet Security 2001". 26 Sep 2000. URL: http://www.symantec.com/sabu/nis/nis_pe/ 10 Nov 2000
= It could be my choice for Windows 9x

Scans

20.[GRCF] Gibson, Steve. "Shields UP! - Internet Connection Security Analysis". GRC Internet Security Detection System. 12 Nov 2000. URL: http://grc.com/su-firewalls.htm 10 Nov 2000
= A popular article about firewalls and Windows security tuning
= Test site offering free simple scans per personal use

21.[NWSC] Wallyware, Inc. "Remote computer Network security scan". Nov 2000. URL: http://networkscan.com/ 10 Nov 2000
= Intermediate free scans

22.[DSLR] DSLreports. "Secure-me Automated online security evaluation". Nov 2000. URL: http://www.secure-me.net 10 Nov 2000
= Advanced free and non-free scans

Last updated: $Date 15/11/2000 $