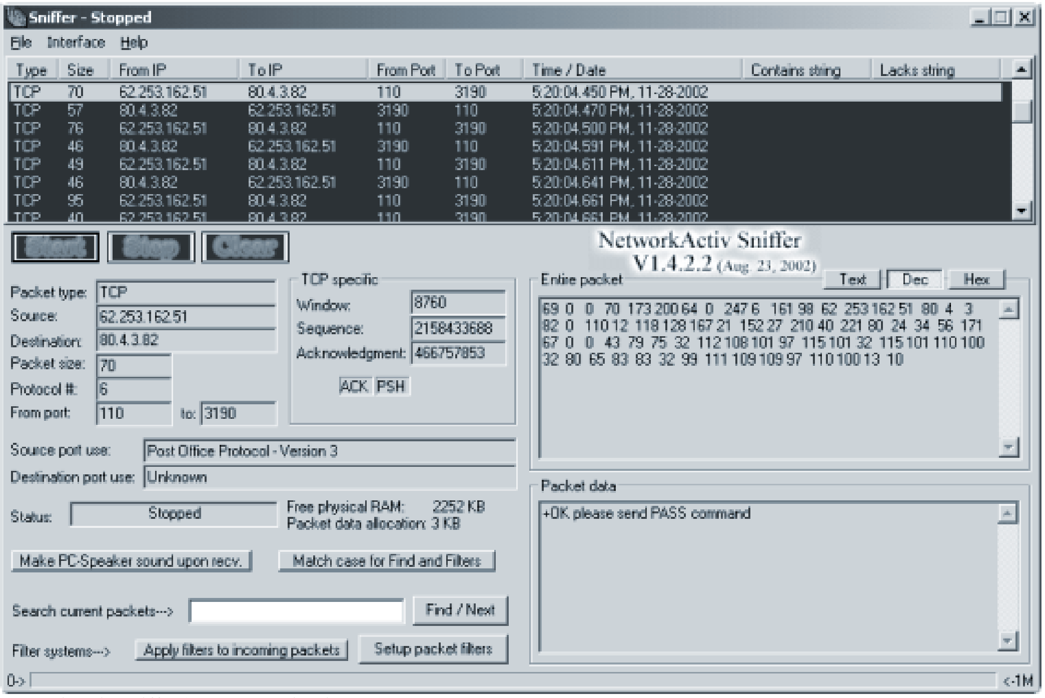
Safe & Secure Home Computing

By D Norris



Type	Size	From IP	To IP	From Port	To Port	Time / Date	Contains string	Lacks string
TCP	70	62.253.162.51	80.4.3.82	110	3190	5:20:04.450 PM, 11-28-2002		
TCP	57	80.4.3.82	62.253.162.51	3190	110	5:20:04.470 PM, 11-28-2002		
TCP	76	62.253.162.51	80.4.3.82	110	3190	5:20:04.500 PM, 11-28-2002		
TCP	46	80.4.3.82	62.253.162.51	3190	110	5:20:04.591 PM, 11-28-2002		
TCP	49	62.253.162.51	80.4.3.82	110	3190	5:20:04.611 PM, 11-28-2002		
TCP	46	80.4.3.82	62.253.162.51	3190	110	5:20:04.641 PM, 11-28-2002		
TCP	95	62.253.162.51	80.4.3.82	110	3190	5:20:04.661 PM, 11-28-2002		
TCP	40	62.253.162.51	80.4.3.82	110	3190	5:20:04.661 PM, 11-28-2002		

Packet type: TCP
Source: 62.253.162.51
Destination: 80.4.3.82
Packet size: 70
Protocol #: 6
From port: 110 to: 3190

TCP specific
Window: 8760
Sequence: 2158433688
Acknowledgment: 466757853

Source port use: Post Office Protocol - Version 3
Destination port use: Unknown

Status: Stopped
Free physical RAM: 2252 KB
Packet data allocation: 3 KB

Search current packets--->
Filter systems--->

Entire packet

```
69 0  0  70 173 200 64  0  247 6  161 98  62  253 162 51  80  4  3
82 0  110 12 118 128 167 21  152 27  210 40  221 80  24  34  56  171
67 0  0  43  79  75  32  112 108 101 97  115 101 32  115 101 110 100
32 80 65 83 83 32 99 111 109 109 97 110 100 13 10
```

Packet data

```
+OK please send PASS command
```

NetworkActiv Sniffer (www.networkactiv.com)

Safe & Secure Home Computing Version 2.2, December 20, 2002

DISCLAIMER

The information in this document is intended to provide a reasonably in-depth breakdown of the security issues and implications of connecting to the Internet, hereafter taken to refer to the global data network, which is otherwise known as the 'world wide web'. It is intended to explain these issues with the minimum possible amount of technical jargon; although due to the nature of the subject itself, this has sometimes proved difficult. It is intended for the 'novice' home user through to the 'moderately well informed' home or 'small office' user. (Home and small business users are the intended readers.) Although I have taken reasonable measures to ensure that the information presented (including remedies for any security related problems involving the reader) is as accurate and up to date as possible, I assume no liability for any loss or damage caused through following the advice provided within – or otherwise through any failure to follow it, including miss-implementation of suggested remedies. For further information, or if you have any issues regarding this, please feel free to contact me directly. My email address is david.norris23@ntlworld.com. You use (or fail to use) the advice provided in this document, at your own risk.

1) Introduction

What are the dangers of being online – And what precautions can be taken? Does this subject really concern me as a home user?

If you have a computer connected to the global data network, known normally as the 'world wide web' or Internet, then this document affects *you*.
All PC's running Windows, especially Windows 9.X and even un-patched, recently installed versions of NT, 2000 & XP are potential targets, more so if they are running externally visible servers, such as IIS, PWS or Exchange servers, or file sharing services of any kind. Any machine running any variant of Unix, especially Linux versions, are potential targets. Apple Macintosh systems, although less of a target for hackers, are certainly subject to virus attacks; and those running Macintosh OS 10 and above, are likely to become a target for many other types of attack in the fairly near future.

What are the risks of being online, or 'could it be you?'

One of the most frequent responses of a home user regarding security is: Why do I need it? Or otherwise, something along the basic lines of 'What can there possibly be on my system that anyone would want to steal'? Well, before I proceed, ask yourself the following questions:

- Have you ever ordered goods or services online?
- Do you use online banking and financial services?
- What other personal information have you stored (For example, regarding your job, personal life, shopping habits – the list is endless)?
- Do you work from home some or possibly most of the time?
- Have you got any copyrighted material, such as software, ebooks or other goods which you have paid for (as an example, you are generally legally

responsible for any software which has, or can be, copied in violation of the license agreement)?

- Are you running an FTP server or Windows 'File and Printer Sharing' which, without your knowledge, would allow a complete stranger to upload and store illegal material on your computer for distribution – and possibly even leaving you legally liable?

The answer is almost invariably yes to at least some of these questions! If you care about your privacy, money and personal data, then please read on! It stands to reason that issues regarding security for the average home user are every bit as relevant for the typical home user as for a business user. You probably wouldn't want a stranger to have access to any hard copies of your personal documents, so why leave your computer open to misuse and exploitation? You may have heard the saying 'prevention is better than cure'. Well this is probably at least as true of computer security as it is in any context!

Out of the box, all Windows versions in particular, and to varying degrees, the various variants of Unix/Linux, are horribly insecure. Virtually all of Microsoft's money making efforts go towards making Windows easy to use, and yet very little effort indeed is contributed towards security considerations, since this makes for a less straightforward or 'user friendly' operating environment. As I will explain later, there's invariably a trade-off between convenience and security.

Any computer system that is connected to the Internet should be considered as being vulnerable to external attack. This is particularly true in the context of 'always on' broadband connections – I'll explain why later on.

In today's world of near-permanent broadband Internet connections, the security of your home computers, as well as those in the corporate or office environment, has become significantly more of an issue. Even if you genuinely have no files on your PC that represent a personal security risk to you, namely personal or financial data, your PC can be used it as a staging ground for what are known as 'denial of service' attacks against other systems elsewhere. And in addition, your PC when used by your children, you might well be exposing them to any number of malicious individuals who seek to exploit children in a multitude of ways.

Furthermore, *every single new release* of an operating system has a number of loopholes waiting to be found, and software installed later may add still more. Once discovered, loopholes are usually advertised, first by the software vendors offering patches, then by various hackers' newsgroups e.t.c. Then random, usually automated attacks against networked computers follow within weeks or even within days. For example, a few years ago, a new vulnerability in the IMAP protocol (Internet Message Access Protocol -used by some email servers and clients), and over the next few weeks, my firewall recorded an escalation in the number of probes for IMAP! And even six months later, these probes were still fairly common. If you have just installed an operating system 'out of the box', it is very likely to be already out of date and for the system to be secured, you will need to update the system software by applying patches, hot fixes, upgrades or security fixes.

Once upon a time, if you, as a home user, used only the relatively brief and occasional modem connection to access the internet, it was considered acceptable not worry unduly about security, although of course, for those few people with 'always on' broadband connections at least a basic firewall was generally considered to be a minimum requirement.

The fact used to be that there were relatively few people online who had the means or the knowledge to break into other people’s computers via the web, and where they did do so the target was usually a large and/or high profile company or government department. Hacking was not an issue which was a prime concern for the ordinary home user of the Internet!

Today, however, the situation is radically different. There are any number of automated programs freely available to scan for security holes across a very large number of computers in a relatively short time. Because of this, no one connected to the net, however occasionally or briefly, is safe, since the entire internet is continuously being scanned for insecure computer systems from many different sources around the globe - and many Trojan horse programs also use probing to find new hosts. I would say that on average six or seven probes against my own machine arrive per twenty four hour period for which it is up and running, and that the number continues to rise! At time of writing, the most popular targets would appear to be FTP and Web servers, Microsoft SQL server (as a new vulnerability has come to light), and port 27374, which is used by the 'Subseven' Trojan horse (I'll explain what a Trojan horse program is later). Netbios, the Windows file and printer sharing service, also remains ever popular as a target, and the number of probes for this service continues to rise, although in my own case this is deliberately blocked at my gateway. The very serious Netbios sharing vulnerability is explained in detail later.

Even where people do give any thought to the security of their home computer, it tends to be quite some way down their list of priorities. The fact that many versions of Windows, in particular, leave much to be desired from a security point of view only adds to the magnitude of the problem. For many years, Microsoft have given little thought to the security of their products, only their functionality. However, now, at last, things have begun to change. Security has now begun to be integrated into recent versions of Windows, for example, in Windows 2000, the security features are now quite good. And although Windows NT was not really designed with the home user in mind, at least not from the outset, now all Windows releases (Such as Windows XP) will be based on NT.

Now, at last, the home user is being given the opportunity to consider computer security as a serious issue. As security features are now built into the operating system, it comes as some surprise that by default, the security settings are not very good following installation. This book attempts to explain, with as little technical jargon as I feel I can get away with, what the risks are, mainly from the point of the home user, and what reasonable steps can be taken to counter them. Remember that as however, security and convenience will always be at odds with each other; it is up to you to decide what is the right level of security for you.
Unlike corporate users, who have invested considerable resources to improve the security of their systems, home users are all too often leaving their computers open to various types of abuse. For example, many companies and individuals are writing software which they use to illicitly steal your personal information to further their aims. And all this happens quietly, behind the scenes, with neither your knowledge nor your consent…

Whilst securing a computer system can admittedly be a *real* pain, and will obviously involve expending some time and, possibly, a small amount of money also, it is an investment well made! If you don't believe me, then just consider the amount of time and money you may well need to expend in the following 'example' nightmare scenarios:

- Your computer has been hacked and used to launch a 'denial of service' attack on another site machine – and you're getting the blame;
- Your system was compromised at some indeterminate point in the past, and you are unsure which of your backup copies are "clean", namely contain genuine, un-falsified data;
- You discover that your system was hacked into several months ago, and it appears that the hacker has changed or deleted some of your important personal, work or study related, or financial, data. You have no backups, because you 'never got round' to making any;
- Your system is hacked and your banking details stolen. You later discover that money has been withdrawn from your account, and the bank will take absolutely no responsibility as you failed to report this breach at the time;
- Your system is being used to distribute pirated (illegally copied) software ("warez") or obscene material via an insecure anonymous FTP server or Windows file share, which you had no idea you were even running. This comes to attention of the police, who do not actually need to prove any intent on your part (as according to current UK legislation!);
- Your system is hacked, and the hacker has installed a 'password sniffer'. All your login, email (and other) passwords are known to one or more unknown individuals, who have been eavesdropping on you for months. Every person who has recently used your computer (yourself, your family, friends, e.t.c) has had their passwords sniffed and must change every single one of them;
- You are unsure of what has, or has not, been compromised. You therefore have to format your hard disk, reinstall the entire operating system from scratch, and all of the software, before you even start thinking about how to secure it. Which you could simply have done in the first place after all, and without all this extra pain…

So, what steps do you need to take to keep your system secure, and to discover where possible attempts to compromise your system's integrity are originating from? In the rest of this document, I will highlight the following points:

- Ensure that all user accounts have strong passwords set; or are disabled;
- Limit where the administrator/root user can login from, and who has access to these accounts;
- Firewall your system;
- Protect yourself from viruses, 'spyware', and other unwelcome additions to your system;
- Proactively check for suspicious activity;
- Avoid offering 'services' you don't actually need to offer, and which can be misused, and; when offering services, only offer them to people that really need to use them;
- Keep logs of successful and failed access attempts;

- Keep up-to-date with security issues, and security ‘holes’ as they come to light.
- Be aware that as a general security rule, *prevention is always better than cure*! After all, you do put a lock on your external doors? The same principle should apply to computer systems.

There is much happening online which you may not even have conceived of. Your computer may well be on the receiving end of many different types of attack, day in, day out. These include, but are not limited to:

- Data packets designed to crash PC;
- 'Trojan horse' programs which attempt to steal your confidential data
- Exploitation of security vulnerabilities in both Windows and Unix systems, all of which you will be quite unaware of - until you install a firewall and get dozens of alerts per day!

Without the most basic of protection, your home computer is a sitting target. A hacker anywhere in the world may get access to your files stored on the hard disk, or just wreak havoc with your settings.
And there are plenty of free software packages which can make finding your computer as easy as counting door handles - even if you are using dial up access to the Internet. Once an attacker has your IP address, they will probe for any security vulnerabilities which will gain them access to your computer, often without your being any the wiser.

Written for the non-technical user, this is a description of the potential risks that lie in wait out in the shady corners of the Internet, and how you can best manage your computer(s) to minimise the risks to your personal data and general privacy.
Using the minimal possible amount of technical jargon, I provide practical advice on how to take the necessary precautions such as changing the file sharing settings on your computer, adding, removing or adjusting file permissions, keeping your antiviral and firewall software up to date, and increasing your awareness of Internet security – without your having to give up your access to a vast store of information and opportunity.

Hacking is a problem that is common place throughout the world, and can affect you no matter where, or who, you are. You could work in a high-class company, worth a lot of money, and get your system hacked into, or be just a home user, like myself, surfing the web for information, when your home computer is hacked into. This is an issue that everyone should be informed about, including the home user, simply because it happens all of the time and you may well not even be aware of it! There may be some very important files of a sensitive nature on your hard drive that could, for example, contain your credit card number or any other personal information. Although some of the files that get stolen may not be as important as others, there is a high chance that some of them could well be important. It does not matter who you are, or what you do whilst you are online, it could still happen to *you* at any time, if you do not bother to maintain an acceptable level of security.

From the security point of view, consider a ‘network server’ as a program component which listens for connections from other computers. The vast majority of computers, from the time they are set-up, run far more network server programs than they need to. In an attempt to provide ease-of-use, even home computers, following the installation of the operating system, will usually be configured to run web servers such as Microsoft Internet Information Server, and possibly even email and domain name servers, that are normally quite unnecessary for the home user. In many cases, the user of the computers will be completely unaware that these services are even present. If the owner does not even know a service is running, there is no reason for them to configure it correctly. In which case, the service is likely to be accessible to outside intruders via the Internet, giving them unintended access to, and possibly control of, the computer.

All servers, whether or not they are well maintained, and intentionally running, are provided by computer software components, some of them very large and complex. There is a tendency for software to become more complex with each release of a new version. The complexity of today's programs means that they are unlikely to be perfectly written or tested: they will contain bugs. A bug is simply an unintended property which may cause the program to fail under certain operating conditions. Attempts to exploit these defects are called denial of service attacks. However a more dangerous type of attack in many respects is one that allows an external user to invoke some function of the computer that was not supposed to be available. This allows the intruder to gain access to the computer. A computer where this type of flaw has been exploited successfully, is no longer under the control of its rightful owner. With some considerable understatement it is referred to as being 'compromised'. The risks of a system compromise *can* however be reduced, although not quite removed. There are three main methodologies by which to achieve this aim:

- Remove any unnecessary services: Removing unnecessary network servers will reduce the number of potential targets available to the intruder. This can be done relatively easily once you understand the means. This involves disabling those services, and then periodically checking that they are not accidentally re-installed at a later time.

- Secure necessary services: Those services that *are* genuinely needed, and in particular those that offer connections to un-trusted external networks, must be kept in the most secure state possible. The software vendor may recommend software updates or amendments, in the form of service packs or 'patches' The source of such recommendations should always be checked however, because unfortunately it is commonplace for malicious advice or 'service packs' to be advertised claiming to be offer improvements.

- Restrict external access: Removing or patching network server components can only protect those computer systems where the services are *known* to be running. For protection of other systems where services aren't required but may end up being run by mistake, it is necessary to set up and correctly configure hardware routers, hardware firewalls or software firewalls to restrict the types network traffic that can access them from the Internet. For example there should be no need to run web servers where you are not intending to offer content, and most home users won't do so. This makes it desirable to block potentially hostile http requests, for example. Since it is considerably easier to know which services *should* be present, the best way to configure a router or firewall is to permit only external network traffic intended to utilise

> those services, and deny all other types of traffic. This results in some loss of convenience, but offers the best chance of protection against any unknown future threats which may come to light.

Following all the advice provided in this book will not make your system "100% secure" (no such thing is really possible!) but will make it more secure than most home computers connected to the Internet. It's a little bit similar to a neighbourhood watch scheme; it doesn't so much reduce crime, it just makes it go elsewhere where there are easier pickings. Removing unnecessary services, patching necessary ones, and installing router or firewall controls cannot entirely remove the risk that your computer will be compromised, but they will very substantially reduce it. Remember that the harder you make it to break into your home computer, the more likely it is that the 'casual' cracker will just move on to another computer that looks easier to exploit. Most casual hackers will simply move on to easier targets if their initial port scanning doesn't turn up any simple open 'gateways' into your machine. Many crackers use commonly available scanning tools that only look for simple exploits, such as unprotected file shares, and if they find none of these then they will simply move on. It must, however be borne in mind that many of the security risks are not unique to the Internet. For example, conventional credit card sales made by telephone are not really very secure. In fact, many risks online are not unlike those offline; it's just that the Internet makes crimes such as fraud easier.
Please see the glossary of terms which I hope will assist in explaining those I have had to use; it is at the end of this book. References to various examples of software tools such as antiviral software, 'spyware' removers and firewalls are made where opportunity offers. Where an especially important point needs to be made, I have marked it with a preceding symbol:

💣

Where you see this symbol from now on, pay particular attention! It is a key point... That said, it is not my intention to put anyone off of using the Internet, and taking advantage of all it's vast benefits. It has to be borne in mind that few activities in life do not come with at least some element of risk involved. Take driving, for example! One does not give up driving for fear of being involved in an accident; however it is most certainly possible (and realistic) to take sensible precautions to *avoid accidents*; this is the approach I am trying to promote here. If asked why people take risks with their personal information, you could just as well ask why people drive 'bumper to bumper' at 70 miles an hour in foggy or icy conditions, knowing the extreme risks they are taking?

---

2) Background

The Internet which we know today, originally developed from a project at the Defence Advanced Research Projects Agency in the United States in 1969.
The Internet has evolved from it's humble beginnings into the position where it is now an everyday part of personal and business life. ARPANET, as this project came to be known, was at first intended to provide reliable, high speed network

connectivity between all government, military, research and educational institutions. The connectivity was planed in such a way that, should one possible routing for data fail, for example as the result of an act of war, there would still be dozens of alternative routes, ensuring that connectivity be maintained. The Defence Advanced Research Projects Agency provided the funding for the project.

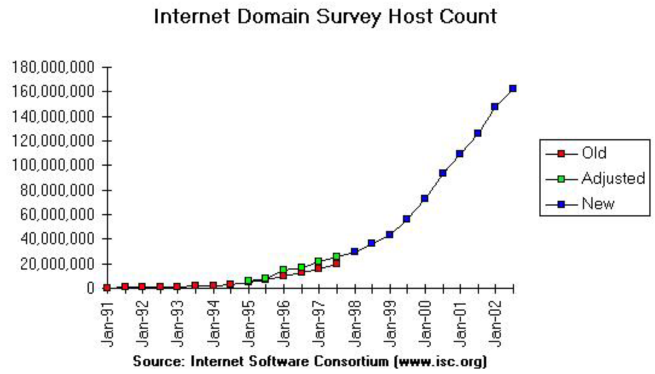
It soon became clear that a wide range of benefits and services could be accommodated, firstly on a nationwide basis throughout the United states, and later, in 1973, internationally. Queen Elizabeth first gained access to email as early as 1976! 1979 saw the first Usenet groups, in which one could talk online to other people who were also lucky enough to be online, and could freely discuss subjects as diverse as politics and science.

The term 'Internet' was first used as far back as 1982. However, a common set of data transfer protocols was needed and hence TCP/IP was devised. By January 1983, all the computers comprising the ARPANET were using the common TCP/IP protocols. Meanwhile, research had also began to focus also on alternative means of communication to cabling, such as radio and satellite links. The use of the personal computer was now fairly common in the workplace, and the notion of communicating with other corporations in a related line of work to their own, and of course with potential customers, was clearly seen as beneficial. By 1984, there were 1000 hosts already making up the Internet. Three years later, this number had increased tenfold. The Domain name system was first introduced in 1984. These are by no means essential for the Internet to operate. Computers in fact recognise only numbers; however as humans find it considerably easier to remember names as opposed to numbers, domain names are assigned. These names must likewise to IP addresses, be unique throughout the entire Internet. When you connect to a particular website, a domain name server (DNS) looks up the IP address associated with the domain name concerned. If you would like to view your own IP address, and are running Windows 95/98/ME, then whilst connected, go to 'start' then 'run' and type 'Winipcfg', and press enter, it will tell you. For Windows NT/2000/XP, and also Unix or Linux, use the 'Ipconfig' command within a command prompt window.

By the end of the 1980's, concerns about security began to surface. The so called 'Internet worm', originally written as an experiment, went out of control and shut down at least 10% of the Internet. This event was partly responsible for the introduction of the term 'hacker'. In 1990, the ARPANET, in it's own right, was officially dropped. However, the 'network of interconnected networks' lived on.

Each connected computer has it's own unique identification number, called an IP address. This is analogous to a unique postal address. This enables data packets to be sent to, and received by, a unique destination. For example, my IP address is 80.4.3.233. Each of the four numbers within each dot, is actually an 8 bit binary number from 00000000 to 11111111, which in decimal is 0 through to 255. In all, there are just over 4.2 billion possible addresses (But as these are nowadays fast filling up, a new six-number addressing scheme has been devised!).

Although in the early days of the Internet, 4.2 billion possible IP addresses looked more than adequate, the number of connected computers has been growing more or less exponentially. The following graph shows the growth of the Internet from 1991 through 2002:



Source: Internet Software Consortium (http://www.isc.org/).

Remember, nowadays there are numerous devices other than personal computers requiring IP addresses, for example set-top television boxes and WAP (wireless application protocol) mobile telephones. The ever-increasing integration of these devices has been correctly predicted. It is little wonder then that the shortage of IP addresses is becoming ever more worrying! The fact that, in the early days, IP address blocks were allocated according to request rather than actual need still continues to worsen the problem. By 1988 there were already 100,000 hosts on the Internet; by 1992 the 1 million mark was passed. And the number continues to grow, with no sign of the rate of growth slowing, at least within the foreseeable future – hence the shortage of IP addresses.

The Internet has become ever more commercialised during the 1990s. Whereas once it was dominated by a small number of providers serving large business users who felt the need for access, it has now become an expected public service which everyone can subscribe to, in much the same way as telephone or entertainment services. Browsers, which attempt to automate the usage of the web, allow easy access to information on a world-wide basis. The original hypertext transfer protocol (HTTP) has had many other 'whistles and bells' added in order to allow website to do far more than simply display information.

The Internet now resembles very little of it's original purposes, such is the normal process of evolution. Computer usage in the home will soon be the rule rather than the exception, and the increasing integration of computing with entertainment services, particularly television, and also of with existing telephone services, when combined with the benefits of electronic mail, will eventually change both out private, and working lives.

However, the haphazard way in which the Internet has developed has many implications for you, the end-user. I'm afraid that there is in fact much to fear whilst online. There are many hazards that can potentially affect *you*. To the majority of home-users, surfing would appear to be firstly, safe, and secondly, anonymous. It is neither. Although the average end user may not realise it until after a very unpleasant event has occurred. There are three main hazards inherent in the Internet.

Firstly, software is never perfect. It has various bugs, which amongst other things, tends to open security holes. It's a fact that today’s large, complex programs inevitably will contain a number of flaws. Unfortunately, Web servers are large, complex programs that can (and in some cases have been proven to) contain security holes.

Secondly, the confidentiality of the data transmitted across the net raises questions. Later, I will explain how it is possible to eavesdrop on data in transit, and show you an example. The TCP/IP protocol, which is in effect the language of the web, was not designed to go global, and therefore security was not built into the protocol. Confidential data transmitted across the web is only as secure as the encryption used to encode it - where any! In fact, your email passwords and FTP passwords are actually transmitted 'on the wire, unencrypted and 'in the clear'. Later, I'll explain all in the 'Packet Sniffing' section.

Thirdly, 'active web content', while on the one hand adding much functionality and convenience to the end-user, for example Java applets, ActiveX controls and JavaScript, introduce the risk that Web browsing may silently introduce viruses, 'spyware' or other malicious software components to the end-user's computer. Home users are most at risk here insofar as they are statistically the least likely to take precautions such as ensuring that their antiviral software is up to date.

Active content also has privacy implications for the end user; Web browsers provide a chronological electronic record of the user's surfing history, from which unscrupulous companies can reconstruct a profile of the user's browsing habits. See my section regarding web browser security.

Remember: The security of any Internet connected computer depends primarily on ensuring that it is running secure versions of system software. As the battle between system software developers and those trying to break or ‘crack’ the security of their products is ongoing, "secure" in a 'real time' context, essentially requires that it be "up-to-date". So all connected computers require fairly regular maintenance of their system software, either by installing relevant security 'patches' or by upgrading the operating system to the latest recommended version. Furthermore, to reduce the risk of 'compromise' and the number of patches that need to be maintained, computer users are strongly encouraged to disable any running services, such as Internet Information Services, that are present by default in the operating system as distributed and configured but are not required in the particular pattern of usage.

Ever since I personally first signed up for an always on 'broadband' connection, my machine has been repeatedly probed from various locations around the world. The probes appear to be looking for published vulnerabilities in Windows operating systems, however, do bear in mind that Unix systems have long been a target, and Macintosh systems, whilst of little interest to date, could well become a far more popular target in the not too distant future.

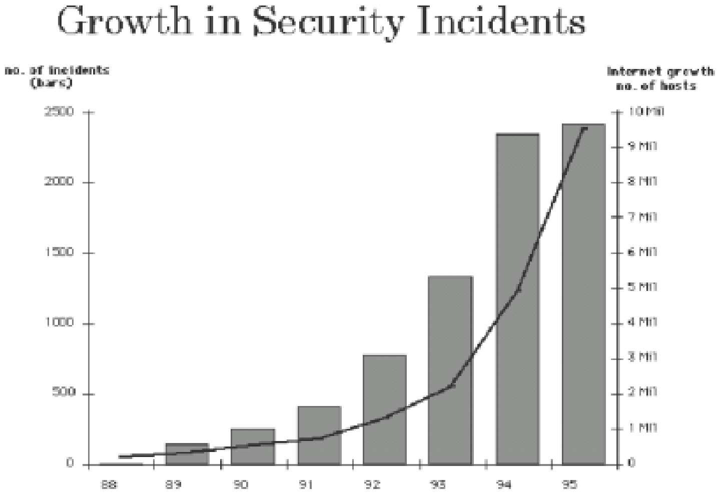
Remember that home computer systems which are always connected to the Internet via a ‘broadband’ connection in the home, like those belonging to a high profile organisation, and are likewise permanently connected, are always subject to constant electronic ‘probing’ from hackers, who are looking for machines that are vulnerable to such an attack. When a vulnerable (easily ‘compromised’) machine is found, it is usually only a matter of time before a hacker successfully takes control of the machine and, all too often, of many more machines elsewhere.

Once upon a time, the vast majority of this type of activity was intended to target Unix/Linux machines, however in recent years there has been an dramatic increase in the number of attacks targeting Windows machines in specific.

3) Where you stand: The Security Perspective

Remember, whenever you connect, whether temporarily via a dial-up connection, or on a continuous basis via a digital subscriber line (DSL) or, as in my own case, via a cable modem, your computer actually becomes a part of the Internet. It has it's own unique IP address, and, even for dial-up users, is able to exchange data with any other computer throughout the entire Internet - given that the remote computer is willing to participate. Few people realise that, in much the same way that you can obtain data from the other computers making up the Internet, it is of course possible for your computer to become a source of information. This is quite legitimate provided that this is a conscious decision; however, it is all too possible for this to happen without either your knowledge or your consent. This is because many of the underlying network protocols, such as the NEBIOS (Network basic input/output system) used by Windows, were intended for small scale usage within the 'trustworthy' confines of private office networks – they were never intended to come into contact with the global Internet. Remember that in particular, 'broadband' networks offering fast Internet access, essentially turn whole towns into local area networks. Your home computer is connected in a way for which 'Windows Networking' was never intended. Even where your files are password protected (For example Microsoft Word, Excel and Money offer password protection), this will often merely slow down a fraudster. This is because people do forget passwords to these files, and many companies offer software to remedy the problem. This software can be likewise used dishonestly.

Somewhat chillingly, as the number of hosts connected to the Internet has grown more or less exponentially since the 1970s, the number of security incidents reported has grown likewise; and this speaks not for the countless number of incidents which surely go unreported! A survey by the Computer Emergency Response Team (CERT), shows this information quite clearly, as the following graph shows. A mere glance tells the story here! A picture is worth a thousand words, as the saying goes. This raises the inevitable question: could my computer or network become part of the statistics soon?



There is almost certainly information on your home computer that is worth protecting, now you have taken a moment to realise this. How about your personal email account, for example? What about your financial details? You certainly wouldn't deliberately leave your credit card number lying around for all to find, surely? And yet all too many people do this on their own hard disks, without even being aware. Somehow people seem to assume that the 'privacy' of their own home will provide adequate security, although this is far from the case. It is true that online banking services encrypt data whilst in transit, however, by leaving your home computer itself completely unprotected, the bank's security provisions can be completely bypassed.

Furthermore, computer owners have security responsibilities extending beyond their own personal PC, or any other devices which happen to be connected to an external network. This is because many serious system break-ins are made using one or more 'third-party' systems which have been left susceptible, in order to make the source of the attack much harder to pinpoint. It therefore stands to reason that your own personal computer or other device, left completely unprotected, can be discovered and used as such a 'third party'. And this raises the question of legal responsibility: if, for example, your machine is set up with root/administrator, accounts left without passwords, and it is subsequently used by an unknown individual or group of individuals to break into a central banking system, you may in some cases be held liable since you failed to take the most elementary measures to secure the machine. Having gained control of your computer gives them the means to attack higher profile computer systems anonymously, such as banking systems for example, possibly making it appear as though *your* machine were the source of the attack. Try explaining this away! Because security online is dependent not only on a computer's own security measures, a compromised computer or system is a threat not only to you personally, but to countless other systems elsewhere. Here you have a joint responsibility to all the other users of the Internet: If your system is compromised, it can be used as the launch pad for a host of other attacks on other computers. If root accounts (Unix/Linux) or administrator accounts (Windows NT) are compromised on your system, then any other systems on a home network are almost certainly compromised immediately also. And this can also apply to other machines elsewhere on the Internet - If you are careless in your security and as a result your computer does end up being used as an intermediary in an attack of this nature, you will not be very popular! An example of this type of attack was recently conducted against servers belonging to Yahoo and Ebay. So think before you connect to the Internet, especially as root/administrator!

For example, an outsider might mount an attack against a company local to themselves via home computers connected via a broadband connection, which are located somewhere else in the world, in an attempt to make it almost impossible to detect the source of the attack.

One new security issue which concerns the home user is that of telecommuting. Telecommuting is becoming increasingly popular as it saves considerable costs for both the employer and their employees (for example, reduced travel costs, reduced office space - due to the fact that space and facilities need be provided only for the total number of personnel present at a given time, rather than the total number of employees within the organisation, and a further attraction involves the reduction in non-profitable time employees spend commuting). However, whilst corporate users are generally becoming much more security conscious, the home computers in use by their employees are generally not very secure, and may provide a ‘back door’ by which to breach the security of the corporate network. Telecommuters with broadband connections are the easiest targets.

You may, for example, think that you are already practicing good security if you use a personal firewall, anti-virus software, and you take the trouble to update these regularly. However, this software installed over the top of an insecure system leaves much to be desired. For example, anti-viral software won’t usually detect unknown viruses, and your firewall won’t block certain types of attack. This is because, although for example, you may have decided to allow access to port 80 on your system because you run a web-server (such as Internet Information Server) on your home PC via your broadband connection; however data packets designed to target vulnerabilities in Internet Information Server will appear legitimate to your firewall! This is why, although a firewall does form an important part of your protection, you must never become complacent and rely on it absolutely as your only means of defence!

Where the hacker is targeting you in person, techniques might be used ranging from packet sniffing (an attempt to log user's details by intercepting them in transit), to a brute-force password cracking attempt.

A small 'Trojan horse' programme may be secretly hidden on your PC which records and transmits or logs keystrokes for the hacker to collect later. As the password is typed within the first few keystrokes, it is then very easy to guess.

This is particularly the case where your Internet access is via a high-speed connection such as DSL or Cable Modem, which is not only always connected and therefore easier to discover, but in addition, IP addresses change rarely, where at all. As for traditional ‘dial-up’ users, who access the Internet by means of a modem at speeds of 56kb/second or less, you are only connected relatively briefly and for a small percentage of the time.

When modem users dial into an Internet connection, an ISP assigns each subscriber a temporary IP address using Dynamic Host Configuration Protocol. The addresses periodically expire, so each time the user logs off and dials in again, he or she is assigned a new IP address. This technique makes it difficult for a hacker to exploit that IP address to gain entry to a corporate network, for example – but it can be done. As your IP address is different on each occasion, it is harder (not impossible, only more difficult) for your machine to be found in the first place. Broadband users, however, usually have permanent addresses, which make them easy game. In addition, cable modems are thought to be slightly less secure than DSL because they share a common network in each geographic neighbourhood, making packet sniffing easy – (I will explain this later), whereas DSL uses an existing telephone network and provides each user with a dedicated line.

Computer systems can be exploited for both fraud and theft either by "automating" established methods of fraud, or by using entirely new methods. For example, individuals may use a computer to illicitly transfer small amounts of money from a large number of individual bank accounts, assuming that such small discrepancies may not be investigated. Financial systems are not the only ones at risk. Systems that control access to any resource are particular targets (e.g., workplace attendance systems, communication systems, university assessment systems, and inventory tracking).

With more people spending increasing amounts of time online, and data rates becoming ever faster, computer security is becoming just as pertinent to the home user as to business and government users. Another growing issue is the transport of Trojan Horses and worms into corporate networks through laptop computers that have been connected to a residential broadband connection at home. This is a nightmare for corporate security managers: Hackers are planting Trojan programs on home PCs, and users are unwittingly bringing in programs via portable computers that can obtain user passwords and account information from behind the corporate firewall and intrusion detection systems which are intended to block or detect any unwelcome activity of this nature.

It is also a fairly well known fact that the Internet contains material, which is definitely inappropriate for children, and therefore a means by which to 'filter' the content which children have access to whilst online becomes an absolute necessity. I discuss this topic in further detail later.

It is vital to remember that security is never perfect when a computing system is first set up. Computer users and software designers alike will continually discover new ways, whether intentionally or unintentionally, to bypass system security measures. Also, changes in the operating System or the software configuration can create new vulnerabilities. There is in addition the problem that the average home user is always the least likely to keep their anti-virus software and firewall up to date (If they even have any!). This effectively makes home computers a fertile breeding ground for viruses and other malware. All of these issues put together make it necessary for the home user to assess their computer's security.

Bear in mind that the very software you use to browse the Internet has capability to steal personal information, for example email addresses from your Outlook address book. Why do Microsoft and other software build this functionality into their products? To explain this, I must briefly discuss the marketing behind the software products.

Have you ever wondered why browsers, such as Netscape Navigator and Microsoft Internet Explorer are free? The fact that you personally do not pay for them mean someone else must do so. Corporations, who fund software development are always looking for personal data for use in marketing activities, for example email addresses to target with advertising material. And unfortunately, this means that software venders are far more inclined to listen not to you, the end user, but to those corporations who do actually pay for the software development costs. This may be why Internet Connection Firewall, which ships with the latest version of Windows (Windows XP), does not block outgoing connections, perhaps? This is yet another infringement of your privacy which you need to be made aware of.

It's not my intention to put anyone off of using either home computers or the Internet – the educational, financial and practical benefits of doing so are vast. But however paranoid this introduction may seem, the belief that existing telephone or postal communications are any more secure is simply a misconception aided by the fact that they have been around much longer. After all, many of us grew up without the widespread access to computing resources, and we are at present in a period of transition in which a gap of a single generation makes all the difference. In my own case, I remember using those BBC machines which were widely used in schools at the time (and which took quite some time to load a program from a tape!). It is therefore quite common for children well below the age of 10 to be far more 'computer literate' than their parents!

Information is, of course, only ever as secure as the least secure element of protection.

Remember that although electronic information may often be easier or more convenient to steal than a ‘hard’ copy, in the sense that electronic theft does not actually require a physical break-in, with a correspondingly higher risk of being caught in the act, a secure computer system will not provide protection for printed copies of files in an unlocked house, office or car, or paper copies of banking details sent through the postal service. It is important to remember that telephone calls can be overheard, and letters can go ‘astray’!

Computer Security is generally regarded as having three main elements:

- Availability -- information should be accessible to those who need it when they need it;
- Confidentiality - information should be available only to those who rightfully have access to it;
- Integrity -- information should only be modified only by those who are authorised to do so.

The aim of this book is to explain, in everyday language as far as possible, what the potential security risks of being online are, along with the methods needed to counter them. Many ‘home users’, particularly those who are not technically minded, are completely unaware of the risks, and therefore take no precautions to secure their computers from either viruses or hacker’ attacks. Obviously, there are some risks which would be present even if your computer weren’t connected to the World Wide Web, namely hardware failures, and physical theft of equipment. One particular (and quite obvious) rule for all computer users need hardly be mentioned: Make regular backups of any critical data, namely that which cannot be replaced. I wouldn’t rely on Diskettes – floppy disks – nowadays it is not necessary to do so anyhow; they are extremely limited in capacity, and also prone to media failure – one bad sector in a multi-disk backup may loose you *all* of the data in the backup.
Keep a copy of important files on removable media such as ZIP disks or re-writable CD-ROM disks. The re-writable CD-ROM’s typically cost less than £1 each, they have generally proven reliable, and furthermore, backing up your data doesn’t take long (particularly compared to replacing it!!!). There should be no excuses for not doing so! Re-Writable CD-ROM disks are far more versatile than ‘conventional’ tape drives which were once commonly used for backing up large amounts of data. The small amount of time and money involved is truly negligible compared to the value of your data. Use software backup tools where possible, and store the backup disks somewhere *away* from the computer. How often? You may just as easily ask yourself: How much are you content to loose?

There is an important warning to be given here: It is frequently difficult to back up a whole hard disk except to another hard disk, as today’s hard drive capacities are equivalent to a large number of CD-ROM disks! It is common to partition a hard disk into two or more ‘logical’ drives; for example you may have a 64GB drive partitioned into two 32GB partitions. In Windows, these will appear as two separate drives C: & D:. There are various reasons to do so, but backing up data is *not* a good one. *Never* make backups from one logical drive to another logical drive which happens to be part of the same *physical* drive – a hard disk failure will render both copies inaccessible! However, there are some reasons to keep your personal files on a separate partition; for example if your boot drive (Usually C:) were to become corrupted you can re-format it and still keep all your files. There may also be some security advantages to doing so, which I discuss later on.

Make a boot disk in case your computer is damaged or compromised in any way: To recover from any losses you do experience, such as from hard disk failure, create a boot disk which will help when recovering a computer after such an event has occurred. Remember, however, you must create this disk before you actually have a need for one(!). Nowadays, it is possible to re-boot most systems from CD-ROM. Older systems will require a diskette.

Most of the information here is intended for users of Windows 95 and later versions of Windows. Although I currently only have limited advice to offer regarding Unix and Macintosh systems, the underlying principles of security are always the same. I also have a section regarding security under Windows CE which runs on pocket personal computers; this I included as an afterthought as I am myself a user of a Pocket PC.

---

4) Just who – or what - is this invisible enemy?

We have all heard of the term ‘hacker’. This term is far too sweeping a generalisation. Hackers can, in fact, be broadly classified into several types:

- Joy riders (or recreational hackers) hack simply because they have the technical competence to do so, and enjoy a challenge. They may enjoy simply the challenge of being able to defy the wishes of a network administrator, who wishes to keep ‘outsiders’ from gaining access to a corporate network, for example. They may do so in order to demonstrate their knowledge to others. Asked why this should be the case, you may ask why people should wish to climb mountains, or swim across the English Channel. They do so not for any practical purpose.

- Then there are simply vandals who are intent on causing disruption, for example by means of conducting a ‘denial of service attack’. This may be due to their harbouring a grievance, or just simply for it’s own sake. This may be the motive of the hackers who broke into Cardiff County Council’s website, replacing their web-pages with a message: "YOU ARE ALL SHEEP - SHEEP I TELL YOU".
- There is also a third group: Profiteers are intent on making money from their exploits, for example by stealing your personal banking details for use in their fraudulent activities.
- A fourth group of hacker is the industrial spy. Some companies actually advertise espionage services to anyone who is willing to pay for them! If you think that this is no concern of the home user, think again. You would have to be leading a very uneventful life not to avoid offering any information useful from a marketing perspective. You may have some ‘spyware’ running on your system right now, harvesting data from your computer, without you being any the wiser! See what I have to say on the topic of ‘spyware’.

- Finally, there are ‘politically motivated’ hackers. These people hack for a political motive. This subject has recently come to light in the wake of the terrorist attacks on September 11th 2001. Recently, it has been reported in the national news that many businesses, and even home users of computing, have become targets for people such as anarchists and international terrorists. There are people out there who are intent on bringing down whole organisations. These are probably the most destructive types of hacker.

It is worth pointing out that hackers are unlike malicious software in the sense that they are unpredictable in nature. A virus, for instance, is found by identifying it’s signature, inherent in it’s program code. It’s effects can often be reversed simply by reversing the effect of it’s code (given that data has only been modified rather than destroyed). This is how antiviral software ‘cleans’ up after a virus attack. On the other hand, where damage is caused by an individual directly, it is often much harder to reverse. Remember however, that many hackers do not intentionally cause changes to a system, in order to make their actions more likely to go unnoticed. It is very rare indeed to catch them in the act; indeed detection is often a process like locating a black hole in outer space, in the sense that they are not directly visible, so instead one looks for their effect on their surroundings, which give them away.

Hacking is indeed a problem that is likely to become more of an issue for the average home user in the future than you might have expected. With the advent of ADSL and other high speed 'always on' connections, hackers could gain access to peoples home machines much more easily, as I shall explain later. Clearly this doesn't threaten national security in itself, in any way the government would regard too seriously, but I do feel that peoples attitudes toward this subject will become much more serious when they have their own personal computer hacked into, and their banking details stolen?

When an external intruder (or hacker) succeeds in gaining access to a computer, he gains access to some or all of the resources of the compromised computer system, and the some or all of the computing power and files stored on that machine. He may also attempt to gain access to other machines on the same network (for example, other users of your Internet service provider) by attempting to capture usernames and passwords. This gives him or her the ability to access or mount an attack against more machines. You must therefore remember that all Internet users owe each other some mutual responsibility for the security of their machines.

Most such individuals are likely to be on the ‘outside’, attempting to gain access via the Internet, or otherwise through a physical break-in. However, there is also the possibility, for example, of your wife or husband attempting to find out what you are doing without their knowledge. Should this be an area of concern, then you may follow the advice as provided; however I don’t wish to question any parties’ possible motives for this particular area of attack. I merely prepare readers for all foreseeable possibilities.

Do, however, bear in mind that computer security actually has three separate elements:

- *Physical security:*

If you have an external connection to the Internet, then you assume responsibility for all usage of that connection (ask your Internet Service Provider if you don't believe me!). You really should protect your computer(s) with a password if they are accessible to others, and logout when you are not using the machine. Any machine which is not protected by a password should be protected by a locked door when the owner is not present. This is also common sense as it makes physical theft more difficult, of course! Don't, for example, place your computer near a window if there is any alternative, it makes a very tempting target…

- *Virus security:*

PCs and Macintoshes must run up-to-date virus protection software, which is designed for the protection of the operating system in use. This should be updated at least once per month, preferably more frequently. Most antiviral software can be updated online for free. There are no valid excuses for leaving yourself, and others, vulnerable.

- *Network security:*

All machines should be running an up-to-date version of the operating system (with the appropriate 'patches' or service packs installed; these can be obtained for free). Your computer should be running only the required network services (FTP servers, Web servers, file sharing services etc) enabled. Note that you cannot simply assume that a brand new computer will be running an up-to-date system! Instead you can safely assume that it is *not,* as any operating system is never perfect when newly installed. Most new systems will need to have 'patches' or security packs installed. Similarly, you cannot assume that no network services will be running! To take an example, many Unix and Linux installations will enable some network services by default (without any user request during installation) and Windows 2000 will install 'file and printer sharing' services (Netbios) unless you specifically tell it not to. Although this is done in perfectly good faith, as the end user will obviously want to get their system up and running as quickly as they possibly can, and with the minimum of fuss, it will inevitably install components which you won't personally need, and which may offer security 'holes' to the potential intruder.

Here is an important point regarding Windows technical support: Remember that Windows versions go out of date, and are not supported when they have done so. Here is the current (December 2002) information for all Windows versions. The situation regarding Unix/Linux is somewhat less clear cut.

For the Windows 9.X series (This series includes standalone DOS, 3.X, 95, 98 and ME):

Currently all these versions up to and including Windows 95 are in their non-supported phase. This means there are no more patches, updates or security releases available from Microsoft any longer. Windows 98 SE has entered its extended phase of life until June 30th 2003, and will be unsupported after this date. Windows ME is in its mainstream support phase until 31st December 2003, and will be supported for a further year - until the end of 2004.

For the Windows NT series:

Windows NT 3.5x entered its end of life phase in December 2001. Windows NT 4.0 entered its extended life phase on June 30th 2002. Windows NT 4.0 Server patches are available from Microsoft at no cost until 31st December 2003, but Windows NT 4.0 Workstation is only in it's extended support phase until 30th June 2003. During this period a subscription may be payable for support.
Windows 2000 will enter its extended life phase in April 2005, and will be supported until April 2006.
Note: In all cases support will be provided for the latest and preceding service pack and any previous service packs are also assumed to have been installed. If you are using a version which has reached the end of it's life, it is now unsupported and you are strongly advised to upgrade, provided that your hardware is capable of running the newer Windows' version.

5) How do outsiders gain access to your computer? (Or, could it be you?)

Some operating systems are inherently more secure than others. At time of writing, most people will be running a Windows NT/2000/XP system. These were the first Windows versions to offer security as a standard feature of the operating system. This is a major improvement compared to Windows 9.X, which was completely defenceless from a security point of view. If you are still running Windows 95/98, it is in your best interests to upgrade in order to gain the advantage of a secure operating system. Alternatively, you may consider learning Unix, or Linux, a free variant of Unix. Keep in mind that there are far fewer software packages and accessories for these platforms than for Windows, however. Do bear in mind that you will still need to update your system from time to time; this is because security vulnerabilities have been found in both the Unix and Windows NT operating systems, and new vulnerabilities are still being found on a regular basis. Keep in mind that both Unix and Windows NT systems are somewhat involved to use than Windows 9.X, largely because the Unix and NT file and user account systems are somewhat complex and need to be configured correctly. Be prepared to use the documentation and help files for a little while after upgrade! In general, the file systems of both Unix/Linux and Windows NT/2000/XP systems allow you to take steps to determine:

- Who is allowed to use the computer(s), and possibly also when;
- What they are allowed to do (different users may be granted different levels of access);
- What constitutes unacceptable use of the computer(s);
- What remote and local access to allow to users.

Needless to say, Windows 9.X has none of this protection, hence my recommendation to upgrade. In the computer security context, the terms 'hacker' and 'intruder' refer to an individual who attempts, whether successfully or otherwise to gain unauthorised access to the resources of a computer system, or to the data held on it.

There are a number of ways a potential intruder can attempt to access a remote computer, ranging from the very crude to the technically competent:

Local Access: This type of hacking assumes the hacker already has a low privilege user account on the system. For example, if you are using Windows 2000 or XP, you may wish to prevent the children, and their friends from tampering with system settings, installing incompatible software, for instance. (And if you use the computer for anything serious, for example to do with your job, it may be wise!). If they can gain assess to your administrator account, for example by finding out the password, they can do whatever they please without you being any the wiser. (Windows 9.X is entirely defenceless in this respect). I know, for instance, of children who have managed to work out the pin codes for cable/satellite television systems (to prevent them from gaining access to 'adult' channels!), and have then programmed in their own codes thus locking out their parents!

Physical Access: If an intruder can physically access your machine (i.e. they can use the keyboard or take apart the system to remove the hard disk), they will be able to get in with little difficulty. (Don't believe me? I know of one other person who tried to boot his PC after returning from holiday, only to find that the entire inside had been stripped out, leaving only an empty case!)

Remote Access: This type of intrusion, from a remote computer elsewhere on the Internet, is the main subject of this book. It involves an intruder who attempts to remotely penetrate your machine across the Internet, without your knowledge or consent. You *can* go some way toward protecting yourself, however. Remember that although these is no such thing as a 100% secure system, it is certainly possible to protect yourself against 90% of dangers by taking minimal precautions, or perhaps 99% by resorting to drastic measures, such as never going online! Remember that system failures, fire or physical theft are also potential risks.

Trojan horses: These programs can be planted on a compromised system. They can take many forms, but amongst other functions they can:

- Contact the program's author, informing them whenever you go online, and what your current IP address is (useful where you are using dial-up connection via a modem, which uses dynamic addressing; namely the IP address of your machine is different each time you connect);
- Forward copies of each email you send to the programs author;
- Forward copies of your personal files or data to the programs author;
- Log keystrokes, passwords e.t.c, and send them to the author of the program whilst you are online, or cache them somewhere on your system to be collected later;
- Log personal data regarding your shopping habits, for example, in order to gather marketing information;
- Destroy or corrupt files stored on your hard disk;
- It is even possible to use your computer as a bugging or surveillance device (Don't believe me? How many computers have microphones and/or cameras attached these days?).

As you can see, the list of possibilities is endless...

It has long been feared (and with some justification) that companies such as Microsoft in particular, can gain access to your computer. I have heard many companies can access data regarding what software is installed, how it is used, and maybe can also copy personal data files whenever you go online. I wouldn’t be in the least surprised if Microsoft have built a remote upload client into the Windows operating system itself, so do treat any open ports which you may have, and cannot account for! I understand that when you upgrade certain products online, Microsoft may even also check the entire system for unlicensed software!

Trojan horses, which amongst other things can transfer your personal data to the programs author whilst you are online are indeed a serious concern, but what about Windows itself?

Most of the networking functionality of Windows was originally designed for the office environment. Here, most of the networked PC's sit behind very strong industrial class firewalls, so the vulnerabilities are never directly exposed to the outside world. Home Users do not usually have this level of protection and have no choice but to expose Windows to the Internet by a direct modem, cable or ADSL connection. This makes those PC's particularly vulnerable to even the most simple hacking techniques. Any operating system, be it Windows, the number of variants of UNIX or Linux, or Macintosh will invariably have a number of security holes; with the size and complexity of programs becoming as excessive as they are nowadays, it's a fact of life that some unintended "functionality" or properties will inadvertently be built in. Take for example a web-browser. A web-browser, for example, having only the features and functionality it needs to do it’s job, would fit onto a single floppy disk. And yet when was the last time you obtained a program on a floppy disk? The most up-to-date browsers are around 30MB (When in the compressed distribution package!). Doesn’t this in itself imply that there is more to go wrong? Remember that Windows 9.X, and to a somewhat lesser extent, Windows NT, are somewhat flaky operating systems, as are many of the programs which run under Windows; they tend to fall over very easily. Unix/Linux is more stable, crashes are rare, although they do have some known vulnerabilities, and more will be found in the future.

There is also the undeniable fact that people are all too often the weakest link in any security scenario! All too often they either fail to realise that they are a potential target for viruses, malicious individuals, spyware, or fraud – to name just a few potential dangers. Or they just take the attitude that their systems don’t contain any valuable information; and yet they are probably wrong. They therefore don't see the value of information security. Instead they either ignorant of the risks, or see it as a cost or inconvenience. For this reason they may not bother to install a firewall, or an antiviral product – the cost is negligible compared to that of having your banking details stolen for fraudulent use. Home users are equally guilty for not password protecting their systems or not choosing a sensible password. Also people are to blame for not getting to know their computers well enough – this accounts for unprotected file shares, anonymous FTP servers allowing uploads.

Remember, it is *your* responsibility to safeguard your computer through appropriate means (i.e. using commercially available firewall and antiviral software) against theft, unauthorised use or file system corruption. Remember that your Internet service provider only provides your access to the Internet; they have no responsibility towards any file content that you may download from the Internet, receive in your e-mail, or is placed on your system by anonymous third parties without your knowledge.

6) Viruses, Worms & Trojan Horses

These are names given to various computer ‘vermin’. A virus is essentially a small program, which ‘infects’ a host program, or even a formatted document with macro capability, such as Microsoft Word or Excel documents. The idea is that when the infected program is run, the virus is run also. The virus usually attempts to reproduce by locating other files of the same type, which it can also infect. It is essentially a code segment that replicates by attaching copies of itself to existing executables. The new copy of the virus is executed when a user executes the new host program. The virus may include an additional "payload" that triggers when specific conditions are met, for example on a ‘significant date’ such as a Friday 13th. Remember that computers do allow such people to ‘play pranks’ which are not possible by any other means.

For example, some viruses may display a text string or humorous message on a particular date, or they may attempt to do something considerably more destructive. Even where the virus’s payload is intended only to play a practical joke, it can still be dangerous. For example, where it is intended to introduce spelling errors into files, the implications may well be dangerous. For instance, what could potentially happen in a case where the name or dosage of medical prescriptions in a database was falsified, resulting in a patient being administered, say, 10 milligrams of a drug instead of 10 micrograms?

In fact it is also possible for a virus to cause damage inadvertently; this is because there are so many possible combinations of hardware and software. Even professional software developers are faced with this problem. (Another problem throughout software engineering is that designers, consultants and end-users are never fully in communication at the ‘grass roots’ level, which results in many mistakes being made. This is one means by which ‘bugs’ can be produced. There is one additional problem of interpretation; two people can read a paragraph in a software requirements manual, for example, and have a completely different interpretation of it’s meaning. Not all ‘computer malfunctions’ are the result of a virus!). Remember that some viruses simply propagate from one system to another without giving any outward signs at all. There are many types of viruses, including variants, overwriting, memory resident, stealth, and polymorphic; the latter type attempt to ‘evolve’, in an attempt to make detection harder.

A ‘Trojan horse’ is a standalone program, which masquerades as something useful, but beholds a sinister purpose or task, which it completes as well as, or instead of, it’s declared function. Once upon a time, these programs used to get around on floppy disks, however nowadays the Internet is the main distribution system. However, there have been a few occasions on which commercial software has unknowingly been sold complete with a virus!

Consider as an example an editing program for text files. This program could be modified to randomly delete one of the users' files each time they perform a useful function (editing text documents), but the deletions are unexpected to the user and definitely undesired!

Worms are essentially self-replicating programs that are self-contained and does not require a host program, unlike a virus. The program creates a copy of itself and causes it to execute in turn; no intervention is required on the part of the user. Worms commonly use network services to propagate to other host systems. These can often consume such significant resources, causing depleted network or system performance, and eventually a denial of service as the system concerned runs out of capacity.

Do I personally need to worry about the threat from viruses, worms and Trojan horse programs, as a home user?

Yes. New computer viruses continue to be written and to circulate around the globe - and these present a real danger to individuals' computer systems and their personal files. It is vital that every computer user takes steps to protect themselves and their computer(s); if you fail to do so you are risking not only your own computer and data but also that of numerous other computer users. Do, however, keep in mind that in the real world, although viruses are more widely publicized (even though only particularly destructive viruses tend to make the headlines), more data is in fact lost to accidents (human error) and to system failure (and lazy users failing to make backups!) than to virus attacks.

A few years ago viruses spread almost entirely on floppy disks. The commonest type of virus some years back in the 1980s was the "boot sector virus", which affected PCs but not Macintoshes, and was acquired by starting up the machine with an infected diskette in the drive. File-based viruses affected both PCs and Macintoshes and were triggered by executing an infected program (.EXE or .COM) file, perhaps copied from another system or arriving on a diskette. Nowadays, there should not be any excuse for getting a boot sector virus, as you can change the bios (basic input/output system) of your computer to boot from the hard disk, or a CD-ROM, in preference. The bios is a program which is stored in ROM (read only memory, which is not dependent on power) and contains the necessary instructions to enable the machine to load the operating system on start-up. For the vast majority of modern IBM-compatible PC’s, it is generally possible to password-protect the BIOS setup (you can enter the BIOS by pressing a ‘hot key’ at a certain point during startup (often the ‘delete/del key), and setting this and other options. Take great care, however, as improper or inexperienced use of the bios setup program can cause problems!). To enter your bios settings, wait for the ‘Press DEL to enter setup’ prompt whilst booting the machine. This will allow you to prevent booting from a floppy disk; therefore it is strictly possible to ensure that the machine will only be booted from either the hard disk as is normally the case, or a CD-ROM disk. You may also be able to boot from a network, using a service such as tftp, although this won’t be of much use to the majority of home users.

Nowadays viruses are much more frequently spread via e-mail. This is a result of the dramatic increase in Internet and electronic messaging use and the increasingly complex functionality which has been added to today’s e-mail clients. For example, these extra functions allow users to attach program files and formatted documents to send around the world, but can also allow viruses to spread further and faster than ever before. Viruses most commonly arrive as e-mail attachments -often with .exe, .com, .bat or .vbs extensions. To infect the computer the attachment must be run, usually by the user clicking on it. The text of the e-mail is in itself harmless, but usually provides an incentive to open the attachment, for example money, sex and humor are commonly used as an incentive to trap the reader. As it is possible to hide the actual extension of the file, the apparent, displayed file extension is *not* an accurate guide to the true nature of the file!

Macro viruses first appeared in around 1997 (at the time I was in my first year at university) and can affect both PCs and Macintoshes. They attach themselves to any Word and Excel macros present in documents and propagate very readily when files are passed around from one machine to another.

The latest type of common virus is the e-mail virus, which propagates by attaching itself to e-mail messages you send to other people, or in some cases by automatically e-mailing itself to addresses taken from your address book. Note that this does not happen by you reading the actual e-mail message; the virus is triggered when you open (usually by clicking on it) the attachment which arrives with the message. Remember that when you 'open' a file of these types (.EXE, .COM, .VBS, e.t.c.) that as these are types of program, 'opening' them runs the program.

Be sure that when you receive virus warnings, that the information is authentic, however. There are always hoax virus warnings in circulation. For example, recently there was such a warning about a certain file which was part of the windows operating system being deleted, claiming it to be a virus. Deleting the file caused Windows to loose support for long file names.

The result of hoax warnings is not confined to a waste of people's time; some people may become quite unnecessarily worried about a nonexistent threat; however some users, on the contrary, go to the exact opposite extreme and assume all warnings to be hoaxes, and are therefore not worried enough!

It is also worth noting that considerably more data loss is caused by human error and computer system failure than by viruses. Regular backups help to protect against these dangers in addition to helping with recovery from a virus infection.

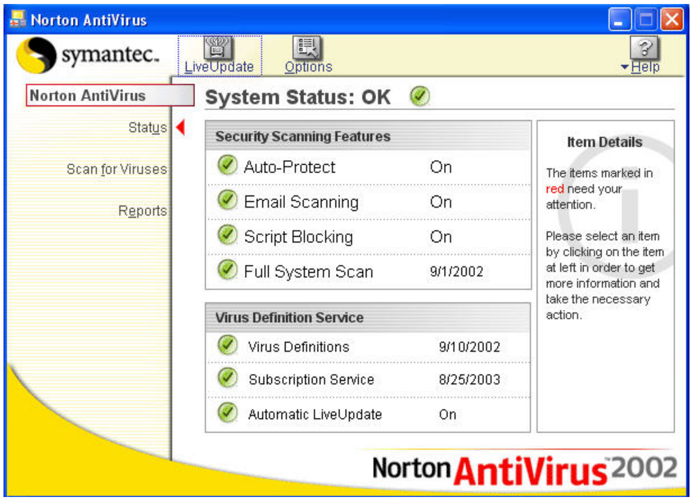
When you make your backups, there are a number of options depending on the amount of information you need to save, and the length of time for which it is be kept. Tapes, high-capacity removable disks and CD-ROMs are all routinely available from many computer dealers, and also stationary shops. Good quality media should always be used. (Avoid using floppy disks – they are of limited capacity, and prone to media failure. There are plenty of far superior media available these days). Re-writable CD-ROM disks are recommended, provided that you have a writable drive. Catalogue and store the backup copies in a safe, ordered fashion so the correct one can be found quickly and easily when the need arises.

If confidential information is being backed up, then do be certain that the backups are stored as securely as the original copies. And above all, make sure backups are taken at appropriate, regular times to give the best chance of recovering information in times of need. Backups taken at the end of a working session give better protection than those taken at the start, for example. Remember that backing up important data will be of little use if you cannot recover files quickly when things go wrong!

The most obvious check, though all too often forgotten, is to check that files are actually being written correctly to the backup tape or disk and that they can be read back from there. It is of no use to find out later that the backup copy is corrupt!

One of the single most important things to do right away is to install antiviral software. All computers, regardless of their operating system, and whether they are used at home or at work, need you to install a good anti-virus package and keep it updated. Remember, with the number of known viruses increasing exponentially as

more are being written, you must keep your anti-virus up to date. Usually updating involves logging onto the software vendor’s website and downloading the updates. Most of the software prompts you to do this automatically.
Personally I use Norton Antivirus 2002. It is good value for money (about £25 sterling) and updates after purchase are free. This is the control panel of Norton Antivirus 2002:



System Status: OK ✓

Security Scanning Features	
✓ Auto-Protect	On
✓ Email Scanning	On
✓ Script Blocking	On
✓ Full System Scan	9/1/2002

Virus Definition Service	
✓ Virus Definitions	9/10/2002
✓ Subscription Service	8/25/2003
✓ Automatic LiveUpdate	On

Item Details

The items marked in red need your attention.

Please select an item by clicking on the item at left in order to get more information and take the necessary action.

Your anti-virus should be set up to automatically monitor for evidence of viruses, and check outgoing email attachments (It is highly embarrassing to accidentally send someone else a virus!), check incoming email for your own protection, and also be run to scan your files regularly, for example, once per fortnight. You can never do so too often, as any file of a number of types that you download, or receive via email or on diskettes could potentially contain a virus. More information on which files are safe to accept, and which are potentially risky, is given later on.
There actually are a lot of viruses out there. And then there are some ‘viruses’ that aren't really out there in existence at all! Hoax virus warning messages are more than time wasting annoyances. After repeatedly becoming alarmed, only to learn
that there was, in fact, no real virus of a given name or type, computer users may well get into the habit of ignoring all virus warning messages they receive, thus leaving them especially vulnerable to the next real, (and perhaps truly destructive!), virus. Perhaps the best example is the AOL4FREE hoax, which circulated some years ago. This began as a hoax virus warning about a nonexistent virus – a program named aol4free.com was passed around, allowing the setting up of fraudulent AOL accounts. This was followed by a hoax about this being a virus. Once it was widely known that this warning was a hoax, somebody began to distribute a destructive Trojan horse (a Trojan horse differs from a virus in that it does not reproduce itself) in a file named aol4free.com, attached to the original hoax virus warning! So if you receive a message like this, asking that it be passed around to everyone you know, or as many people as possible - don’t – until the warning is confirmed to be genuine!

In addition to the above types of computer ‘vermin’, there is one other type of program which can cause you problems, and do not fall into the above categories. ‘Greedy programs’ are simply programs which are allocated system resources such as memory, disk space or processor time, and do not free them up when finished with. These can be either accidental or malicious. If malicious, they are obviously designed to waste system resources; if accidental, they are simply poorly written or tested. Many software distributions come with some ‘sample’ programs or scripts, to demonstrate the use of the product. The trouble is that often they are not always subject to the same quality control procedures as the main product, and I’ve seen one or two scripts which are appallingly badly written.

To see whether such a program is responsible for a system slowdown, try using the Windows task manager (only Windows NT/2000/XP have a task manager). Press control-alt-delete, and select the task manager.

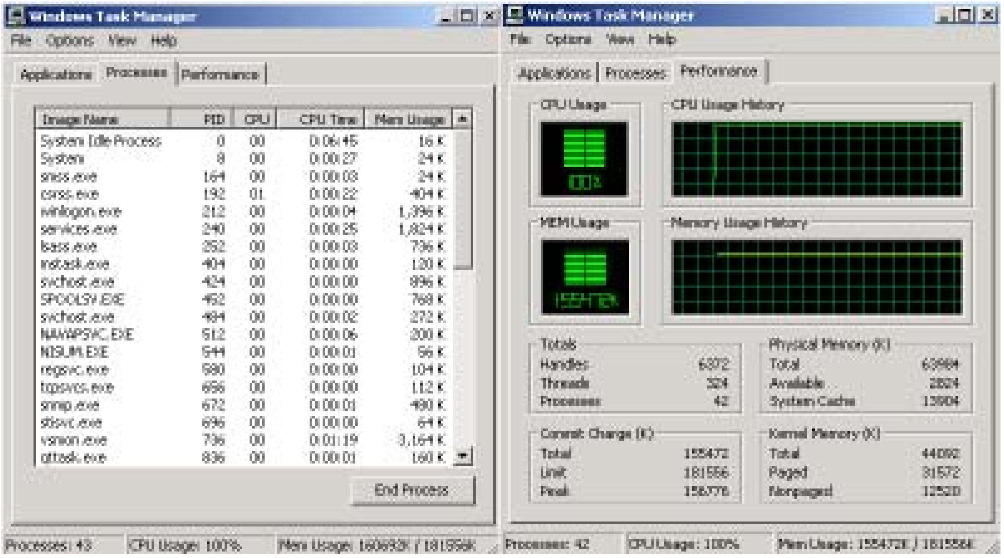


Image Name	PID	CPU	CPU Time	Mem Usage
System Idle Process	0	00	0:06:45	16 K
System	8	00	0:00:27	24 K
smss.exe	164	00	0:00:03	24 K
csrss.exe	192	01	0:00:22	404 K
winlogon.exe	212	00	0:00:04	1,396 K
services.exe	240	00	0:00:25	1,824 K
lsass.exe	252	00	0:00:03	736 K
instask.exe	404	00	0:00:00	120 K
svchost.exe	424	00	0:00:00	896 K
SPOOLSV.EXE	452	00	0:00:00	768 K
svchost.exe	484	00	0:00:02	272 K
NAVAPSVC.EXE	512	00	0:00:06	200 K
NISUM.EXE	544	00	0:00:01	56 K
regsvc.exe	580	00	0:00:00	104 K
tcpsvcs.exe	656	00	0:00:00	112 K
snmp.exe	672	00	0:00:01	480 K
stisvc.exe	696	00	0:00:00	64 K
vsmon.exe	736	00	0:01:19	3,164 K
gttask.exe	836	00	0:00:01	160 K

Processes: 43 CPU Usage: 100% Mem Usage: 160692K / 181556K

Totals	
Handles	6372
Threads	324
Processes	42

Physical Memory (K)	
Total	63984
Available	2824
System Cache	13904

Commit Charge (K)	
Total	155472
Limit	181556
Peak	156776

Kernel Memory (K)	
Total	44092
Paged	31572
Nonpaged	12520

Processes: 42 CPU Usage: 100% Mem Usage: 155472K / 181556K

Have a look at the ‘Performance’ tab as illustrated on the right. If the CPU or memory usage history remains at or close to 100%, even in spite of you having no applications running, you may have a ‘greedy program’ running as a process. Select the ‘Processes’ tab (on the left) and view the list of processes. Close any applications you have running, and make sure that you have no unsaved work! Now, select a process and click ‘end process’. You will receive a warning about possible system instability – hence my advice about saving your work! Now, select ‘yes’, and when the process has been terminated, look again at the ‘Performance’ view. If the resources available increase dramatically, then you have discovered the greedy program! Make a note of the name of the program concerned. Note: Windows NT will not let you terminate any vital system processes, even if you are logged on as an administrator.

Generally, a process corresponds to a program file (.EXE) which has to be located somewhere on your hard disk. Use the search facility to locate it.

When you find it, feel free to delete it – but be careful if it’s located in a system folder! You can only delete files from directories such as your Windows directory (c:\winnt by default) or your program directory (c:\program files) if you’re logged in as an administrator. If not, seek your system administrator’s advice, explaining the problem. Take care not to delete anything important, however! If in doubt, seek advice here.

7) How can I get a virus?

One method by which a virus can be spread is via email. This is probably the most prevalent means of transport these days. Once upon a time, viruses mainly spread via diskettes – floppy disks, which where used to transfer data from one computer to another. The Internet potentially offers a much quicker transfer medium, however. This is because nowadays one spends very little time reaching for floppy disks; it is quicker and easier to send fairly small files as email attachments, or if the files are large, using zip disks or re-write able CD-ROMS.

Be very wary indeed of attachments from unknown senders, or messages even from known senders, which have suspicious attachments. Your antiviral software really should check email attachments, whether incoming or outgoing. Remember that if the attachments have the following extensions (.EXE, .COM, .BAT or .VBS), they are actually programs and are potentially risky...

It is possible for such an attachment to be sent in error from a known sender (Remember that's how they are usually spread after all! Witness the Melissa Virus, for example). Unless you are expecting to receive such an attachment, it's safest to delete it. In order for such a virus or other malicious program to do any harm, you must actually open the attachment (remember that opening an attachment of this type actually runs the program!). Remember that more usual types of attachment such as images (files having extensions such as .JPEG, .JPG, .BMP, .PNG for instance) or plain text (.TXT) are harmless, as they contain no program code. Please note that files such as formatted documents (for example Microsoft Word/Excel) having .DOT, .DOC, .XLT or .XLS for example, are not programs, however these can contain macro viruses, so in Word or Excel always disable macros unless you are expecting to receive them. Should the macros be legitimate, then disabling them may lose you some functionality; however the file contents will be left intact. Should you receive files with extensions such as .ZIP, these are compressed archive files, which can be opened with WinZip or other compatible software. Compression is useful as it reduces the file size making it easier to email. Although the archive in itself is harmless, do check the contents before opening! For a comprehensive list of file types and their associated extensions, visit www.whatis.org.

Besides picking up a virus from an e-mail attachment, you can acquire a virus or worm from files you download from a Web site, or on a diskette someone shares with you. If your computer is not virus protected, once you download and run the program, the virus can spread. Viruses can sometimes spread around the world in a matter of hours. But even after a virus is no longer mentioned in the news, it may still be active and can continue to harm computers that are not protected. Here are some examples of the harm they can cause;

They can make numerous copies of itself, possibly filling up your hard disk over a period of time;

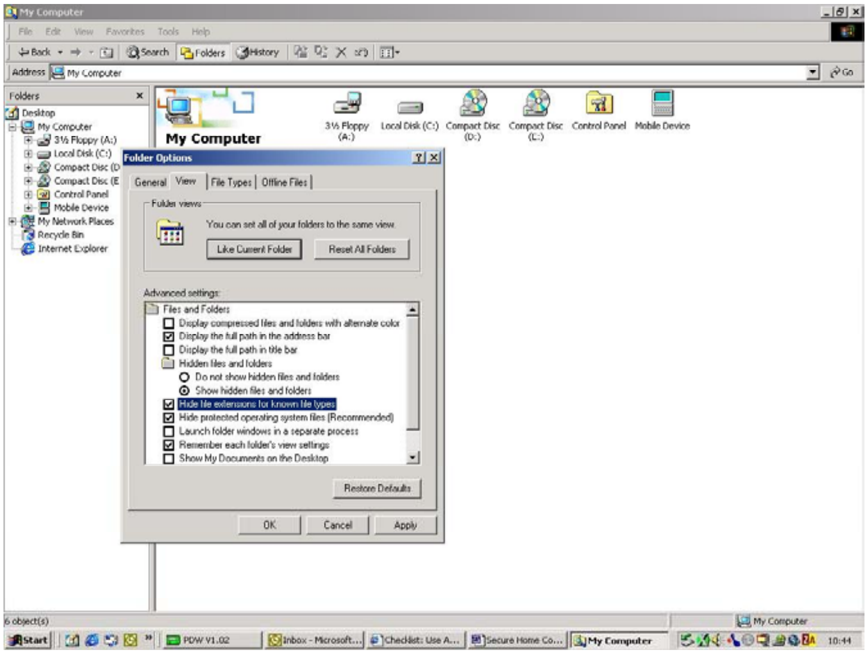
Send copies of itself to everyone else on your e-mail list (via the address book), embarrassing and unpleasant to your friends who may never trust you again;

Reformat your hard drive and/or delete your files and programs;

Install hidden Trojan horse programs, in order to distribute obscene material or pirated software for instance, that can be distributed and sold using your machine (without your knowledge, yet possibly leaving you legally liable!).

Here, there is another word of warning. Programs such as Windows Explorer have an option to hide file extensions. This is enabled by default when Windows is first installed. Virus authors are known to exploit this in order to hide the true file type, even adding a visible false extension, in order to make the file appear harmless. For example, Games.txt.vbs will appear as Games.txt with the extension hidden! Remember that should a file appear to have more than one extension, it's the last one, which counts! To show all extensions, and give you some peace of mind, do the following:

Open Windows Explorer. Under the tools menu, choose folder options. Next, on the view tab, uncheck the 'hide file extensions for known types' option. This will allow you to see the full extension for *all* files. This is illustrated below:



Folder Options

Folder views

You can set all of your folders to the same view.

Advanced settings:

Files and Folders
- ☐ Display compressed files and folders with alternate color
- ☑ Display the full path in the address bar
- ☐ Display the full path in title bar
- Hidden files and folders
  - ○ Do not show hidden files and folders
  - ● Show hidden files and folders
- ☑ Hide file extensions for known file types
- ☑ Hide protected operating system files (Recommended)
- ☐ Launch folder windows in a separate process
- ☑ Remember each folder's view settings
- ☐ Show My Documents on the Desktop

If you really must open attachments before you can verify the source, take the following precaution:

Be sure your antiviral software is updated;

Save the file to your hard disk (Preferably in a directory containing no other files);

Scan the file using your antiviral software;

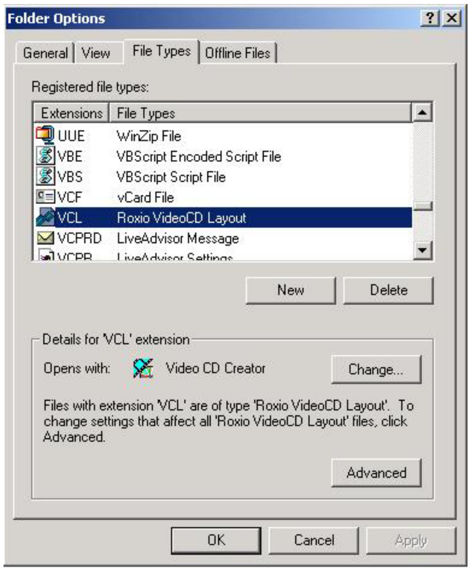
Disconnect your computer's network connection before opening the file;

Then open the file.

It is best not to send executable files as email attachments, just as a precaution. You may inadvertently be sending viruses to other people! If you do want to send this type of file, then virus scan it first, and package it in a .zip, .gz or .sit archive, depending on whether the intended recipient is running Windows, Unix or Macintosh respectively. (An .exe file is an MSDOS or Windows program anyway, so it's probably of little use to Unix or Macintosh users).

Recently (September 2002) one company (Messagelabs) reported that a as many as 1 in 24 email attachments contained a virus of some description! Furthermore, some message processing software, such as Exim, returns messages with this type of attachment (.exe) to the sender anyhow. And as for VBS attachments, you have no reason to deliberately send such a file as an email attachment, unless you are working on a joint Visual Basic program with someone else.

You can render these programs harmless by removing the file association. To do this, open Windows Explorer. On the file menu, select 'folder options', and then 'file types, as shown below:



Registered file types:

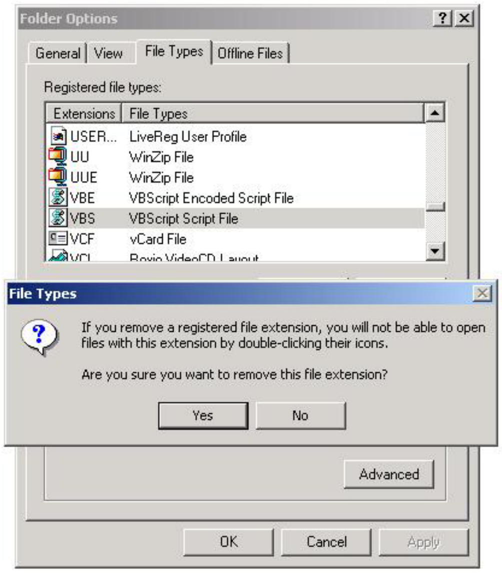
Extensions	File Types
UUE	WinZip File
VBE	VBScript Encoded Script File
VBS	VBScript Script File
VCF	vCard File
VCL	Roxio VideoCD Layout
VCPRD	LiveAdvisor Message
VCPR	LiveAdvisor Settings

Details for 'VCL' extension

Opens with: Video CD Creator

Files with extension 'VCL' are of type 'Roxio VideoCD Layout'. To change settings that affect all 'Roxio VideoCD Layout' files, click Advanced.

The registered file types are shown alphabetically. Find the 'VBS' entry and disassociate it with a Visual basic Script'; to do this, click 'delete', you should now see this dialogue:



Registered file types:

Extensions	File Types
USER...	LiveReg User Profile
UU	WinZip File
UUE	WinZip File
VBE	VBScript Encoded Script File
VBS	VBScript Script File
VCF	vCard File
VCL	Roxio VideoCD Layout

File Types

If you remove a registered file extension, you will not be able to open files with this extension by double-clicking their icons.

Are you sure you want to remove this file extension?

Now click 'yes' – this should render this file type harmless. Do the same for an encoded Visual basic Script (having a .VBE extension). The same procedure can be followed for other types of suspicious file; (But not for EXE; if you do then you won't be able to start any programs!!!). Please note that I am using Windows 2000; the version of Windows Explorer which ships with other versions of Windows may appear slightly different.

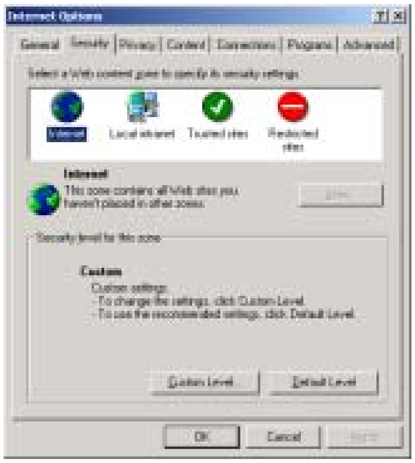
8) Web Browser Security

Web browsers can, and should, be configured to limit vulnerability to intrusion. Since web browsers are installed, and in frequent use, on virtually all computers, and as their purpose is to communicate directly with other (possibly untrustworthy) computer systems, Web browsers present a serious threat of security and privacy compromise. This is due in part to the fact that they lack many security protections, and those which are provided are not set very securely by default following installation. For example, 'plug-ins' which allow content other than web-pages (such as video/audio content, Microsoft Office documents and spreadsheets, and Adobe Acrobat documents, for example, should be limited to only those plug-ins actually required by the end user. Active content, for instance Java applets, and particularly JavaScript and Activex controls, should be disabled or used only in conjunction with trusted websites. Although the advice is tailored to Microsoft Internet Explorer and Netscape Navigator, the principles apply equally to any Web browser.

The browser itself should be kept up to date as new vulnerabilities come to light. Privacy is also a serious concern whilst you surf the web. Cookies are the best publicised threat, and can be disabled entirely, or as a less drastic measure, may be selectively blocked via use of browser privacy settings, or better still, third-party applications.

There are several ways in which you can improve security in your web browser. Many website designers wish their pages to do more than simply display information. Automated online shopping sites, for example, often make use of programs which are launched from their pages, and which run on your computer, rather than the web server. The downside is that the programs employed can be either poorly written, or tested, or worse still, downright malicious.

Scripting languages, such as JavaScript, have been a known source of security risks whilst surfing the web. Many browser-based security risks involve active scripting and usually, but not always, another software design flaw. For example, there have been some high-profile attacks that allow unscrupulous web sites to copy personal files from the end users computer. From a security point of view it may be desirable to disable all scripting; however, many perfectly reputable sites also make perfectly legitimate use of scripting. Therefore, disabling it may result in a loss of functionality, and may render a small minority of sites completely unusable. There are a few pages which display only scripting, and if disabled, the page will appear blank. Therefore, it may be desirable to disable scripting for most sites (the 'internet' zone in the 'Internet Options > Security' toolbar of Internet explorer, and add those trusted sites to the 'trusted sites' list:



Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones.

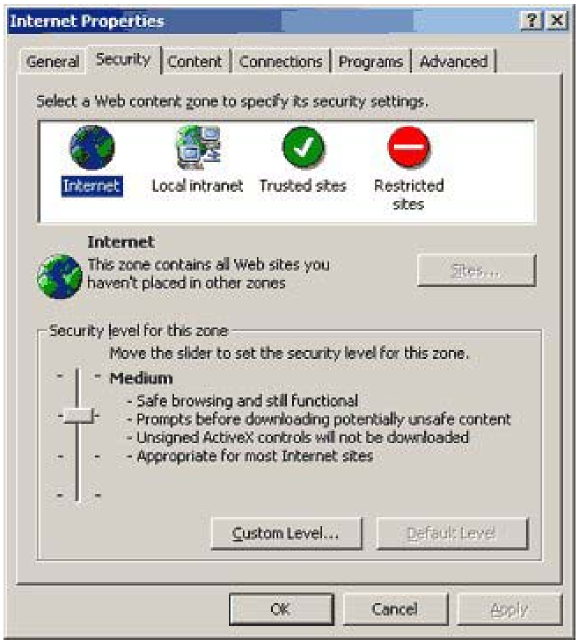
Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

The ‘restricted sites’ list should employ the ‘high’ security level (see the ‘custom level’ menu. The ‘trusted sites’ list may use either the ‘low’ or ‘medium low’ default level, as can the ‘local intranet’ list. The ‘Internet’ list incorporates all sites not added to another list, and may use the ‘medium’ security level at minimum – however I still recommend editing this level using the ‘’custom level’ button, and disabling cookies and active scripting, for both security and privacy reasons, as explained below.

The Java programming language is designed so that a program written in Java cannot take control of your system; therefore Java programs (not to be confused with JavaScript, which is unrelated to Java, and whilst easier to learn, has none of the security protections of Java), are harmless except for a relatively small number of bugs which have been discovered. However, unbeknown to most people, Microsoft have their own scripting system (Activex) which is intentionally designed so that Activex programs can have full, unrestricted access to, and control over, *your* computer. Microsoft really is bent on world domination! This, amongst other things, means that Activex controls can be malicious, namely they can do almost anything that the programmer wishes.
This is because applications are ‘digitally signed’ by their developers using a signature scheme known as Authenticode, which revolves around comparing each control with a known ‘certificate’. Security is therefore left entirely in the hands of the software developer, and the user’s background knowledge of security!
The Authenticode process does ensure that ActiveX applets cannot be distributed anonymously (i.e. without the user being aware whether the control is signed or not), and a signed control is protected from interference such as reverse-engineering. The ActiveX certification scheme places the responsibility for the computer system's security entirely in the hands of the end user. This does not work well in the real world, as most end users are unaware of the risks involved.

You may feel safer if you disable scripting except for the ‘Trusted Sites’ zone. This procedure will also render many of those annoying advertising banners inoperative (although see also JavaScript). Have you ever encountered any of those sites which, once you access their server, launch browser window after browser window faster than you can close them, until your system runs out of memory (or you reboot in order to regain control). This procedure may also disable this kind of malicious action. As always however, do bear in mind that there is always some trade-off between security and convenience. Remember that you may loose some legitimate functionality on some websites. To turn off ActiveX and Java in Internet Explorer: Under the Windows Start menu, select the Settings > Control Panel command. Double-click on the Internet Options icon in the Control Panel window. Next, select the Security tab in the Internet Properties dialog box. Select ‘Internet zone’. Click on the Default Level to make sure that the Internet zone is *at least at the Medium level*. Next, push the ‘Custom Level’. button.



Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

Security level for this zone

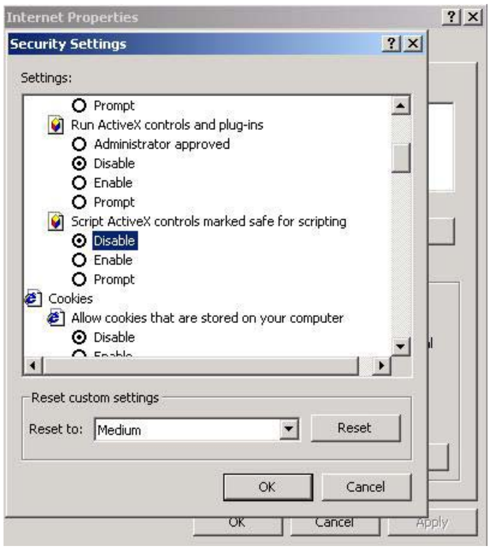
Move the slider to set the security level for this zone.

Medium

- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

Scroll down to the setting labelled "Initialise and script unsigned activex controls" in the Security Settings Dialog box and check the Disable option. You may also wish to disable activex controls marked safe for scripting, should you wish. Remember, the unsigned controls present the most risk. Note, by changing only this setting, ActiveX controls are effectively disabled. No annoying warning messages are displayed if a page attempts to use an ActiveX control.

To disable scripting in Microsoft Internet Explorer:
Select ‘tools’ form the toolbar, then ‘Internet options’. Next, select the ‘Security’ tab. Ensure that at least the ‘medium’ security level is selected (this prompts before any activex controls are downloaded); or if you want to disable Activex totally, select the ‘high’ security setting. As I mentioned earlier, the content of some sites will not function correctly. Lower the security level only before visiting sites that you trust, and reset it afterwards.
If you want to run at the medium security level, then again scroll down to ‘Script ActiveX controls marked safe for scripting’ and select the ‘disable’ option. The checkbox should look like this:



Settings:

○ Prompt
Run ActiveX controls and plug-ins
○ Administrator approved
● Disable
○ Enable
○ Prompt
Script ActiveX controls marked safe for scripting
● Disable
○ Enable
○ Prompt
Cookies
Allow cookies that are stored on your computer
● Disable
○ Enable

Reset custom settings

Reset to: Medium

You should now be safe from any malicious Activex controls.

To disable scripting in Netscape Navigator (Version 3 or higher):
Start Netscape Communicator. Under the ‘edit’ menu, select ‘preferences’. Then under the ‘category’ list, click on ‘advanced’. Should you wish to disable JavaScript, uncheck ‘enable JavaScript’, but leave Java enabled as the two are not in fact connected – Java is generally safe. Then press OK to accept the changes.
Next, click the padlock icon in the bottom left hand corner of your browser. The security ‘info dialog box should appear. Then click the ‘Navigator’ link from the list. The Navigator security settings box appears. In the ‘show a warning before’: area, make sure the options ‘Viewing a page with encrypted/unencrypted mix’ and ‘leaving an encrypted site are checked. Lastly, click OK to accept the changes and close the dialog box.

To also disable Java should you wish, scroll down to the "Java Permissions" selection, and check the disable option here. Java is ostensibly safe, but it has its flaws. Java applets, unlike Activex controls, run in a protected memory area known as a ‘sandbox’. So on the whole, there is minimal risk from Java applets. However JavaScript – rather than Java – can actually be more of a pain than it’s worth. You may well want to disable Javascript simply for the sake of being able to surf in peace! Do note that this will prevent some pages from displaying correctly, and some online forms will likewise be disabled.
There are some highly annoying features to put up with when surfing the web! Some sites will constantly bombard you with intrusive and annoying advertising windows and banners, whereas others keep displaying stupid "alert" messages. There are even some who keep constantly redirecting you to other pages against your wishes. And the ‘back’ button won’t get you out because it is disabled.
Of course, Javascript does have some good uses, but these are relatively few in number and none are essential. You may wish to consider ‘ad-blocker’ software as an alternative to disabling JavaScript if you prefer. Disabling JavaScript does certainly disable the worst annoyances of all – these include web pages that "trap" viewers, for example they may disable some functions, such as those on your edit menu. They may force themselves onto the top Window, spread themselves across your full screen, and

take away your back button, address bar, and toolbars. You will probably agree that these are online experiences we'd all rather do without.
Javascript can be disabled using the above menu. Disable 'active scripting' to accomplish this. (You may want to put sites which you trust onto your 'trusted sites' list, allowing more relaxed settings to be used when browsing these sites).
Remember that disabling Activex or JavaScript will inevitably disable some useful web content or functionality. If you regularly visit trustworthy sites which utilise these scripts, add them to your 'trusted sites' list. In Internet explorer, this is accomplished using the 'tools' menu. Select 'Internet Options', and select the 'security' tab. Highlight the 'Trusted Sites' icon, and click 'sites'. You can now type or paste in the name of the site. Click 'OK' to enter the information. From now on, your browser can utilise a lower level of security when you visit these sites. A 'trusted sites' icon is displayed in the lower right of the browser window confirming that you are visiting a site which you have added to this list.

Disabling Cookies:

Have you ever read George Orwell's book '1984', which pictures life in a world in which your every move is being scrutinised by an all powerful, pervading government? I have, and although we have thankfully been spared the horrors of a police state, we are certainly being watched more than we realise whilst online!
One means by which sites (and individuals) can find out who you are is via your email address. There exist a number of databases which allow them to do this – or they could possibly do so via packet sniffing – which is explained later. You may often type your email address into online forms, when registering at a site, for example.
Some cookies are justified, as a legitimate means to 'personalise' your browsing experience. For example, many sites use them to identify you as an individual visitor, so that you do not have to re-enter the same details on each subsequent visit. For example, some web sites offer users the option of "remembering" their password or retaining information used in greeting the user at the beginning of subsequent visits. This is an example of a legitimate use of cookies, which allow the web server involved to save the user record on the computer's hard disk. This information allows a visitors preferences to be retained for later retrieval. Many online shopping sites use cookies to associate a user with a particular shopping cart; they are using the cookie to track a user around their own site. This is a convenient feature when used for its intended purpose.

However, during a given week my firewall blocked just over 6000 cookies, during which time I had not visited any sites requiring me to enter any such information into an online 'form', for example, nor had I ordered anything online either – some sites which take debit or credit card purchases utilise cookies simply as part of their own security scheme. So in short, there is no 'legitimate' reason for many sites to use cookies, yet the vast majority choose to do so.
If not used with care by the web sites that use them, cookies can in themselves create a Serious risk to your privacy. As cookie data is not encrypted; as a result, anyone with access to your hard disk can view your cookie data, for example, your boss may do this to find out what you have been doing on your PC! This is an even more serious risk where sensitive information (such as account or credit card numbers, for example) is stored as a cookie.

The most frequent use of cookies online seems to be to track users around various sites, often without their knowledge. For example, companies such as Double-click are known to share cookie information. This type of sharing can give a third party access to personal information. The usual method is for many separate companies to display files (usually images) on their own pages, which are in fact loaded from Double click's server, allowing Double-click an opportunity to place a cookie on your system, even though you never consciously visited double click's own site! This allows a number of sites to share cookies, allowing a profile of your browsing habits to be compiled over time. Here is precisely how these companies collect your personal data, and construct a user profile:

An advertising network creates a large network of sites that display their advertisements. These advertisements are retrieved from the advertising company's site, not the site which you are intentionally visiting! This allows them to place a Cookie on each and every visitor's hard drive, given that the cookie is not blocked. They often also log other details, such as the date, time, member site visited, and the IP address of the user's computer. Even though you did not ever visit the advertiser's own website directly, they can certainly keep details of those sites you did visit. Some sites, in particular those which directly sell a product, require user registration. They require you to provide contact details, along with your debit/credit card number. This gives them, amongst other details, your email address.

If your email software, for example Microsoft Outlook, supports HTML e-mail messages, these may contain images which may be fetched from the advertiser's site. This then gives away details such as the date and time of access, and confirms that the email address is used regularly. It also log's the IP address of the customer's computer. This happens even where the cookie was blocked by a firewall, for example. So, simply by receiving an email, a profile can be constructed for each and every user... This behind-the-scenes activity is often invisible to you. Unless you have set your browser preferences so that you will be alerted whenever a cookie is being placed on your computer, you won't even know about it at the time. When you later return to the same web site, you won't be aware that a cookie is being retrieved from your hard disk. Most people will not have their preferences set up to alert them to cookie activity, either because the browsers are not set up this way by default, or because cookies are used so extensively that the alerts are frequent enough to be a source of annoyance.

Actually, many sites do indeed use cookies' to track your every move whilst online. So called 'banner ad' sites such as Double-Click are particular offenders in this respect. (This is in much the same way as many supermarkets employ so-called 'reward cards', ostensibly to save you money, yet in reality, they waste your time, and the cashier's time, simply to gain information relating to your shopping habits. I do not agree with this simply by principle; and anyway are there not more obvious and genuine means to save their customers money? And furthermore, the hidden cost of running such a ludicrous scheme is silently passed on to you, surely?).
From a performance point of view alone, do you really want your hard disk to become cluttered up with hundreds of thousands of cookies? Such a huge number of small files represent a very inefficient use of disk space indeed.

Cookies are small files that are placed on your hard drive by various Web servers. They are commonly used by marketers to track your browsing activities as you surf across sites.

A cookie is a small text file (.TXT); it contains a unique identifier that a web server places on your hard disk: They contain a unique serial number used to retrieve your records on the next occasion you visit their site. These cookies can persist for years afterwards, often with neither the user's knowledge or consent. If you look in your 'cookies' directory you may see the links to web sites that you cannot even remember visiting! If you use search engines, the queries you type are often logged also! Although as I have already mentioned, some sites do use them for legitimate purposes, some less reputable ones do use them to facilitate the collection of personal information or to infringe upon your privacy. For this reason, you may well wish to either disable cookies within your browser, or preferably configure your firewall to block them. In general, if you care about your privacy, you may wish to completely disable cookies, and enable them only briefly when needed (for example when shopping online), and disabling them afterwards. A more elegant solution would be to make use of a cookie management package, or to configure your firewall to block them. For example, software firewalls such as Zone alarm Pro and Norton Personal Firewall have this capability. Zone labs also offers 'Internet Cleanup', which manages cookies, and also plug-ins, hidden links, and suspicious active content.

How to disable cookies:

A 'cookie management package' is one possible means by which to safeguard your right to privacy. These can be configured to accept those from certain sites which use cookies for legitimate purposes, whilst blocking others. (Sites which use them for legitimate reasons normally inform you when an attempt to place a cookie fails). Disabling all cookies may cause you to be locked out of a small number of sites that require cookies to access their facilities, for example hotmail.com. (Personally I don't much like hotmail myself; I prefer proper SMTP email services as I find them more convenient – hotmail messages can be read only at hotmail's pages, and the advantage of SMTP is that when you press send & receive, the messages are retrieved, and then deleted from the mail server. This means that the messages are not stored on the server for a long period of time. There are some security advantages here, and if you receive a lot of attachments, you won't run out of storage space on the server, which will result in any further messages being 'bounced' back to the sender. Also, with SMTP your mail client can be set to check regularly for new messages, which is particularly useful if your connection is 'always on'.)

To avoid this, you can install cookie management software that will let you block all cookies but the required ones. If you don't have a cookie management package, you can also configure your browser not to accept cookies, or to warn you before a cookie is placed on your hard drive. On Windows 9.X systems, this is in C:\Windows\Cookies, by default; for Windows NT/2000/XP this is in C:\Documents & Settings\Username\Cookies, where 'username' is your login name. Also, check out the 'Temporary Internet Files' directory, which is located in either c:\windows or c:\winnt and the 'Local settings' directory also. Press control-A to select all cookies, and then right-click and select delete. This will remove all cookies already on your system. Having done this, go to the recycle bin and empty it. Note that if you are using Windows NT/2000/XP at work, note that the system administrator may well have prevented you from accessing these directories directly via NTFS file permissions. In this case, you must simply be wary about your use of the Internet, so as to avoid getting cookies placed there in the first place! A very important warning is needed in this point:

💣

As cookies bear filenames related to the web pages and sites visited, be extra careful about your browsing activities at work! Remember, if for example they bear evidence of a visit to www.sexonline.com, say, a cookie could loose you your job! In addition, the timestamp also tells them whether or not the visit was in office hours or not. This is another reason for removing existing cookies, and then blocking them in future. Remember, it may not always need a visit to your computer by an administrator to check on your usage; your use of your PC may be monitored remotely via the network, so take care…

Note: Earlier browsers unfortunately only allow you to reject each and every cookie, rather than refusing them automatically. You may wish to upgrade your browser in this case.

Disabling cookies under Netscape 3 or earlier:

Select 'Network Preferences', then 'protocols'. Under the 'show an alert before' menu, check 'accepting a cookie'. (Then save your setting.)

In Microsoft Internet Explorer 3.0: Select 'view', then 'options', and 'advanced', select the 'warn before accepting cookies' box.

On Netscape Communicator 4.0b2, go to the 'edit' tab, then select 'preferences', and 'advanced', and click 'never accept cookies', or if you prefer the 'warn me before accepting a cookie' box.

For Microsoft Internet Explorer versions 4 and above: select 'view', then 'internet options', and 'advanced', then scroll down to the 'security' box. Select 'cookies', and 'disable all cookie use'. You can also right click the Internet Explorer shortcut on the desktop, select 'properties', followed by 'advanced', then scroll down to 'cookies', and finally select 'options'. Then save settings. As some sites use cookies as part of their own security scheme, for example those which take payments via credit or debit cards, you may well want to enable cookies only when you require them.

Alternatively, a compromise is to use the 'prompt' setting – your browser will ask for your permission before accepting a cookie. You may be astounded at how often the prompt dialogue box appears whilst you surf!

To frequently get rid of cookies 'at start-up', you can write a batch file to be run automatically, or do so from the Autoexec.bat file in Windows 9.X. The command is: 'del c:\windows\cookies\*.*' for Windows 9.X or 'del c:\documents & settings\username\cookies' for Windows NT (Including Windows 2000). Note: take care to specify the directory carefully!

Many firewalls will allow you to block cookies. This is easier if:

You use more than one browser;
Different users of your computer prefer different browsers;
You have more than one logon account per computer.

Note that some websites (a small minority) will not function if you block cookies. They may be purposely set up in this way! A very small number will deny you access altogether. However, if a condition of use is that you let them intrude into your privacy, then ask yourself the following question; do you really want to visit them anyhow?

Security Vulnerabilities Involving 'Plug-ins':

Firstly, we need to understand what a plug-in actually is, and what functionality it has. A browser plug-in is a (usually hidden) program which allows your browser to handle file types not supported by the browser itself. This allows you to view files such as Microsoft Word and Excel documents online as though they were WebPages, rather than having you first download, and then open the file separately. This is equivalent to streaming audio or video over the Internet using Windows Media player or Real player, for instance.
The plug-in is activated automatically when the browser detects the content type associated with it. For example, Adobe Acrobat (and the free PDF reader) come with an Activex control which allows online viewing of PDF files.
Unfortunately, this automatic nature of plug-ins makes them easy to exploit. For example, they can potentially be used to run malicious program code on the computer used to surf the web. Poorly written and/or tested plug-ins, like active scripting, can also contain accidental flaws which may be damaging. In order to reduce risks associated with plug-ins, follow these guidelines:

- Don't download or install plug-ins which you don't need or use. For example, if you use a particular computer exclusively for work-related purposes, you probably need a plug-in to view Adobe PDF and Microsoft Word documents, but not for streaming media.
- Be sure to download your plug-ins from a well known, reputable source. Avoid any offered by shady websites which may not be trustworthy.
- Remove or disable any plug-ins which are not needed, or which you cannot account for.
- Configure your browser to prompt you before running a plug-in. For example, if the Adobe Acrobat Plug-in wishes to run when the file you are attempting to view is not of type Adobe Acrobat (PDF), then this may well be due to someone attempting to launch this particular plug-in in order to exploit a design flaw inherent in the plug-in.

Reviewing and disabling Plug-ins installed in Internet Explorer:

From the Internet Explorer menu bar, select "Tools" and then "Internet Options."
The "Internet Options" window will open. From this window, select the "Security" tab.
Select "Internet" by clicking on the picture of a globe. (See Figure 4.2).
Once Internet has been selected, click on the "Custom Level" button.
This will open the "Security Settings" Window.
From this window, scroll down until you see the "Active-X and Plug-ins" section. There
may be several selections to disable in order to completely disable plug-in and Activex components.

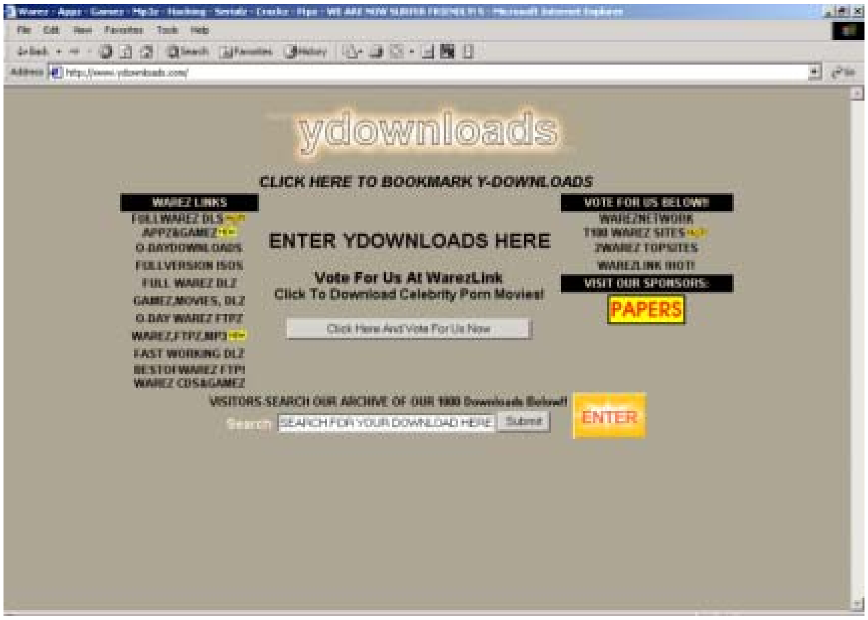
Click the "OK" button at the bottom of the "Security Settings" window.
Click the "OK" button at the bottom of the "Internet Options" window.

To View/Remove unneeded plug-in's in Netscape Navigator:

To review plug-in's that are installed on your machine, enter the Uniform Resource Locator "about:plugins" in the location bar.
From the menu bar, select "Edit" then "Preferences."
Select the "Applications" item from the tree at the left.
A scroll list of various document types appears.
To remove an unnecessary plug-in, select it and press the "Remove" button.
You may also instruct Netscape to prompt you before running plug-in's by clicking the "Edit" button and checking the "Ask me before opening downloaded files of this type" to tell Netscape to prompt you before running a plug-in.

Malicious software (Viruses etc):

These are some examples of means by which by which you may obtain some level of protection from malicious code whilst surfing the web. However, it's best to be careful about which sites you visit. Remember that although there has been a lot of publicity in recent times about copyright theft, particularly on the part of the RIAA, in fact there is much worse material out there, including malicious program code and offensive material. See my section on content filtering, for example.
There are numerous sites, which you can find which are offering illegal copies of software, movies, obscene material and such like – at a price. The nature of the Internet is such that it is often easy to stumble into such sites by accident, for example by typing a wrong keyword into a search engine. Once there, then very often it is made deliberately difficult to get out – for example, you may find that the 'back' button is disabled and you are bombarded with numerous browser windows, which appear faster than you can close them, to tempt you with still more illicit material. Below, I have an illustration of a site, which I chose as an example of the type of site at which you may get into trouble of this nature:



Here, 'ydownloads.com' is offering numerous examples of what's really best avoided. Be very wary of sites, which use words such as 'pirate' and 'warez', for instance. These are the kind of places where you may well receive malware or malicious cookies, for instance. Where these people are prepared to openly flout the law in this manner, they probably have equally little regard for you, your children, your privacy, or your computer.

In order of preference, here are the methods by which to get out of such a site. The methods are listed roughly in order of preference:

- Try using the alt-tab and alt-F4 shortcuts to close the Windows as they appear. This is far quicker and easier than attempting to click on the 'close' tab of numerous pop-up windows of different sizes.
- Or, use control-alt delete. In Windows 9.X, highlight your browser and select 'End Task' to kill your browser windows. It's a little drastic, but better than re-booting your computer to escape, (or when so many Windows are active that you run out of memory). In Windows NT/2000/XP, select the task manager and use it to terminate your browser.
- You may of course disconnect your modem or network cable. Then close your browser, save any open files, then re-boot before re-connecting.
- If you really have no choice, then you may have to re-boot, if none of the above methods work, then be sure to clear this site from your history list.

You may wish to check for any cookies or files, which may have been left behind after the event, and run a virus scan in case of Trojan horses. Do this after restarting your system – *and as soon as possible*.

There are also unfortunately, less obvious signs that someone may have access to or control of your computer. These include:

- A sudden or unexplained slowing of your connection;

- An sudden escalation in disk activity, for example, even though you are not placing any demand on your hard disk, for example by opening or saving files;
- Files appearing on your hard disk without knowledge or explanation. Or, of course, files which are mysteriously vanishing or being modified!
- If you get any messages such as 'access/sharing violation' on attempting to open a file. And the file is not already opened by another application, or can be opened by a legitimate' user on your private network. If none of these can possibly be true, then the chances are, someone is accessing your files right now!!!
- If you get any messages as you attempt to shut down or log off, such as 'there are currently users connected to your computer. Shutting down will disconnect them. Are you sure?' If you are not part of a private local area network, beware, you have just caught an intruder in the act…
- Your external modem or network interface card will usually have a 'data transfer indicator'. This should not be flashing at all, (or only very intermittently) when you are not sending or receiving data. Where it is flashing rapidly, where you are not even currently using your connection, this is probably a cause for concern – the indicator should have no business to be doing so! Internal modems are at a disadvantage here, as they do not normally possess this indication, at least not where it is visible from in front of the computer.

Some of the above activities can occur for other reasons than intrusion, for example occasionally a file may not have been correctly closed due to a program crashing. And a few data packets are sometimes transferred continually, for example routing packets on cable modem networks. Also, verify that you have no sharing programs running, for example Bearshare, which can be configured to load on start-up.

To find out who is currently connected to your computer, open an MSDOS or command prompt Window and use the 'netstat' command to list the connections. Look for any you cannot account for. You may wish to note the IP address, and find out whom it belongs to. All service providers have an abuse section, and you may wish to send them an email regarding their 'browsing habits'. The address is of the format 'abuse@serviceprovider.com'. See also my advice later regarding the tracing of IP addresses, antiviral software, and firewalls.

---

9) Why can intruders break into your computer?

Software and operating systems are written and designed by human beings, who can make mistakes. Given that modern software engineering is extremely complex by comparison with many other engineering disciplines, and that it is also a comparatively new area of engineering, i.e. there is relatively little previous experience to fall back on, it is inevitable that 'bugs', or namely design flaws will tend to emerge from time to time. Add to this the overwhelming to rush software (and almost any other!) product to the market before it's particularly well designed and tested, and you can envisage the problem. System Administrators and Programmers alike can never track down and eliminate all possible flaws. And a hacker may need only to find one flaw, which they happen to know how to exploit, and they're in…

Security Flaws: Some background information

The problem is somewhat involved, however I'll try to be as straightforward as possible. Here are the flaws which give rise to vulnerabilities…

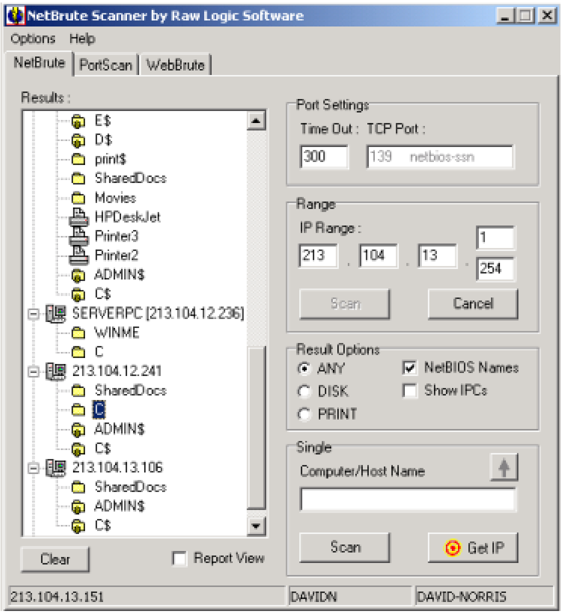
Buffer overflows: Many flaws security holes you hear about are related to this problem. Say that, for example, a program needs to accept the user's telephone number as an input. To use this as an example, when you purchase a product online, you may be asked for your telephone number (so you can be contacted when the need arises). You can expect three digits for the country code (044 for the United Kingdom), five for the area or STD code, and six for the number. A total of 14 digits, and no more? A hacker may want to attempt to enter, say, 1000 digits. As the 'array' (a small area of memory set aside to take this input) may well overflow, it is possible to overwrite a portion of the operating system or another program, causing your system to crash, and possible loss of unsaved data.

Remember that whenever a new service or operating system is released (Most recently Windows XP at time of writing), then within weeks some new susceptibility will come to light. Almost immediately, there is an escalation in the number of probes for the service involved – and yet the first service packs or 'patches' my still be weeks away. At least take advantage of these once they are made available! Do bear in mind however, that should you need to re-install the component involved, the service pack must be installed also.

Multiple Inputs: Most programs are written to handle valid input. Most programmers do not consider what happens when somebody enters input that doesn't match the specification. Even where they do, it is hard to foresee every possible input and it's possible outcome. Indeed, there are no standards relating to the handling of multiple or invalid inputs to a system.

Default/supplied configurations: Most systems are shipped to customers with default, easy to use, configurations. For example, Windows 9.X (when installed on a new system) comes without any password protection. Even where a password is required, hit escape and you're in. It won't let you access a network, but you still have full control of that PC. It's very convenient, but also totally insecure. (Windows NT and 2000 by default, insist on a correct password). Little wonder then, that Microsoft has long been criticised for the lack of product security. At least in Windows 2000, security is quite good.

Unprotected Windows file shares: Having 'File & Printer Sharing' active on a PC which is directly connected to the Internet will share any files in shared folders to the whole Internet! Should you share the root directory of your hard disk, all files in all directories may be accessible – they may be read-only, or if full access is allowed, the files can be easily modified or erased by a remote hacker. There are a number of programs which can find these shares, such as the NetBrute scanner provided by Rawlogic Software (shown below), or the Legion Netbios scanner featured later on.



Results :

```
E$
D$
print$
SharedDocs
Movies
HPDeskJet
Printer3
Printer2
ADMIN$
C$
SERVERPC [213.104.12.236]
    WINME
    C
213.104.12.241
    SharedDocs
    C
    ADMIN$
    C$
213.104.13.106
    SharedDocs
    ADMIN$
    C$
```

☐ Report View

Port Settings
Time Out : 300   TCP Port : 139 netbios-ssn

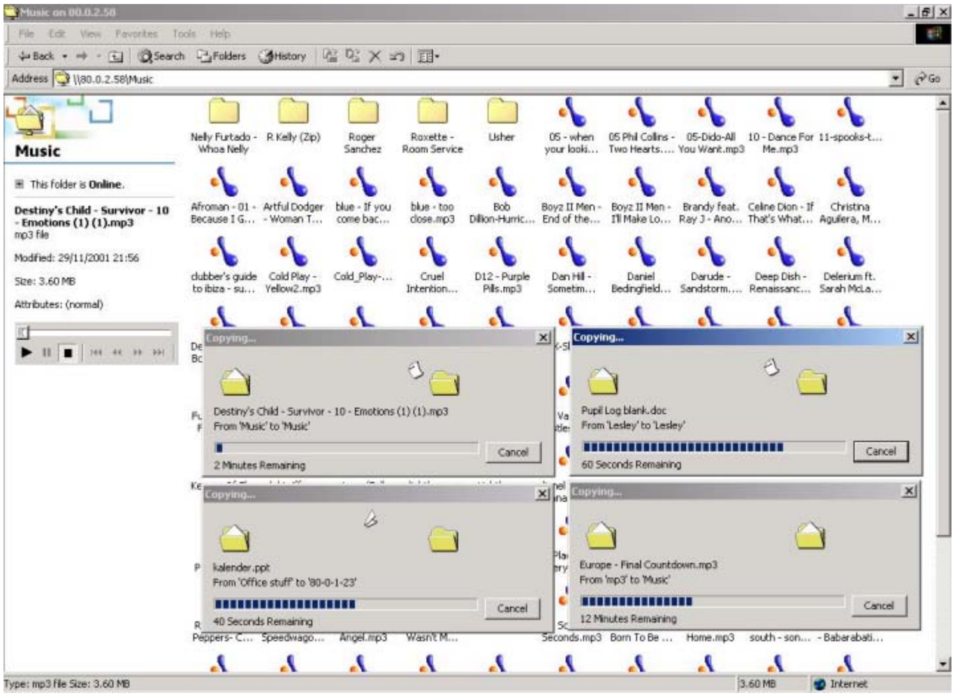
Range
IP Range : 213 . 104 . 13 . 1 – 254

Result Options
● ANY   ☑ NetBIOS Names
○ DISK   ☐ Show IPCs
○ PRINT

Single
Computer/Host Name

213.104.13.151 | DAVIDN | DAVID-NORRIS

If you thought that ‘peer to peer file sharing’ was entirely about such programs as Napster or Gnutella, you’ve got a rude awakening coming. Here’s what can really happen if you have unprotected file shares exposed to the Internet:



Address \\80.0.2.58\Music

This folder is Online.

Destiny's Child - Survivor - 10 - Emotions (1) (1).mp3
mp3 file
Modified: 29/11/2001 21:56
Size: 3.60 MB
Attributes: (normal)

Destiny's Child - Survivor - 10 - Emotions (1) (1).mp3
From 'Music' to 'Music'
2 Minutes Remaining

Pupil Log blank.doc
From 'Lesley' to 'Lesley'
60 Seconds Remaining

kalender.ppt
From 'Office stuff' to '80-0-1-23'
40 Seconds Remaining

Europe - Final Countdown.mp3
From 'mp3' to 'Music'
12 Minutes Remaining

Type: mp3 File Size: 3.60 MB | 3.60 MB | Internet

This is a screenshot from Windows’ Explorer copying four files from four separate remote computers, completely without the knowledge of their owner. Now, this really is what you call file sharing with a vengeance! Although this was demonstration was ‘set-up’ with the permission of the computer’s owners, this could be happening to you right now…

Remember, tools are available for download, completely for free, which can scan a large IP address range for ‘open gateways’ in very little time. One that was frequently in use a few years back was called ‘mscan’, and this was used against whole networks throughout the UK and around the world. Remember, if you have only one computer, and your firewall logs a single probe, you are probably not alone; the same probe is probably replicated across a large number of computers; and yours just happened to be one of them.

Lazy users: A surprising number of machines are configured with an empty administrator password (i.e. blank!). Or alternatively people use ‘easy to remember’ passwords, such as their girlfriend’s name, or their mother’s name, or even simply ‘password’ or ‘computer’. One of the first things an intruder will do on finding a ‘password protected’ machine or account is to scan for empty passwords or easily guessed passwords. Admittedly, one obvious problem is that, although it is recommended that a password should ideally consist of at least eight characters, and a combination of upper and lower case, maybe with numeric digits also, such passwords are hard to remember and simply end up being written down. And what about those people who are silly enough to write their pin code on their cash cards?

Failing to find an easy password, the intruder can next try a "dictionary attack". In this attack, the intruder will use a program that will try every possible word in the dictionary. This is either by repeatedly logging into systems, or by collecting (not very securely) encrypted password files (*.PWL) on many Windows systems, and attempting to find a match by similarly encrypting all the possible passwords in the dictionary. This takes some determination but it can be done. However, a long complex password provides literally millions of possible combinations, hence my above comment about avoiding short passwords.

An intruder may even try all possible combinations of characters. A four letter password may take just minutes to crack with a custom written program, having around 500000 possible combinations). However, 7character passwords consisting of upper and lower case characters and numbers and punctuation also may have around 10 trillion possible combinations.

‘Secure’ sites *do* proudly claim (usually truthfully) that they encrypt personal information, such as credit card details, whilst in transit. However, there are means by which their security systems can be entirely circumvented, should your own computer be left open to attack! I am not attempting to reveal too much detail, only to demonstrate some potential pitfalls.

What makes a good password?

All users of your system should ideally have their own login account. All accounts should have passwords set. In particular, you need to have a strong, un-guessable password for root (Linux or Unix) or Administrator (Windows NT/2000/XP).

The password you use should aim to make it as difficult as possible for others to guess. This leaves the determined individual with no alternative but a brute-force search using a tool he either creates himself, or obtains from a third party, trying every possible combination of letters, numbers, and punctuation. A search of this kind, even conducted on a computer that could try one million passwords per second (in practice, most machines can actually try less than one hundred per second), would require, on the average, require many years to complete. Here is some advice on choosing a sensible password:

- Don't use a password shorter than six characters.
- Don't use your own name in any way at all.
- Don't use your girlfriend/boyfriend/husband/wife's name, for example.
- Don't use other information easily obtained or guessed about you. This includes car license numbers, telephone numbers, the brand of your car, the name of your street, etc.
- Don't use your login name: (even where it's reversed, capitalised, etc.).
- Don't use a password of all digits, or all of the same letter. This significantly decreases the search time for a hacker.
- Use a word contained in English (or other language) dictionaries.
- Use a password with mixed-case alphabetic characters – where passwords are case sensitive.
- Use a password that is easy to remember, so you don't have to write it down(!), for example on post-it notes near the computer.
- Use a password that you can type quickly, without giving others time to see it.
- Use a password with non-alphabetic characters, namely digits or punctuation.

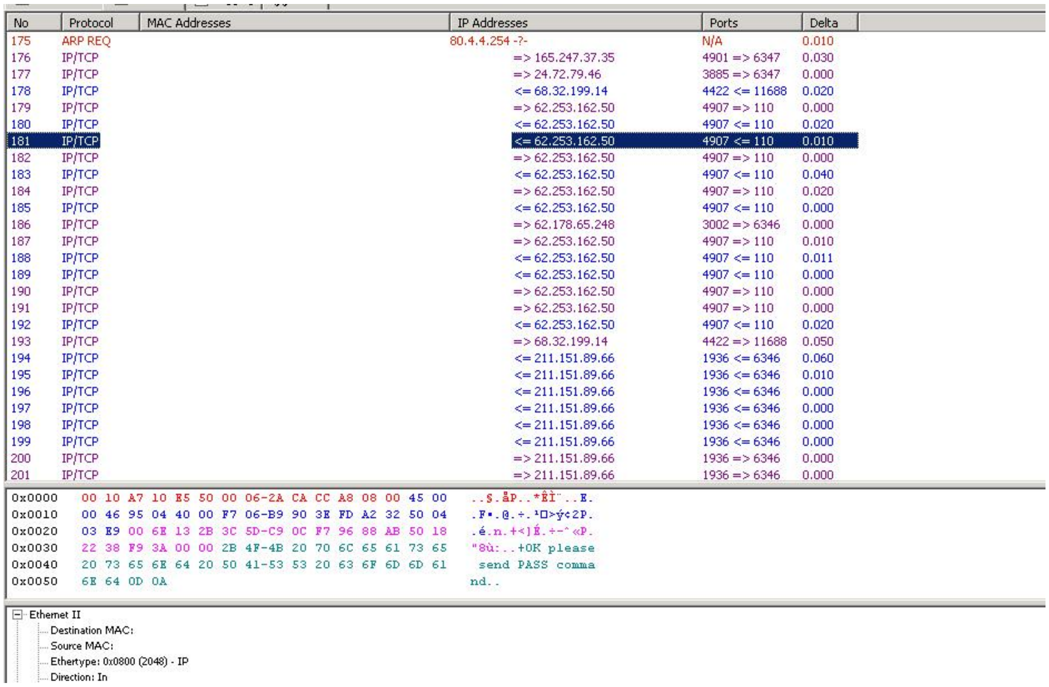
Do any users of your computer(s) keep passwords in world-readable files, such as ASCII text (.TXT)? This is not a good idea! (In fact, users should not keep passwords in any files at all. If the root/administrator account is compromised on your machine then the contents of the file are exposed and this gives the hacker a trivial route into any other computers you may have, and all material stored on them!) In general, avoid writing passwords down; where this is unavoidable keep them well away from the computer, preferably in a different building. Under no circumstances keep them in a readable file (for example plain text!), and then copy this to a network drive or send it via email (horrors)! You should never share them with others anyhow. Here is a tip: On a Windows NT/2000/XP system, passwords are case-sensitive. If your login was rejected, even though you are adamant that your username and password was correct, check that the 'caps lock' light is off. I still make this mistake on a regular basis!
Incidentally, at work you may come across machines which are set up to prompt for a password before actually loading the operating system. This is possible because the system is performing a 'network boot', it is starting from the network. This is possible because the network-card start-up software is run during the start-up period prior to the operating system loading, namely before control is passed to code which is loaded from the hard disk. This avoids the possibility of an employee tampering with the system. However, it BIOS passwords *are* vulnerable as there are some programs available which can read the BIOS password from the CMOS aboard the computer's motherboard, which can possibly also decrypt it, if it is encrypted. However, password authentication is required to get the workstation into a state in which such a program can be run!
It is, of course very easy and quick to open up a PC's case as there are few screws to be undone, and to discharge or disconnect the lithium battery which keeps the CMOS memory alive, where the bios is stored, causing it to revert to default settings. However, some corporate users even go so far as to take precautions such as 'loop alarms' discourage such attacks.

10) Packet Sniffing

Below is an example of a packet sniffer in use. Packet sniffers are able to display and log data as it is sent out ‘over the wire’. They can be used as either a security or hacking tool, depending on how used. You can use them to discover whether a ‘secure website’ actually lives up to it’s promise to encrypt the data to be sent (such as credit card details). On the downside, if you are using an unencrypted service (http, ftp and telnet for example) the username and password are *definitely not* encrypted. So take a great deal of care when using these services. Furthermore, note that if you use a ‘cable modem’ service, i.e. one that delivers your service via a cable television network; as the bandwidth is shared, you are more prone to packet sniffing. As for digital subscriber lines, and obviously standard modem connections are somewhat less susceptible to packet sniffing as each customer has a separate line, but it is still possible. It is even possible to use an ‘inductive wiretap’ to overhear conversations on a standard telephone line or intercept modem data without actually having to splice into the cable. This obviously requires physical access to the cable or distribution cabinet, which may or may not be easily accessible. Remember that having your personal data intercepted by your telephone company or Internet service provider is also a possibility.

In the example below, I have deliberately falsified some of the details (which would leave me susceptible to hacking!), such as my IP address and MAC address. However I have deliberately left the remaining details for demonstration. You can see the traffic passing through my network connection: I chose to highlight a packet belonging to an email check (after pressing send & receive in Microsoft Outlook, for example), and this packet lies between my username being accepted, and the password being sent. Rest assured that the username and password are just as easy to read!

Now for the good news. At any rate, even on a cable modem connection or a corporate LAN, it is necessary to be on the same network segment as the hacker in order for them to read your traffic. For example if your computer’s IP address is 10.1.3.75, only machines having an IP address beginning with 10.1.3. will normally be able to intercept your packets directly. Note that a packet sniffer can be used on your own connection to see what is being uploaded without your permission! It is quite legitimate to do so. This is a packet sniffer called Commview (Vendor Tamosoft, Inc.) in operation:



No	Protocol	MAC Addresses	IP Addresses	Ports	Delta
175	ARP REQ		80.4.4.254 -?-	N/A	0.010
176	IP/TCP		=> 165.247.37.35	4901 => 6347	0.030
177	IP/TCP		=> 24.72.79.46	3885 => 6347	0.000
178	IP/TCP		<= 68.32.199.14	4422 <= 11688	0.020
179	IP/TCP		=> 62.253.162.50	4907 => 110	0.000
180	IP/TCP		<= 62.253.162.50	4907 <= 110	0.020
181	IP/TCP		<= 62.253.162.50	4907 <= 110	0.010
182	IP/TCP		=> 62.253.162.50	4907 => 110	0.000
183	IP/TCP		<= 62.253.162.50	4907 <= 110	0.040
184	IP/TCP		=> 62.253.162.50	4907 => 110	0.020
185	IP/TCP		<= 62.253.162.50	4907 <= 110	0.000
186	IP/TCP		=> 62.178.65.248	3002 => 6346	0.000
187	IP/TCP		=> 62.253.162.50	4907 => 110	0.010
188	IP/TCP		<= 62.253.162.50	4907 <= 110	0.011
189	IP/TCP		<= 62.253.162.50	4907 <= 110	0.000
190	IP/TCP		=> 62.253.162.50	4907 => 110	0.000
191	IP/TCP		=> 62.253.162.50	4907 => 110	0.000
192	IP/TCP		<= 62.253.162.50	4907 <= 110	0.020
193	IP/TCP		=> 68.32.199.14	4422 => 11688	0.050
194	IP/TCP		<= 211.151.89.66	1936 <= 6346	0.060
195	IP/TCP		<= 211.151.89.66	1936 <= 6346	0.010
196	IP/TCP		<= 211.151.89.66	1936 <= 6346	0.000
197	IP/TCP		<= 211.151.89.66	1936 <= 6346	0.000
198	IP/TCP		<= 211.151.89.66	1936 <= 6346	0.000
199	IP/TCP		<= 211.151.89.66	1936 <= 6346	0.000
200	IP/TCP		=> 211.151.89.66	1936 => 6346	0.000
201	IP/TCP		=> 211.151.89.66	1936 => 6346	0.000

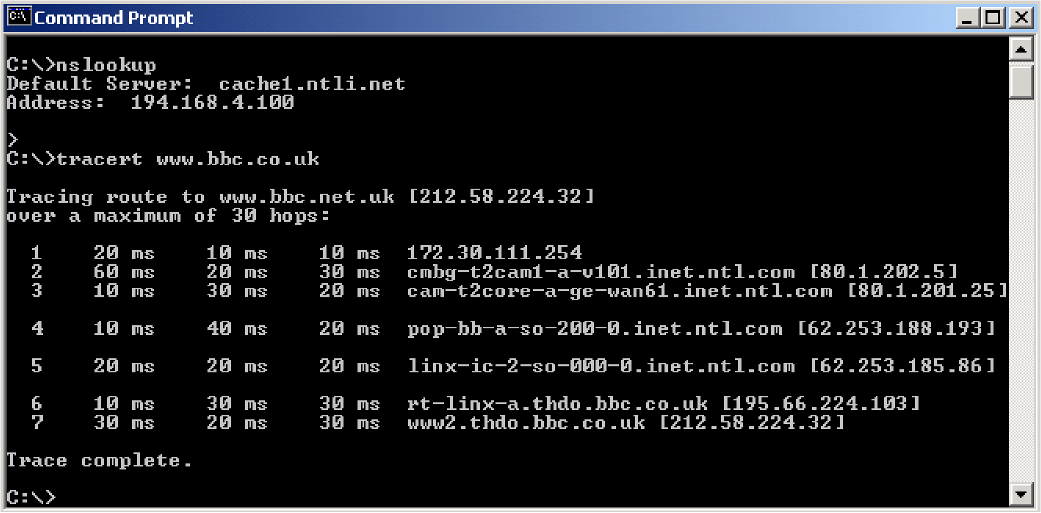
```
0x0000   00 10 A7 10 E5 50 00 06-2A CA CC A8 08 00 45 00   ..§.åP..*ÊÌ¨..E.
0x0010   00 46 95 04 40 00 F7 06-B9 90 3E FD A2 32 50 04   .F•.@.÷.¹□>ý¢2P.
0x0020   03 E9 00 6E 13 2B 3C 5D-C9 0C F7 96 88 AB 50 18   .é.n.+<]É.÷–ˆ«P.
0x0030   22 38 F9 3A 00 00 2B 4F-4B 20 70 6C 65 61 73 65   "8ù:..+OK please
0x0040   20 73 65 6E 64 20 50 41-53 53 20 63 6F 6D 6D 61    send PASS comma
0x0050   6E 64 0D 0A                                       nd..
```

```
⊟ Ethernet II
    Destination MAC:
    Source MAC:
    Ethertype: 0x0800 (2048) - IP
    Direction: In
```

Another example of a packet sniffer in use is presented on the cover page.

Do bear in mind that when you send an email, the message does *not* pass directly from your computer to the recipient's mail server; it's more like an electronic 'pass the parcel' game, where many different machines forward the message to it's final destination. So take note of the fact that as the message is 'spooled' on many machines en route to the recipient, anyone with access to any one of these machines can potentially read your email.

In Windows NT, and Unix, you can use the 'tracert' command to determine the path between your machine and any other on the net. (For Windows, open an 'MSDOS' prompt or command prompt window, and type 'tracert' followed by the IP address or domain name of any other computer. Here is an example:



```
C:\>nslookup
Default Server:  cache1.ntli.net
Address:  194.168.4.100

>
C:\>tracert www.bbc.co.uk

Tracing route to www.bbc.net.uk [212.58.224.32]
over a maximum of 30 hops:

  1    20 ms    10 ms    10 ms  172.30.111.254
  2    60 ms    20 ms    30 ms  cmbg-t2cam1-a-v101.inet.ntl.com [80.1.202.5]
  3    10 ms    30 ms    20 ms  cam-t2core-a-ge-wan61.inet.ntl.com [80.1.201.25]

  4    10 ms    40 ms    20 ms  pop-bb-a-so-200-0.inet.ntl.com [62.253.188.193]

  5    20 ms    20 ms    20 ms  linx-ic-2-so-000-0.inet.ntl.com [62.253.185.86]

  6    10 ms    30 ms    30 ms  rt-linx-a.thdo.bbc.co.uk [195.66.224.103]
  7    30 ms    20 ms    30 ms  www2.thdo.bbc.co.uk [212.58.224.32]

Trace complete.

C:\>
```

In this example, the path is from my own machine to the BBC's web server. You can see that the packets actually pass through six other machines before reaching their destination.

If you are connected to the Internet via a cable modem, the cable modem itself is normally configured more like a 'bridge' than a router in the sense that although it passes some broadcast data packets bound for other computers on your network segment, most of the data bound for other computers is not made accessible to your network card. This means that although in theory your personal data is not available to other computers on your network segment, it is possible for others with the technical knowledge to circumvent this protection. Remember that it is quite easy to 'see' the other computers on your network segment, and add them to your 'network places' wizard. So bear in mind that 'network neighbourhood' can literally mean your neighbourhood if you are on a broadband connection! It is possible to transfer files from one computer one the network to any other, and even print files on somebody else's printer, just as you would on a local area network at work!

---

11) Port Scanning

In order to explain what this type of attack is all about, I first need to explain what ports are. A network port is not a physical port, but rather a virtual one. All possible ports, whose numbers range from 1 to 65536, can either be potentially 'open', namely accepting connections from outside, or closed, in which case no connections are ever accepted by that port number. Another computer, attempting to connect to a closed port, will merely receive an error message in response.

Ports 1 through to 1023 are assigned to specific services as registered to the Internet Assigned Number Authority, and are used by standard services. I can't list them all here, but for example, here are some examples of commonly used ones. A full listing is beyond the scope of this book; however if you would like an exclusive list, visit http://www.iana.org/assignments/port-numbers. Here are some examples:

21: FTP	File transfer protocol: FTP Sites
23: Telnet	Telnet: Useful service, not so well used now, can be misused!
25: SMTP	Your Incoming email
80: HTTP	Web servers (Hypertext transfer protocol)
110: POP3	Your outgoing email
139: Netbios	Windows File & Printer sharing (Not Unix or Macintosh)

Note that although it *is* possible for services to run on other ports than those listed, this is very unusual. For example, it is possible to run one web (http) server on the standard port 80 for public use, and a second on port 81 for private use. By default, a web browser only 'sees' servers on port 80. It is necessary to specify a port number to access servers on other ports.

A number of network 'services' have some specific inherent security flaws. Here I describe some of the services. The easiest way to secure a given service is to disable it if it is not needed. Many machines may be running mail, file sharing and even possibly, on Unix systems, domain name services.

The vendor generally considers it better from a user standpoint to supply and enable services that may or may not be needed, than to complicate the installation process and introduce delay; the end user simply wants to get their system up and running as soon as possible, and with the minimum of fuss. Identifying and disabling those services which you don't actually need (and closing the corresponding open ports) will result in a dramatic improvement in your system's security. This is because the rremoval of unnecessary services clearly reduces the number of potential targets available for the potential intruder to attack. This can be done relatively easily as part of the installation process for each computer to be set up, however continued checks are then needed from time to time to ensure that services are not added or re-enabled accidentally during the life of the system.

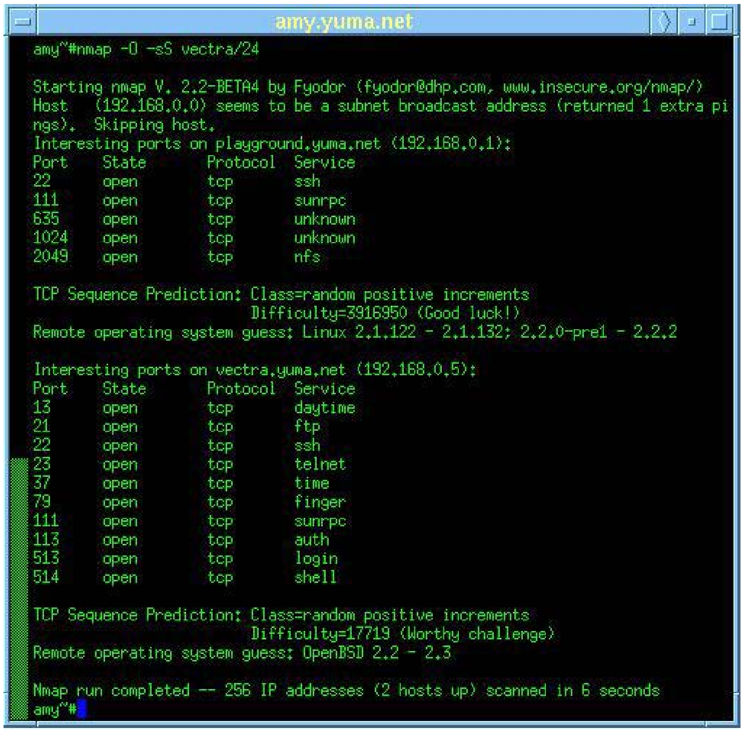
Services that are needed should be kept up to date with security patches. Most vendors now provide mailing lists for notification of fixes and workarounds; advice from these official lists should be acted on promptly.

Those services that *are* needed, and in particular those that accept connections from external and possibly un-trusted systems, must be kept in as secure a state possible. It may be possible to remove some unneeded features following the installation of the operating system; thereafter it is essential to act promptly when security notices are issued by the software vendor and other trustworthy sources. For example, Microsoft's website supplies patches and service packs in response to any vulnerabilities which come to light following the release of a product. The source of such recommendations should always be checked before acting on them, because unfortunately it is not uncommon for malicious advice or programs to be distributed claiming to be security improvements. (See also my advice regarding virus hoaxes).

So now I will explain what a port scan is all about. Any service (and a corresponding open port) accepts connections from other computers). It is a general rule of computer security that the fewer network services you run, then the more secure your system will be. This is because each individual service may possess security flaws as discussed earlier. A port scanner probes one or more ports on once or more remote computers to return a list of open ports, which can potentially be used by a hacker to 'break in'. You may not be aware just how much port scanning goes on throughout the Internet, until you install a firewall and start getting dozens of alerts! I have logged port probes against my own system on a day-to-day basis, originating from computers all over the world. Your firewall logs can be used; as evidence should you wish to make any complaints.

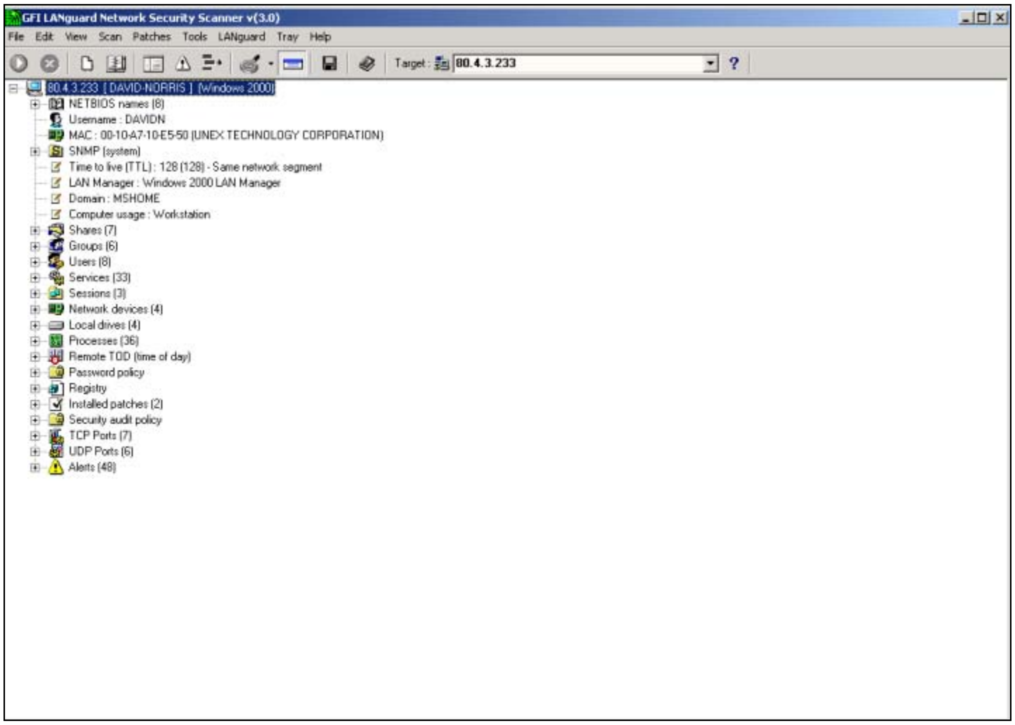
The bad news is that, by default, your computer may well run some services you don't actually need. Software vendors have a difficult problem here; they want the user to 'get up and running' as soon as possible, so from their point of view it is best to install and run services which you don't need than to make life any more complex than need be. So unfortunately the novice user may, when setting up a new system, get a whole lot more that they bargained for. I must admit that on my (test) machine, whether running either Windows or Unix, I deliberately installed all of the default services along with both operating systems, later to find that, unsurprisingly, it 'lit up like a Christmas tree' when port scanned…

Here is a screenshot of Nmap in operation. Nmap is a very comprehensive port scanner which runs on Unix, and is available from www.insecure.org. It can be regarded as either a hacker's tool or a security tool – it is of course true of such tools, may of which are freely available for download – that the same functionality which makes such a tool ideal for one purpose makes it just as ideal for the other, the same is true of packet sniffers, for example!



```
amy^#nmap -O -sS vectra/24

Starting nmap V. 2.2-BETA4 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Host   (192.168.0.0) seems to be a subnet broadcast address (returned 1 extra pi
ngs).  Skipping host.
Interesting ports on playground.yuma.net (192.168.0.1):
Port    State       Protocol  Service
22      open        tcp        ssh
111     open        tcp        sunrpc
635     open        tcp        unknown
1024    open        tcp        unknown
2049    open        tcp        nfs

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=3916950 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.1.132; 2.2.0-pre1 - 2.2.2

Interesting ports on vectra.yuma.net (192.168.0.5):
Port    State       Protocol  Service
13      open        tcp        daytime
21      open        tcp        ftp
22      open        tcp        ssh
23      open        tcp        telnet
37      open        tcp        time
79      open        tcp        finger
111     open        tcp        sunrpc
113     open        tcp        auth
513     open        tcp        login
514     open        tcp        shell

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=17719 (Worthy challenge)
Remote operating system guess: OpenBSD 2.2 - 2.3

Nmap run completed -- 256 IP addresses (2 hosts up) scanned in 6 seconds
amy^#
```

To find out what services are running on your machine, you may like to use a program called ‘Probe Me’; it’s free and available at http://www.ericphelps.com/probeme/index.htm. This is a fast method by which you may learn which services are running on your computer right here and now! For more comprehensive information about your PC’s security, I recommend that you try Languard network scanner. You can download an evaluation copy from www.webattack.com. Please don’t get too curious and be tempted to scan other people’s computers, without their prior permission – it will be detected as an attack against them by their owner’s intrusion detection tools – and you don’t want to be accused of hacking, now do you? Here is a screenshot of this, following a scan of the PC on which I wrote this article:

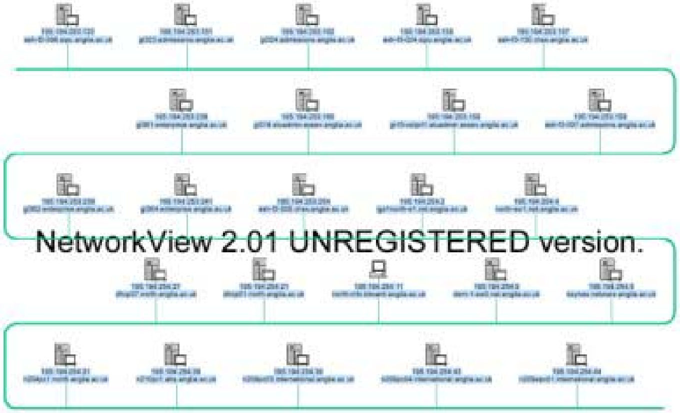


GFI LANguard Network Security Scanner v(3.0)
File Edit View Scan Patches Tools LANguard Tray Help
Target : 80.4.3.233

```
80.4.3.233 [ DAVID-NORRIS ] (Windows 2000)
  NETBIOS names (8)
  Username : DAVIDN
  MAC : 00-10-A7-10-E5-50 (UNEX TECHNOLOGY CORPORATION)
  SNMP (system)
  Time to live (TTL) : 128 (128) - Same network segment
  LAN Manager : Windows 2000 LAN Manager
  Domain : MSHOME
  Computer usage : Workstation
  Shares (7)
  Groups (6)
  Users (8)
  Services (33)
  Sessions (3)
  Network devices (4)
  Local drives (4)
  Processes (36)
  Remote TOD (time of day)
  Password policy
  Registry
  Installed patches (2)
  Security audit policy
  TCP Ports (7)
  UDP Ports (6)
  Alerts (48)
```

I have deliberately hidden a few details (Which I feel would comprise a security risk to myself) from this illustration. Languard is an excellent program, which I feel is certainly worthy of a mention here.

Many security tools can also be used to gain information about which hosts are running at a given time. This is a screenshot from another tool called Network View, which is a network discovery tool. If you are interested, an evaluation version is available from www.networkview.com. It produces a graphical representation of the network topology over a given IP address range. It also logs which services are running on each host. This serves to demonstrate how security tools can double as hacking tools (and visa versa!). This was used to 'discover' my cable modem network segment in order to produce this illustration:



Each node is assigned a different icon, according to the information discovered. Techniques include port scanning, SNMP queries, and DNS lookups. Commonly encountered services are probed for; the list can be edited and labelled. Here is some explanation of some of the more common network services you may find yourself running, without even being aware. Do bear in mind that I'm only listing the commonest ones for a home computer user to be running, and which are perhaps the biggest security risk. Although I researched details of these services for both Windows and Unix machines, note that you need only pay attention to the information regarding the services and operating system you are actually running. I have provided information for both Windows systems, which are the commonest, and Unix/Linux systems, which are likely to be running the most services by default.

The File Transfer Protocol (FTP) service (Port 21)

Anonymous FTP servers can easily be open to misuse:

FTP servers that are open to misuse are a particular worry because hackers find the servers very easily, and leave material (usually pirated copyright material ('warez') or illegal pornography) on the machines, then advertise the site on newsgroups or IRC channels. The only way to be sure whether an FTP server is open to such misuse or not is to try to write (upload) a file to the server and then see if it can be read.

Do you or other users of your system keep world-writable files? You may be running an FTP service without realising it. (See also Netbios). Some FTP services permit "anonymous" access. This means that any user in the world can access certain files! If the anonymous access is set up correctly, only a restricted set of files is accessible anonymously. Some FTP services switch on support for anonymous FTP if the user ftp service is defined on the system. So you may be running anonymous FTP without realising it. The last, very dangerous, but least common, configuration is the "incoming" mode. This lets anonymous users actually place files on your FTP server. While you may have intended it for use by just your colleagues, family, or fellow students at your university, for example, these servers get found by others very easily and are typically exploited by people such as software pirates and pornographers. There are many good reasons for NOT running anonymous uploads in particular:

- They can upload any files they choose, possibly overwriting other files of importance.
- They can use your ftp site as a temporary holding place for distribution of large and/or illegal material.
- They can use up your disk space and waste your bandwidth - and possibly run up a large bill you are responsible for, depending on how you access the Internet.
- Hackers are constantly looking for ways to penetrate FTP systems - they have programs that scan for such weaknesses and exploit them.

💣

Warning: Under UK law, and maybe those of other countries, if you are found with certain types of pornography on your system you are guilty of a serious crime. *Under the British legal system, the prosecution need prove no intent on your part. Do not allow anonymous uploads. Where uploads from remote users are really necessary, be sure to make users log-in by supplying a password. It is also a good idea to ensure* *that, where uploads are genuinely required at all, to ensure that read access to the upload area itself is blocked. This will help to deter misuse of the server. Inspect the uploaded material in order to ensure it is safe before moving it to a download directory later.*

The service is not needed just to run the FTP client on a system, i.e. if you just want to be able to get files from elsewhere via FTP, to download onto your own computer. If you allow remote users access to files through Unix or Windows clients like ftp or Macintosh clients like fetch, or if you allow anonymous FTP then you need this service running. Otherwise, you do not.

To remove this open port:

To turn off FTP services altogether on a Unix system, comment out or remove the ftp line in the file /etc/inetd.conf. After editing the /etc/inetd.conf file the inetd service it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.

On a system with a System V style ps:

```
# ps e | grep inetd
133 ? 0:03 inetd
1513 pts/5 0:00 grep inetd
# kill HUP 133
```

On a system with a BSD style ps:

```
# ps ax | grep inetd
212 ? S 0:00 inetd
1549 p2 S 0:00 grep inetd
# kill HUP 212
```

On a Windows system using Microsoft Internet Information Server (IIS), FTP can be disabled by stopping the service from the IIS Console File menu, and then going into the Services Control Panel and disabling it there as well. If you need FTP, but not anonymous FTP, the latter can be disabled by double-clicking on the relevant service line (ftp here) in the IIS Console and un-ticking the Anonymous system. If you need access via ftp you are best to limit it to named machines (by IP number) and low-level (User or Domain User) accounts.

For Windows NT 4.0 go to Control-Panel > Services. Find FTP service, Highlight FTP service and click STOP. Click on the Start-up Button and make sure the service is selected as being disabled.

For Windows 2000, go to Control Panel Administrative tools Services. Find and open the FTP service, Stop the service (if running), go to the Start-up type pull down menu and select disabled. If you are running IIS and do not need FTP services, uninstall them as well.

To disable FTP access to a Hewlett-Packard Jet Direct network printer, connect to the printer by telnet (which should have a password set), and type ftpconfig: 0 then quit. See this document on HP's support Web site for more details.

The Hypertext Transfer Protocol (HTTP, Port 80)

The Hypertext Transfer Protocol (HTTP, Port 80) is the web server protocol. Any system running a web server must be running some program to provide that service.

The default port for a web server is port 80, but other port numbers may be used as well. Here is a list:
Port 98 is used by linuxconf's network interface
Port 311 is used by AppleShare IP ;
Port 591 is used by FileMaker Pro;
Port 801 is used by StarOffice;
Port 2077 is used by SGI's web admin facility;
Port 2301 is used by OSF/1's insightd;
Port 3128 is used by squid;
Port 8888 is used by dynaweb.

By far the most common web server on Unix platforms is the Apache web server. Web servers can run programs for users via Common Gateway Interface (CGI) programs, Active Server Pages (ASPs) or Server Side Includes (SSIs). Intrusions via web servers typically enter via these routes rather directly through the static web page service. If you are intentionally running a web server, then you need to be running this service. You do not need to be running it to browse the web!

To remove this open port:

The web server is a service that runs continually. There will be a start-up script that launches it at boot time. You can either remove this start-up script or read it to see if it checks for the presence of a configuration file to decide whether to launch the service. Removing or renaming the configuration file would then also stop the service being launched. If you want to run the web server but not the program running components (CGI, ASP, SSI) you will need to consult the documentation for the particular server you run.
On Windows NT systems, you need to uninstall Internet Information server. To do so, open control panel, choose the ‘add/remove programs’ menu, followed by the ‘add/remove Windows components’ menu. If ‘Internet Information Services’ components are present, feel free to remove them unless you use them. Note that some versions of Windows install these components at installation, whereas others do not.

Internet Message Access Protocol: Ports 143/220

The Internet Message Access Protocol (IMAP) is a mechanism for reading and manipulating mail on a remote server. It comes in two versions, IMAP 2 and IMAP 4. There was an experimental protocol called IMAP 3, but IMAP 4 superseded it before implementation. You typically don’t need to be running this service. Only systems that store mail for it to be read by a third party need run this service. It is very rarely indeed used by a home user. It is installed by default on many Unix variants. I do not know of any Windows or Macintosh versions which do so.

To remove this open port:

IMAP is started under Linux from the inetd. Edit the /etc/inetd.conf file and comment out or delete the imap entry:

```
# Imap stream tcp nowait root /usr/sbin/tcpd in.imapd
```

After editing the /etc/inetd.conf file the inetd service it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.
On a system with a System V style ps:

```
# ps e | grep inetd
133 ? 0:03 inetd
1513 pts/5 0:00 grep inetd
# kill HUP 133
```

On a system with a BSD style ps:

```
# ps ax | grep inetd
212 ? S 0:00 inetd
1549 p2 S 0:00 grep inetd
# kill HUP 212
```

Simple Mail Transfer Protocol: Port 25

The Simple Mail Transfer Protocol (SMTP) is the protocol by which email messages are sent from machine to machine. This does not include the reading of mail by the POP or IMAP protocols.
The most common Unix mail service is Sendmail which is a truly ancient piece of software dating back to near the dawn of the Internet. More recently smail, qmail and Exim have risen to replace it. You need to be running an SMTP listener only if your system is using a mail hub – not usual for a home user! Windows does not come with an smtp listener enabled.

To remove this open port:

As described above, you may not want to disable the service, but only its listening habits. The most common Unix mail service is sendmail and the other services based on sendmail. It is started in an initialisation script run at start-up. If it is started with the 'bd' option it will run as a listener. You need to remove this option from the start-up script to stop sendmail from listening after the next reboot. Then kill and restart the sendmail service without the option to deal with the current instance.
For Windows NT systems, see the documentation provided with any Windows NT add-on mail programs.

Simple Network Management Protocol: Port 161

The Simple Network Management Protocol (SNMP) is a protocol for the remote management of networked devices. It's typically used by such things as network hubs and print servers, but there are also implementations for most full-blown operating systems. SNMP agents (as its servers are usually known) typically allow one to gather various information about the network stack of a device, and often of many of its other aspects. Most implementations also allow at least some parameters to be changed remotely. Access to SNMP agents (at least in simple implementations) is controlled by "community strings", which are effectively passwords. Most implementations use "public" as a standard community string for read-only access.

The default community string for read write access varies between vendors, and anyway it's a good idea to change it.
You need to be running an SNMP agent only if you want to be able to manage your system remotely using SNMP. SNMP is not often of much use for most home users. Some systems may run SNMP without it being obvious. Hewlett-Packard's JetAdmin and 3Com's Quick Config Manager are examples.
To remove this open port:

Since so many types of device run SNMP agents, it's very difficult indeed to provide comprehensive instructions for either disabling SNMP or changing community strings. Here, I can provide some instructions for some systems I've used in the past.

For Windows:

Here, you need to go into the control panel (under settings on the start menu) and select the 'add/remove programs' menu, then 'add/remove Windows Components'. Once there, select 'Internet Information Services' and click the 'details' tab. If the SNMP agent is installed, de-select it's tab and click OK. This installs the SNMP agent. This is installed by default in Windows NT/2000 server, but not NT workstation or Windows 2000 professional. I am not certain as to what the state of play with Windows XP is regarding snmp.

Unix/Linux systems

SNMP services are usually provided by a process called snmpd, which runs continuously. You should be able to modify your system start-up scripts to disable it.
Solaris (version 2.6/7)
In Solaris, the SNMP agent is in the "SUNWsasnm" package, and can be disabled by removing this package.
In Solaris 2.6, the agent defaults to allowing read write access with the community string "private". The read/write community string can be changed by editing /etc/snmp/conf/snmpd.conf. If you only need read access, you should edit /etc/snmp/conf/mibiisa.rsrc so that the command line reads:
Command = "/usr/lib/snmp/mibiisa r p $PORT"
Solaris 2.7 is configured like this by default.

3Com network hubs and switches: In general, the easiest way to change the community strings on 3Com hardware is using the terminal interface. This can be accessed either by telnet over the local network, or by plugging a serial console into the back of the unit. While many recent hubs have pretty Web interfaces as well, it tends not to be possible to set SNMP community strings using them.
Most 3Com hardware has three levels of user, "monitor", "manager" and "security". There are usually three users configured into the system by default, with the same names as their levels. More recent devices add an extra "security" level user called "admin". The default community strings for these users are (respectively) "public", "manager", "security" and "private".
It's usually possible to modify which users of a device are allowed to access it by which route (serial, telnet, SNMP, web), so if you don't need read and write access by SNMP, it's probably a good idea to disable SNMP access for all users except "monitor".

3Com Super Stack II PS Hub 40/50 (version 1.xx):

As far as I know, the command line interface to these hubs doesn't permit the changing of community strings. Instead, you should use the Quick Config Manager (documented in the manual that came with the hub) to change each community string in turn. The relevant dialogue system is "Edit Access Levels", available from the "Access Conf" pane of the "General Info" system.

3Com SuperStack II PS Hub 40/50 (version 2.10)

The community string for "manager" and "security" level users can be changed through the device's command line. Connect to it by telnet or through the serial port, log in as a user at the appropriate level, and type ‘snmp community’. You will be prompted for a new community string for that user, which you should provide. You can then log out of the device by typing logout, and repeat the process with the other user names. SNMP access for individual user levels can be disabled using the Quick Config Manager (Configure > General Info > Access Conf).
To disable all remote access to the hub (telnet, web and SNMP), connect by telnet or through the serial port, log in as a "security" level user and type ‘system access disable’, then log out. You will now only be able to log in over the serial line.

The TELNET protocol: Port 23

TELNET is the original remote login protocol. You need to be providing TELNET services only if you want people to be able to log in to your system over the Internet. Many embedded systems in printers and other hardware devices use TELNET for configuration purposes.

To remove this open port:

On Unix systems, the TELNET service is provided by a program called telnetd or in.telnetd. This is usually spawned from inetd, so to disable it you need to remove or comment out the telnet line from /etc/inetd.conf. After editing the /etc/inetd.conf file the inetd service it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.
On Windows systems, it is to be found as a sub-component under Internet Information Services. This component can be un-installed in the same way as the SNMP agent. Remove the entire Internet information services group if you don’t run any servers at all (if you’re using dial-up access to the Internet, you probably won’t be anyway).

Trivial File Transfer Protocol: Port 69

The Trivial File Transfer Protocol (TFTP) is a simple UDP based protocol for transferring files. Its two major uses are for bootstrapping diskless machines (or machines which are being installed over the network) and for installing new firmware images in networked devices such as printers and hubs. A typical home user does not need it! Any computer generally only needs to run the TFTP server if it's acting as a boot server for other systems in some way, either for diskless clients, or for remote installations. I have come across some unnecessary TFTP servers before, running on

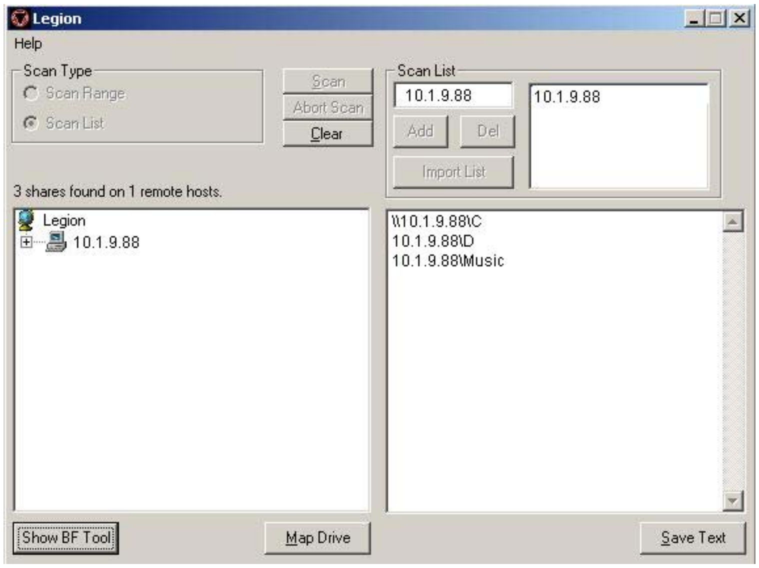
Linux/Unix systems. I haven't come across this service as yet running on a Windows system.

To remove this open port:

On Unix systems, the TFTP service is provided by tftpd or in.tftpd. This is usually spawned from inetd, so to disable it, comment out (with a # at the start of the line) the line in /etc/inetd.conf which begins tftp. After editing the /etc/inetd.conf file the inetd service it configures must be instructed to reread its configuration file. To do this it needs to be sent the HUP signal.

Netbios: Network Basic Input/Output System (Windows Only: Port 139/445)

This is seen on a Windows system under 'File & Printer Sharing' in control panel. This service is not as benign as the term 'file & printer sharing' would suggest. If you thought that it was entirely about sharing files and printing on your home network alone; you're wrong. The trouble is that, in development, it was intended for liberal usage in the trusted confines of your home or office, where all users of the LAN are known. However, when running on a home computer, without a firewall in place, it will share any files or directories which you select for sharing (or even your entire hard disk!) to the whole of the World Wide Web, without you even being aware. So don't use any computer which is directly connected to your modem, or cable modem, as a fileserver, particularly unless you run a firewall! NETBIOS represents one of the most serious security vulnerabilities on a Windows system. If you don't believe me, here comes the supporting evidence;
There are port scanners which only scan for unprotected Windows' file shares. Here is one in use:



Scan List: 10.1.9.88

10.1.9.88

3 shares found on 1 remote hosts.

Legion
10.1.9.88

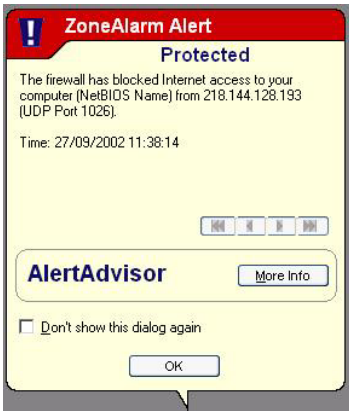
```
\\10.1.9.88\C
10.1.9.88\D
10.1.9.88\Music
```

It's well written, comes complete with a brute force tool to crack password protection on the file shares, you can map a network drive, can scan 64 subnets at once, and it's free. Now, I am not trying to promote Netbios scanning, rather to make people aware of the problem of unprotected network shares. Netbios doesn't really care less whether it's operating on a private network or the global Internet. I have used it on a

private LAN and (although I changed the IP address and some other detail) – and it will allow anyone to find any unprotected Windows shares on your PC. In this example, this is what the hacker sees, if your drive C: drive D: (both from the root directory!) and a directory called 'Music', are shared. On Windows 9.X, the access may be read-only or full depending on how you set up sharing; on Windows NT then access may be further restricted according to NTFS file access permissions. Later, I shall explain all. You can use a tool like this to scan your own computer(s), to find out for certain what you may be sharing to the outside world. Take my word for it, I ran a scan on an IP address range known to be populated by cable modem home users – and to my sheer amazement, about 20% of the Windows machines running had port 139 open, and a minority of these had their whole hard disk shared to the Internet!!!
To remove this open port:

As a home user, you probably don't need file and printer sharing running anyhow. If not, then go into control panel and disable it. If you really do need it, then be sure to share only those files and/or directories you need to within your home network, and use a firewall on machines connected directly to the outside Internet. For more information on firewalls, see my firewall section later. Also, see my remarks about Windows NT and the NTFS file system which allows permissions to be allocated to individual files or directories, as opposed to FAT, which is entirely defenceless. Obviously, if you really want to share any files to the entire web, make sure it is a conscious decision.
If you really must share files (for example, if you need to access files on your home PC from work) then here is some advising on how to (best) keep your network shares secure.

Please note that *anyone on the Internet* can gain access to your computer over the Internet if they know your IP address (a Netbios scanner such as the Legion scanner discussed above can soon find it), and the user name and password of a user – particularly the administrator. Anyone who gains access to your computer via the Internet can view all shared directories and files, even those that are protected using NTFS file permissions, provided they know your administrator password! Remember that many free programs such as Legion have a 'brute force' password-cracking tool included. Therefore, create a difficult password for the Administrator account, and for heavens sake do not be lazy and leave this password blank – this allows anyone to log in as an administrator without a password!!!
You can stop sharing files temporarily using Windows Explorer by right clicking on it, selecting sharing, and then selecting 'Do not share this folder'. This will temporarily disable the shared attribute of the directory, but remember that if you do so, then re-starting the computer will re-enable sharing. And for heavens sake don not share the entire hard drive from the root directory!!!
The best advice if you *do not really need to share files or directories* is simply to disable the service – in fact uninstall the 'file and printer sharing' service in the Windows' control panel. Right now. This is an alert by Zone alarm, caused by a Netbios scan from a remote machine:



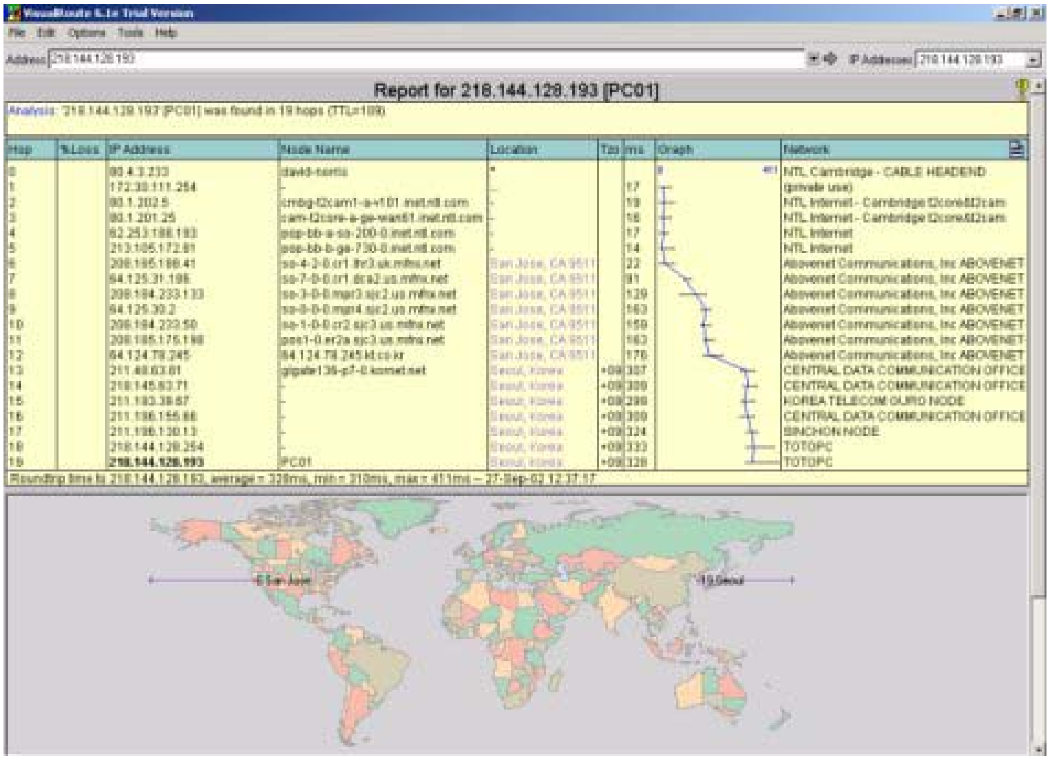
Protected

The firewall has blocked Internet access to your computer (NetBIOS Name) from 218.144.128.193 (UDP Port 1026).

Time: 27/09/2002 11:38:14

□ Don't show this dialog again

This alert is probably the result of a probe for port 137. Tracing the owner of the IP address reveals the service provider as Korea Telecom in the Far East. Although it is not worth too much worry as a one-off event, a large number of alerts coming from a single IP address (or a particular address range, remembering that most home users are accessing the Internet using dynamic addressing) would be well worth investigation. VisualRoute by Visualware, can be obtained as a 14-day trial version. It essentially performs the same task as the 'tracert' (traceroot) command in Windows NT/2000 only it graphically displays the route that the hacker's data packets took to reach your computer. Here I used it to trace the remote computer in Korea which set off the alert shown above:



Address: 218.144.128.193 IP Addresses: 218.144.128.193

Report for 218.144.128.193 [PC01]

Analysis: '218.144.128.193 [PC01]' was found in 19 hops (TTL=109)

Hop	%Loss	IP Address	Node Name	Location	Tzo	ms	Graph	Network
0		80.4.3.233	david-norris	*			0 411	NTL Cambridge - CABLE HEADEND
1		172.30.111.254	-	-		17		(private use)
2		80.1.202.5	cmbg-t2cam1-a-v101.inet.ntl.com	-		19		NTL Internet - Cambridge t2core&t2cam
3		80.1.201.25	cam-t2core-a-ge-wan61.inet.ntl.com	-		16		NTL Internet - Cambridge t2core&t2cam
4		62.253.188.183	pop-bb-a-so-200-0.inet.ntl.com	-		17		NTL Internet
5		213.105.172.81	pop-bb-b-ge-730-0.inet.ntl.com	-		14		NTL Internet
6		208.185.188.41	so-4-2-0.cr1.lhr3.uk.mfnx.net	San Jose, CA 9511		22		Abovenet Communications, Inc ABOVENET
7		64.125.31.198	so-7-0-0.cr1.dca2.us.mfnx.net	San Jose, CA 9511		91		Abovenet Communications, Inc ABOVENET
8		208.184.233.133	so-3-0-0.mpr3.sjc2.us.mfnx.net	San Jose, CA 9511		129		Abovenet Communications, Inc ABOVENET
9		64.125.30.2	so-0-0-0.mpr4.sjc2.us.mfnx.net	San Jose, CA 9511		163		Abovenet Communications, Inc ABOVENET
10		208.184.233.50	so-1-0-0.cr2.sjc3.us.mfnx.net	San Jose, CA 9511		159		Abovenet Communications, Inc ABOVENET
11		208.185.175.198	pos1-0.er2a.sjc3.us.mfnx.net	San Jose, CA 9511		163		Abovenet Communications, Inc ABOVENET
12		64.124.78.245	64.124.78.245.kt.co.kr	San Jose, CA 9511		176		Abovenet Communications, Inc ABOVENET
13		211.48.63.81	gigabit36-p7-0.kornet.net	Seoul, Korea	+09	307		CENTRAL DATA COMMUNICATION OFFICE
14		218.145.63.71	-	Seoul, Korea	+09	309		CENTRAL DATA COMMUNICATION OFFICE
15		211.183.38.67	-	Seoul, Korea	+09	299		KOREA TELECOM GURO NODE
16		211.196.155.66	-	Seoul, Korea	+09	300		CENTRAL DATA COMMUNICATION OFFICE
17		211.196.130.13	-	Seoul, Korea	+09	324		SINCHON NODE
18		218.144.128.254	-	Seoul, Korea	+09	333		TOTOPC
19		**218.144.128.193**	PC01	Seoul, Korea	+09	328		TOTOPC

Roundtrip time to 218.144.128.193, average = 328ms, min = 310ms, max = 411ms – 27-Sep-02 12:37:17

You can see that the route taken by the traceroot (once it had left my local network – the Cambridge NTL Cable Headend) is shown on the map. You can also view the list of intermediate computers which relayed the packets. Visualroute also looks up the details of each computer in the list from a central database. You can see that my IP address is 80.4.3.233, and that the first 5 routers are part of the NTL wide area cable network. On leaving the NTL network, the packets are transferred through seven further routers in San Jose California (which belong to AboveNet Communications) before being forwarded to Korea Telecom. The hacker's computer (IP address 218.144.128.193) is 19 hops away. It must be stressed that there is more than one potential route for the packets to take, of course – but the originating computer has been traced.

Another source of the offender's IP address or service provider, in instances where you may receive 'Spam' or namely unwanted email messages, is from the message header. To view this, you generally select a 'tools' option under a 'view' menu (This is true for Microsoft Outlook; other software will clearly differ in this respect). You can also save the message in 'message format' (.MSG), and view the header by opening the .MSG file in a plain text editor, such as notepad. This file can also be sent as an attachment to the abuse section of their service provider as supporting evidence. A helpful program here is 'IPLookup' which can retrieve the relevant details, as mentioned later. The program is free to download at this address: http://www.softnik.com/products/iplookup/index.htm.

Note that Windows file and printer sharing should not be confused with third-party software for peer-to-peer file sharing, such as Gnutella. These programs have to be downloaded and installed by the user specifically for the purpose of intentional file sharing. These programs generally use higher port numbers above 1024, for example Gnutella uses port 6346. Please note that the crucial difference is that the user must install the server to share any files; this is not the same situation as is the case with Windows sharing, where people are often unaware that they are sharing files.

Where you use sharing programs, such as Gnutella or the popular Bearshare, do ensure that you only share files and directories that you wish to share (Some inexperienced users have been known to share their whole hard drive).

Do note that a large number of probes for port 6346 are most likely to be the result of other Gnutella clients attempting to establish contact with those running on other computers elsewhere; this is how the Gnutella clients work. It is not due to a port scan!

If however you *do* receive an unwelcome intrusion from a machine via the Internet, you should an e-mail to the abuse section of the internet service provider concerned as soon as you notice the intrusion, and include in this the following information:

- The IP address number of your machine;
- The IP address number of the attacker's machine;
- The port probed for (please ensure that this is a genuine security threat and not simply normal Internet traffic such as ident (port 113) or gnutella responses, port 6346);
- The extract from your firewall logs in a plain text format (note that the ISP may not be able to read proprietary log formats);
- The time zone of your logs (either Greenwich Mean Time or British Summer Time if you are located in the UK);
- An indication of whether your logs are time synchronised and if not, how far off true time your machine is.

Remember that a one-off alert may not necessarily be due to a port probe; it may have other causes such as someone mistyping an IP address, for example. Where you get a large number of probes on multiple ports, then this is more likely to be suspicious.

Remember: removing or patching services can only protect those systems on which the services are known to be running. To protect other systems where services should not be needed but may be run by accident, it is necessary to use a firewall to restrict the network traffic that can reach them from the Internet. For example, unless you are intentionally running an FTP server on a machine, there is no need for potentially hostile FTP requests to reach that machine. Since it is often much easier to list the services that *should* be present, the best way to configure a hardware router or firewall is to permit only incoming traffic for those services to pass, and deny all others. This also gives the best chance of protection against unknown future threats. Remember that removing unnecessary services, patching any necessary ones, and installing a router or firewall cannot entirely remove the risk that computers will be compromised, but they will very substantially reduce this risk. The vast majority (say 90% or more) of system compromises whether in a domestic, or working environment, could have been prevented had these measures been taken in good time. If you would like to get some immediate information regarding what your PC is offering to the Internet right now, why not try visiting Steve Gibson's excellent site at https://grc.com/x/ne.dll?bh0bkyd2? For a more general overview regarding current hacking trends, try visiting www.cert.org - Cert is an abbreviation for Computer Emergency Response Team.

💣

A Word of caution is needed here. Many sites which provide free, online vulnerability tests, such as the excellent Gibson Research Corporation (http://grc.com), have overlooked one or two potential causes of misleading results:

- Where your computer is located behind a gateway or router, as in my own case, or as you almost certainly are at work, your computer will not be reachable from the outside Internet (your own access to the Internet is via the gateway which uses something known as 'network address translation', (NAT). This applies also to a gateway or router device which you have used to share Internet access for your home network, if you have enabled NAT. This means that your computer will have one of those IP addresses which fall within the 'private' ranges, namely those IP address ranges which are reserved for private network usage and are *not* visible to the public Internet. When you access the Internet, data packets sent by your computer are received by the gateway via it's 'private' IP address visible only within the private network. At the gateway, the packets have their 'sender' address changed to that of the gateway's 'public' address; which is namely the gateways own Internet address. Data from the Internet, which is received by your computer, is send to the gateway's public IP address, and the gateway then changes the 'sender' address to that of it's private network address, and it's recipient address to that of your computer. The private address ranges have two main objectives; Firstly, to save 'public' address space available on the Internet, as only the gateway itself needs a public address, and secondly, the computers within the private network are secure from hacking as no data packets send directly from the Internet can reach any machines within the private network. For example, port scanning the gateway will reveal only which ports are open in the ‘public’ side of the gateway. (Servers run on a computer on a private network, in order to be accessible to the outside world, must be relayed through the gateway to appear as a public service on a ‘virtual port’, visible on the outside of the gateway. Many servers can be run in this way, so long as none of them require the use of the same port externally. Note: should you run an external security check such as that from grc.com, the results will be correct for the gateway, not your individual computer! However, you are safe from external attack anyhow. In this case, your IP address will be in one of the following ranges:

10 . 0 .0.0 – 10 .255.255.255

169.254.0.0 – 169.254.255.255

172. 16 .0.0 – 172. 31 .255.255

192.168.0.0 – 192.168.255.255

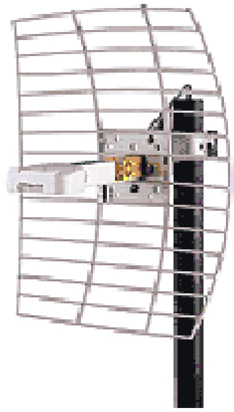
- Note, however, that if you are on a network which is part of the outside Internet, but where there is an intermediate device which blocks certain services, such as Netbios (Windows file sharing), then a test run from outside that network may report that you are not vulnerable to a particular danger, when in fact you are. For example, if you are on a cable modem network, and your service provider blocks Netbios, the test will report that port 139 on your system is unreachable, but other people within the cable network can still access your unprotected file shares!

---

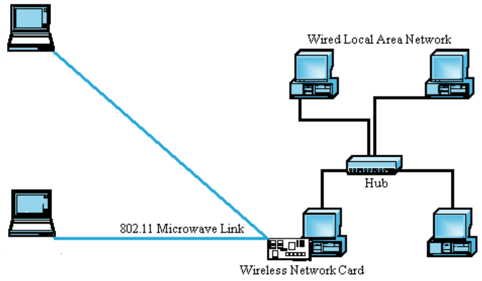
12) Wireless Network Vulnerability

Wireless networks do away with the need to run cables all over the home or office. They also allow portable computers, such as laptops, to remain connected to the network whilst they are moved around the coverage area of the Wireless LAN. These networks use a microwave radio link operating at 2.4GHz (about the same frequency as a domestic microwave oven, or in some cases 5GHz, but only at very low power levels) to carry the data. Although quoted ranges are around 100 metres, which is more than adequate for the average home or small office, they actually do radiate a great distance further. This is a typical wireless access point:

The range quoted applies to the inefficient aerials which are built into the wireless network cards. However it is possible to detect these signals at much greater distances using a higher gain aerial (several kilometres under ideal, line of sight conditions). These can be ordered for under £100, or even constructed using metal cans of the correct physical dimensions! Over a line of sight path, a high gain aerial can detect the wireless network access point's signal several hundred metres away! I have seen a parabolic dish antenna advertised offering a gain of 24db! Also, at microwave frequencies, signals are highly reflective, so objects such as buildings can reflect and scatter the signal over quite some distance. Here is an example of a parabolic dish aerial:



With wireless networks becoming ever cheaper (less than £100 for access points, and around £60 for Wireless network cards), there has been an explosion in their usage, both in the workplace, and in the home. However, few people really appreciate the security implications of a wireless LAN. This is a typical topology for a partially wireless network, which perhaps started out as a wired LAN and has had a wireless access point added:



If your wireless network access point's signal extends well outside of your property, it is easily possible for a complete stranger to access it using a portable computer. Worse still, there are people who may be prepared to go out of their way to find wireless networks in operation, and access them, either to steal confidential information, or simply to access the Internet for free!

As a rule, the lower the signal strength, the less bandwidth a wireless connection will provide. Most manufacturers quote expected performance over a given distance, assuming that the supplied aerials are in use. At the limit of the range, the bandwidth may reduce to about 1 megabit per second, which is slower than wired local area networks operating at 10 or 100 Mbps; however this still compares quite favourably with domestic broadband connections which generally operate at 128 or 512 kbps, or 1 Mbps! Certainly this far exceeds the performance of a standard dial-up modem operating at a maximum of 56kbps. It therefore stands to reason that some people may want to hack into other peoples wireless LAN's simply to gain some free bandwidth. So anyone parked outside using a laptop may be worthy of suspicion!
Remember that when a wireless LAN card detects an access point's signal, it will contact that access point. If access is granted, then that computer will be allocated an IP address on the network, given that the network is using dynamic IP addressing.

A wireless access point behind a hardware firewall, or behind a PC running a software firewall, potentially represents a totally uncontrolled back door to a malicious individual. In the case of fixed-line connections, your home or office network will have a single, or at the very most a few, points of entry which are the Internet connections to your service provider.
However, in the case of a wireless network, any point at which your signal can be received, within the three dimensional radiation pattern, be it next door, or in the street, is a potential point of access to your network! And it may additionally be difficult, in the event of such an intrusion, to determine the location of the intruder. Wireless networks do offer some built-in protection. The 802.11 network protocol includes an encryption scheme called WEP (Wired Equivalent Privacy). Some wireless network cards offer 40 bit encryption, others 128 bit encryption. Although it is possible to crack the encryption scheme, it will deter all but the most persistent and dedicated hacker, as there are easier pickings elsewhere. But it is essential to remember that, given sufficient time and incentive, someone can still break in.

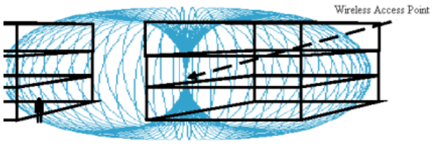
To secure your wireless network:

Enable WEP, unless you intentionally want others to be able to access your network using their own laptops or other devices, for example a Pocket PC. Remember that privacy aside, if you allow unknown individuals access to your network, then they may well cause damage to your own equipment, or use your Internet connection for illegal activities which they would not carry out using their own account, leaving you liable. Although WEP is not foolproof, it will deter all but the most determined intruders.

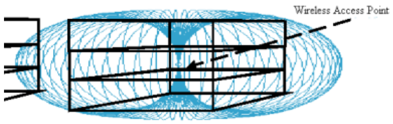
Change the default password supplied with your access point. Remember that the default password settings for various wireless components are made available by the manufacturers should you loose or forget them. Avoid passwords which are easily guessed or cracked. See my earlier suggestions for password choice.

You may want to disable DHCP, and use static addressing on your home network. Note that this tip is for users who are reasonably fluent with set-up and maintenance of a network. This will require some planning, particularly where you have more than two or three computers comprising your network.

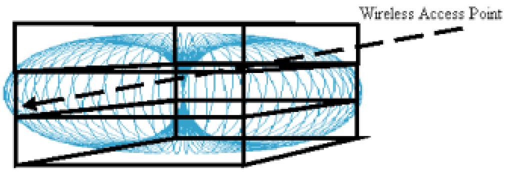
Be sensible about the location of your access point. Remember that placing it geographically in the centre of your property will reduce the coverage of your access point. This is because walls and floors will attenuate the signal leaving your property. Windows, on the other hand, are virtually transparent to microwave energy. If the access points are located near a window, a stronger signal will be radiated outside into the street making it more likely to be detected. This is the typical effect on the access point's coverage pattern:



In the first example, the access point is placed near an external wall or (worse still) a window. The signal easily extends across the street into other buildings opposite, particularly where the access point is near a window. It may also be visible from outside, and saving intruders the need to locate it! Below, the access point is located in the centre of the house.

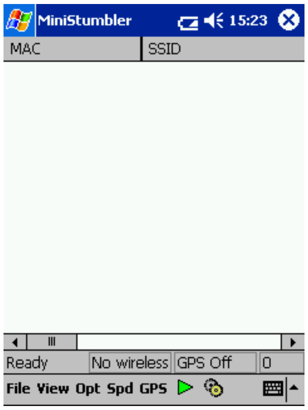


Also, many access points and wireless LAN cards allow the power output to be adjusted. By default, they are normally supplied with the power set to maximum, in order to reduce the number of people experiencing coverage difficulties. Most homes are not large enough to require the full power output to provide adequate coverage. This will reduce the coverage area of the devices, and the area in which a hacker can gain access:



Remember, this diagram is simplified. In practice, microwave signals will be reflected by some objects, and blocked by others, so the actual coverage pattern will be more complex than shown.

You can discover the extent of your wireless local area network using a pocket PC or laptop. Here is a program which is used to test wireless network access; it runs on the pocket PC and is available for free, in versions which run on the MIPS, SH3 and ARM processors, used in various versions of the pocket PC. A desktop/Laptop version is also available, of course. To date, I haven't a WLAN card for my pocket PC, so I can't show you the program in action.



Try to gain access to your LAN from your garden, your car parked outside, or a neighbours house, for example. You may even find that you can gain access several streets away under the right signal propagation conditions, and much further away across open fields in a rural location! This experimentation will give some idea of where a hacker could potentially hide. You may possibly even stumble across someone else's wireless network signal!

Remember that in addition to the security risks inherent in any wireless network, most base stations are supplied in an insecure configuration. This is to make setup easy. It is your responsibility to increase the security level following installation. See the vendor's documentation for instructions here.

Firstly, many wireless base stations come configured allowing any computer to connect to a base station with or without the appropriate SSID. You will need to change this setting.

Most wireless base stations have the identification name/number set to a default factory setting, in order to assist with user support and to provide a method of resetting the unit in the event of a user forgetting the access password, for example. These are well known, and often available from the vendor's website! Therefore, you must change the SSID to something less easily guessable.

Most wireless base stations come with encryption disabled. You should enable WEP and set this to the highest possible value (128 bits if supported; failing this, then use the highest supported value). Remember that for 'every extra 10 bits' in the encryption key, there are 1024 (2 raised to the power of 10) more possible key values.

Most wireless base stations come configured with well-known default SNMP community strings. If not changed, this allows anyone to change the settings on the wireless base station via the Internet. SNMP (Simple Network Management Protocol) allows remote management of network components; although useful in a corporate environment, for example, it is not generally needed by the home user. If you need remote access, then at least change the community string (which is the SNMP equivalent of a password). Where remote access is not required, disable remote management, or if preferred, make it configurable only from known IP addresses (such as your employer's gateway).

Disable broadcasting of the SSID (Base station identity) if possible. Although difficult to crack if WEP is used, and only rarely broadcast, there is some danger that it could be accomplished where someone is sufficiently determined.

Also, disable unneeded services on computers making up the wireless network.

Above all else, ensure that you enable the Firewall option built into the access point; this uses network address translation to protect your network from scans mounted from the outside Internet. If you wish to run servers from behind the firewall, open up only the 'virtual ports' needed. Avoid using the DMZ (demilitarised zone) unless there is no alternative. (Some games and other applications may have problems if run from behind a network address translation firewall or gateway). Use a software firewall on any machines in the DMZ.

13) Some 'General Security Tips' for Each Operating System

Here I provide some general security tips for typical home computer users, which I have listed per operating system. Remember, although the advice may seem rather excessive for the average home user, you may change your mind after the event, when something drastic has already happened! It is *up to you* to decide what level of security is appropriate, or right for, you. Remember that security and convenience are always at odds with each other! All I can do is provide advice on the possible means by which your system *can* be made more secure. Remember, none of the operating systems are particularly secure when first installed. Also, remember that although I am attempting to provide adequate advice for versions of each operating system to date, future versions may require different precautions. As an example, Windows 2000, which is version 5 of NT, has subtle variations on NT4, and Windows XP, which is also based on NT, has further variations.

A further point is also valid here. Many home users of Linux do dual boot their Linux system with one version of Windows or another, for example, in an attempt to obtain the 'best of both worlds'. Although this is not in itself a security risk, it should certainly be noted that personal computers which are configured with multi-boot capability are, of course, only as secure as the least secure operating system which can be booted. Considerable expertise is needed to configure a computer system sensibly, whatever the operating system. Further to this, one cannot, in general, expect the average home computer user to be sufficiently expert in a particular operating system to know of every possible security flaw.

Important: Windows Product Lifecycle Information:

This page provides current information regarding the lifecycles of Microsoft Windows products for technical support purposes.
It is important to keep in mind that Windows' versions do go out of date. If you are running a version which has, or is shortly about to enter it's unsupported phase, you are very strongly recommended to upgrade given that your hardware is up to running the newer version of Windows. This is because, once a particular Windows' Version has actually reached the end of it's supported life, no further technical support is available; and eventually new software releases will stop supporting it also. Bear in mind however, that although one or two hardware components should generally prove easy enough to upgrade, if your system is generally underpowered, you are generally better advised to replace it rather than to upgrade multiple components.

Windows 9.x Series Versions (These actually include Stand-alone DOS, Windows 3.x and ME);

- Currently all Microsoft operating systems in this series, up to and including Windows **95** are in their non-supported phase. This means there are no more patches, service packs, updates, security releases, or technical support in general.
- Windows **98 SE** has entered its extended phase of life (June 30th 2002 -June 30th 2003).
- Windows **ME** is in its mainstream support phase until 31st December 2003.

However, as none of the above versions offer any system or file security, and in future all Windows' versions will be based on NT, it is generally recommended that you replace your existing Windows 9.X version with Windows 2000 or XP where possible.

Windows NT Versions (NT 3.5x,4,2000,XP);

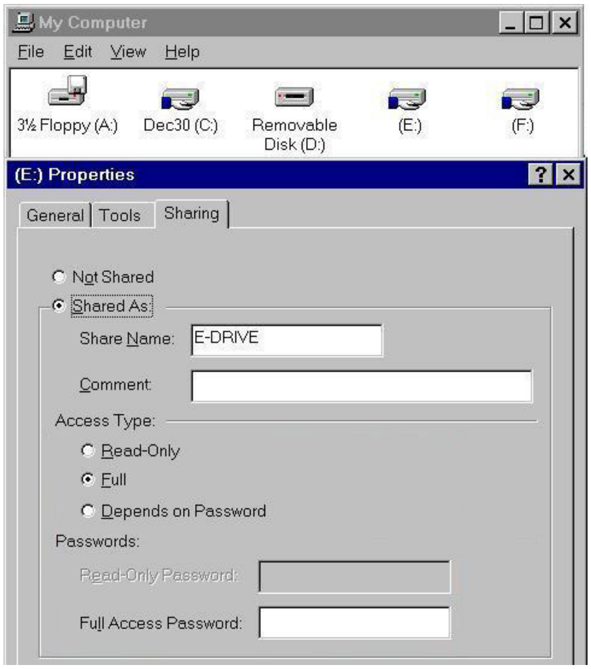
- Windows NT 3.5x entered its end of life phase in December 2001.
- Windows NT 4.0 entered its extended life phase on June 30th 2002. Windows NT 4.0 Server patches are available at no charge until 31st December 2003.
- Windows NT 4.0 Workstation is only in extended support until 30th June 2003. During this period a subscription charge may be payable for technical support.
- Windows 2000 will enter its extended life phase in April 2005.
- At time of writing, Windows XP is the newest Windows version; this is in it's

mainstream support phase until 2007.

To increase WinNT/2000 security:

The following lists items that make WinNT or 2000 (Which is NT version 5) more secure, including detection of intrusion, as well as prevention.
At installation, use the NTFS file system instead of FAT. NTFS allows permissions to be set on a per-file/per-directory basis. NTFS also allows auditing on a per-file/per-directory basis. It is also possible to convert existing FAT drives to NTFS. Note that many people recommend using FAT as the boot drive and NTFS for all other drives (due to the convenience in booting into DOS to fix things such as bad clusters on a FAT drive – note that DOS cannot read NTFS). However, using NTFS for all drives definitely offers the best possible file system security. Bear in mind however that other operating systems (Windows 9.X, DOS, and Unix) cannot access NTFS drives except across a network (Important if you dual-boot Windows NT with other operating systems). Also remember that although FAT drives can easily be converted to NTFS, the conversion process cannot be reversed, except by reformatting the drive partition.

Warning: Disable file and printer sharing. If you are a home user having a single stand-alone machine it is simply not needed. If you have a home network, and really need sharing, then at least use a firewall to protect the computers directly connected to the Internet. And do not share any of your drives from the root directory – without a firewall you are making your entire hard disk available to the entire Internet! Here is an example of what *not* to do:

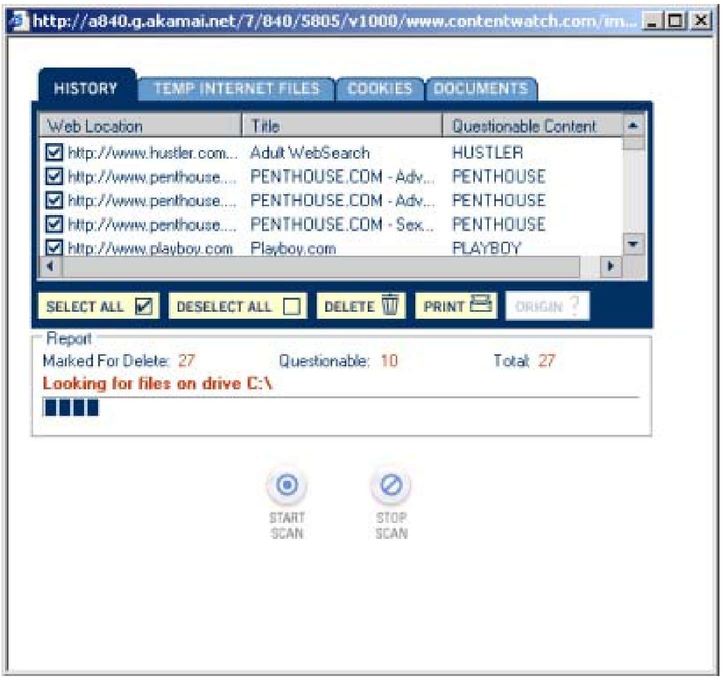


○ Not Shared
● Shared As:
Share Name: E-DRIVE
Comment:
Access Type:
○ Read-Only
● Full
○ Depends on Password
Passwords:
Read-Only Password:
Full Access Password:

This will share your whole drive to the Internet! And full Access as shown will mean that not only can your personal files be read by anyone having your IP address, but modified or deleted also, depending on file permissions. They can also upload files to your hard disk, including Trojan horse programs and other objectionable material. I know of instances where people have discovered pornography hidden in directories all over their computer's hard disk, without them being any the wiser, until they stumbled across it by accident. It later emerged that they had 'file and printer sharing' enabled, and the pornographers had been uploading the pornographic material over a period of several weeks via their broadband connection. Had they been caught in possession of this material, they would have faced legal action.
There is often no easy way to check if an intruder has accessed your system, but here are some obvious signs to look for:

- Any files that you don't recognise;
- Any strange or unusual activity, such as rapidly flashing modem/Network indicators when the connection should be idle;
- Any processes or programs running that you don't recognise.

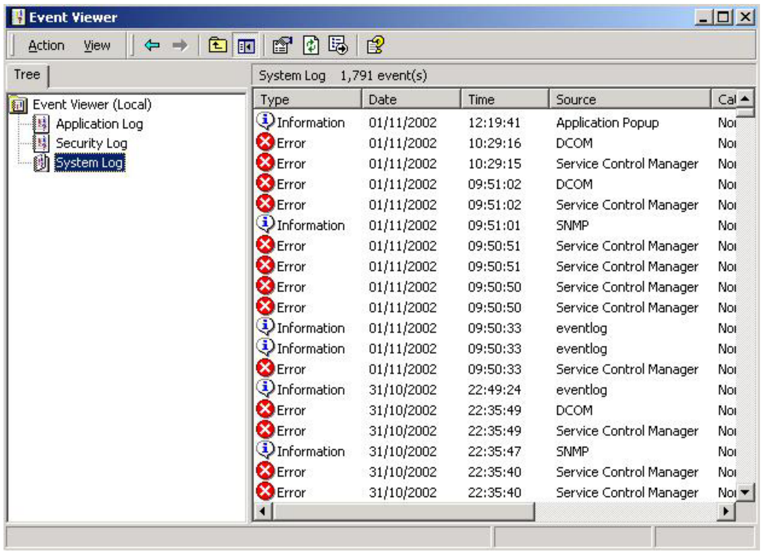
If you suspect that you may have already been targeted in this way, there are many sites which offer remedies. Remember, you should use a different machine to seek help if it is at all possible. For example, Content Watch (www.contentwatch.com) offers many reasonably priced tools to do this. This is a screenshot from their 'Content Cleanup' software, which scans your hard disk for files, links and cookies which are related to pornography:


http://a840.g.akamai.net/7/840/5805/v1000/www.contentwatch.com/im...
HISTORY
TEMP INTERNET FILES
COOKIES
DOCUMENTS

Web Location	Title	Questionable Content
☑ http://www.hustler.com...	Adult WebSearch	HUSTLER
☑ http://www.penthouse....	PENTHOUSE.COM - Adv...	PENTHOUSE
☑ http://www.penthouse....	PENTHOUSE.COM - Adv...	PENTHOUSE
☑ http://www.penthouse....	PENTHOUSE.COM - Sex...	PENTHOUSE
☑ http://www.playboy.com	Playboy.com	PLAYBOY

Report
Marked For Delete: 27 Questionable: 10 Total: 27
Looking for files on drive C:\

Examine your system log files for connections from unknown IP addresses, or for other unusual activity which appears 'out of character'. You can use the Event Viewer which is supplied with Windows NT to check for any unexpected logon, failures of services, or unexplained system restarts. Remember, however, that many 'elite' intruders do edit and falsify log files in an attempt to hide their activities and their effect. The event viewer is found under the 'administrative tools' menu in the control panel. Note that you will need administrative privileges to view all of the information, including the security log.



System Log 1,791 event(s)

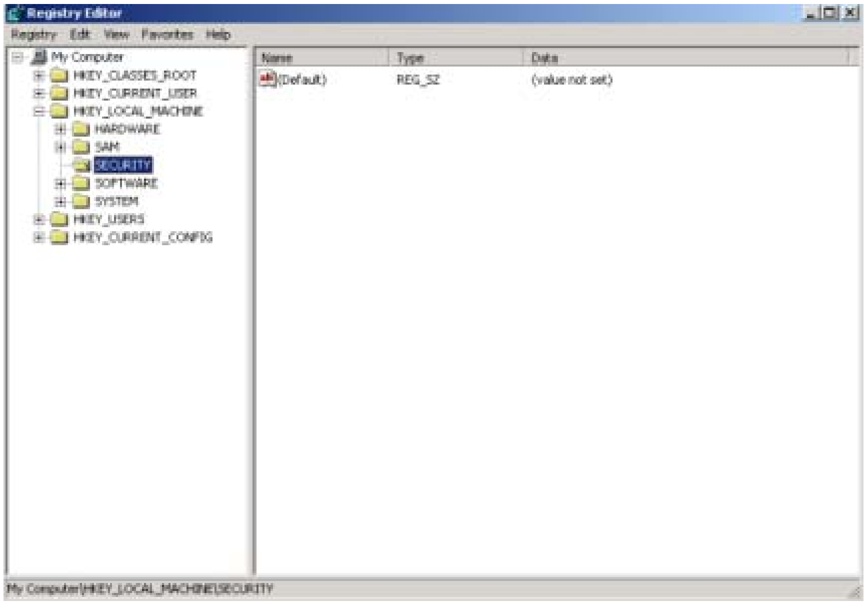
Type	Date	Time	Source	Cal
Information	01/11/2002	12:19:41	Application Popup	Noi
Error	01/11/2002	10:29:16	DCOM	Noi
Error	01/11/2002	10:29:15	Service Control Manager	Noi
Error	01/11/2002	09:51:02	DCOM	Noi
Error	01/11/2002	09:51:02	Service Control Manager	Noi
Information	01/11/2002	09:51:01	SNMP	Noi
Error	01/11/2002	09:50:51	Service Control Manager	Noi
Error	01/11/2002	09:50:51	Service Control Manager	Noi
Error	01/11/2002	09:50:50	Service Control Manager	Noi
Error	01/11/2002	09:50:50	Service Control Manager	Noi
Information	01/11/2002	09:50:33	eventlog	Noi
Information	01/11/2002	09:50:33	eventlog	Noi
Error	01/11/2002	09:50:33	Service Control Manager	Noi
Information	31/10/2002	22:49:24	eventlog	Noi
Error	31/10/2002	22:35:49	DCOM	Noi
Error	31/10/2002	22:35:49	Service Control Manager	Noi
Information	31/10/2002	22:35:47	SNMP	Noi
Error	31/10/2002	22:35:40	Service Control Manager	Noi
Error	31/10/2002	22:35:40	Service Control Manager	Noi

Install the latest service packs and/or patches, for any published security vulnerabilities. These are listed at http://www.microsoft.com/security/. If you are using WinNT 4.0 and you don't have Service Pack #3 (SP3) installed, an intruder can break into your system via such susceptibility. Install this service pack as soon as you can! After all, the service packs are made available for a reason…
User Management (USRMGR): Rename the "administrator" account. A common attack is to use a Dictionary or brute force attack on the "administrator" account, in order to gain administrative access. Normal user accounts (or power user accounts) can be configured to automatically (and temporarily) "lock out" the user after a few failed password attempts, just to be safe. However, this feature simply isn't compatible with an administrator account, because it would make a 'denial of service' attack very easy indeed - (i.e. preventing administration of the machine by deliberate locking out of the administrator account).
If you want to be very awkward for hackers, then create a new account named "administrator" for detecting intrusion attempts. This is known as a honey pot. The trap is set…

Disable the "guest" account. As a home user you probably have no real use for it anyhow. It may let anyone have access to anything accessible to the guest account, without a password being needed! Fortunately, the guest account is at any rate a low privileged account.

Disable "write" access for "Everyone" on the %systemroot%/system32 directory.

Run REGEDT (the Windows registry editor), and turn on auditing for "HKEY_LOCAL_MACHINE\Security" in order to detect remote registry browsing. (You will need to be logged in as an administrator in order to do so). But do not attempt to do this unless you know exactly what you're doing – and back up the registry first. You may end up having to re-install Windows from scratch! This is why you must log in as an administrator to do so! This is an example of the registry editor in use:



Name	Type	Data
(Default)	REG_SZ	(value not set)

My Computer\HKEY_LOCAL_MACHINE\SECURITY

Do not install in a "C:\WINNT" directory, which is the default. Use another name instead. Sometimes intruders will be able to access files if they know the filename; installing in some other named directory prevents a prior knowledge of this. Better yet, if you are feeling very susceptible, install in C:\WINNT, then reinstall in some other directory, then turn auditing on within that directory to alert you to people accessing those older files.

After installation, use the boot partition only for booting and for system files. Put data and applications on a separate partition. (You will need to have partitioned your hard disk to do this – note that re-partitioning a hard disk once set up destroys all data on the volume!!!

It is also sensible to separate applications from data files.

You can use control panel to enable "Password Protected" on the screensaver to deter tampering when you are away from the machine temporarily. The best screensaver is "Blank Screen". You would think that screensavers use limited system resources, but this isn't necessarily true, so you can increase the performance of your computer by using a "Blank Screen" as your screensaver. Also, this will save you some power consumption by the monitor, which typically use about twice as much power as the PC base unit; particularly those that can detect a blank screen and turn themselves off. You can also use the power management option to turn off the monitor after a set period without usage. This is useful if you often leave your computer running to receive or process data, for example.

You can disable account/share information via anonymous access, from the registry editor. Add the"RestrictAnonymous" DWORD with a value of "1" set to the registry key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA" Note that if you see an error "Could not find domain controller for this domain." while setting this option, you may have to change it back. Take care with the registry as I mentioned earlier.

Enable lockout of the "administrator" account for remote access. This causes a remote intruder who fails to guess the correct password after three attempts to be locked out, for example if they are trying to guess the password, or are using a password-cracking program. After lockout, the administrator can only log in locally at the computer concerned. You can also disable remote administrator access completely in the user manager, by removing the right "Access this computer from the network" from "Administrators", (however this disables all remote administration, which makes administration very time-consuming where a large number of WinNT systems are used. If you are a home user, this shouldn't normally be a problem).

Use the 'users and passwords' utility in control panel wisely. Even where you will be the only user of the machine, avoid the temptation to run as administrator all the time. Set yourself up a user account in the 'power users' group instead. The first rule is not to log in using the administrator account for normal computer usage, as doing so leaves you susceptible to many risks. So resist the temptation to run as administrator all of the time, whether or not you *are* the only user of the machine. Anyone who has access to your computer, whether locally or not, can do absolutely anything they choose without restriction. They can copy or erase your data, make modifications to your system, the list is endless. This is particularly true of portable equipment which can potentially be tampered with by a greater number of people each day. So set yourself up a user account as either a power user or regular user.
You are also susceptible to Trojan horse programs, whilst running as administrator. which can make any system modifications they choose! You may, for example, obtain one unknowingly from an unscrupulous website. If you are logged in with administrator privileges, a Trojan horse program can, amongst other things, format your drives, delete all your files, create a new user account with remote administrative access. Choose a strong password and avoid writing it down. Also, enable the option to force users to press control-alt-delete to log in. This should knock out any password capturing programs. You have a responsibility to other users of a computer to keep your system secure. If it succumbs to enemy action, all users data is put at risk.
You should make yourself a member of either the users or power users group. Also disable the guest account if you don't need it. I strongly recommend that the kids' be given only user privileges, it will prevent them from tempering with settings or installing software you don't like, for example. They also are prevented from messing about with any important files! If you should want, for example to install a program without having to log off, and then login again as an administrator, then right-click on it's icon and select 'run as'. This will prompt you for the administrator password before continuing.
Are your computer's users secure from each other?
Your users may all trust one another and *are* all trustworthy. But if one user's account gets successfully compromised and your system is internally insecure, then all your other users files are immediately vulnerable. If any data they have is supposedly confidential, take this into consideration. Warn other users to keep their login accounts secure.
Users should *always remember...*

- Never to lend their account passwords to someone else;
- Be careful about what other accounts they trust;
- Pick good ('strong') passwords. Avoid names, dictionary words and other easily guessed words.

In general, give other users of your system only the access they genuinely need. In Windows NT 4, everyone who is not an administrator is a user; in Windows 2000, there are several types of user. This is the default security level for each type of user (For Windows 2000, using the NTFS file system):

Administrators:

Members of the Administrators group can perform all possible operations. Administrators can grant themselves any rights that they do not have by default. Ideally, administrative access should only be used to install the operating system, hardware devices and software, or to upgrade or repair the operating system. It is also needed to configure system settings, user accounts, passwords and so forth. Occasionally, you may need administrative access may be needed to install and run programs older than Windows 2000, and which may need access to such resources as the system registry. Do not loose or forget the administrator' password as the only possible remedy is to re-install Windows from scratch!

Users:

This group provides normal users with a secure means of normal usage, but they cannot compromise the operating system or other user's data Also, users cannot modify registry settings, operating system files, or program files. Users can create local groups if they wish, but can manage only the groups that they created. They can run certified Windows 2000 programs that have been installed by administrators. Users do also have full control over all of their own data files (%userprofile%) and their own personal portion of the registry (HKEY_CURRENT_USER).

However users *cannot* install programs that can be run by other users, and cannot access other Users private data or settings.

Users will not be able to run most programs written for older Windows versions because previous versions of Windows did not support file system and registry security of Windows 2000. If Users have problems running older applications, then instead make them members of the power users group.

Power Users:

Power Users have all permissions of a user, and in addition, may perform any task except tasks reserved for only administrators. In other words, their user rights are mid-way between those of administrators, and those of users.
Power Users can also, in practice, install programs that do not modify operating system files or the registry. They can also create local (but not network) user accounts, but obviously cannot add themselves or others to the administrator group. They also cannot access other users' data except where they have been given access to

it by either the user concerned, or an administrator. They can, however, create network shares.

Backup Operators:

In case you're curious, members of the Backup Operators' group can back up and restore all files on the computer, regardless of the permissions that protect those files. But however, they cannot change system settings. Note: because backing up and restoring data and system files requires permissions to read and write those files, note that they can also read and modify other users' files.
There are also other 'special groups', I have decided not to cover these as they are not generally relevant to home usage.

Logon authentication *can* be enforced for Windows NT/2000/XP given that the NTFS file system is used; (not FAT). This is because the NTFS file system is secure, i.e. users cannot gain direct access to the hard disk without going through the operating system (the repair utilities provided on the CD-ROM still require the administrator password as authentication).

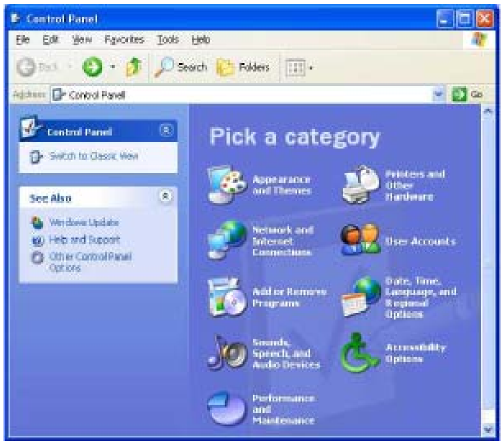
Check for unexplained user accounts. You can use the User Manager tool to view a list of users, or the `net user' command from a command prompt window. The 'net user' command lists the users registered, whereas the 'net group' command will allow a list of user groups to be returned. You may also want to check for users who are members of an incorrect user group, particularly the administrators' group. Backup operators can access any file on the system (as is needed for them to backup data). Power users can create network shares, so you may also wish to check which folders are shared from time to time using the 'net share' command, to list all netbios shares. You may also want to review any additional user rights. Although by default the settings are reasonably secure, take care when giving any user extra rights which they do not have by default.
It is also advisable to check the start-up folders (c:\winnt\profiles\*\start menu\programs\startup) to view which programs are set to run at boot time. Many Trojan horses and spyware programs set themselves up to run automatically. Remove any which you don't recognise, but take care so as not to remove anything important. In general, also remove any programs which are not needed.
Use the task manager (or the pulist or tlist commands) to check for any unauthorised running processes. Each will correspond to an .EXE file somewhere on the hard disk, so if you can locate the executable file, it will tell you something about it's nature. Again, do take care before removing programs. You may need to terminate the process in order to do so; although any 'system critical' processes cannot be terminated. Inadvertently terminating an important process may cause system instability, so be sure to save any open files first!
You may need to check the permissions on system files and registry keys to prevent unauthorised modification. The NT security configuration manager can be used to compare two configurations to determine whether the system configuration has been modified.
If you *do* find any evidence of intrusion, you may be well advised to also check any other machines which you may have connected via a home network. If one machine is compromised, then the chances are that the others may have been also.

To increase Windows XP security (See also NT/2000 advice above as this advice is also relevant):

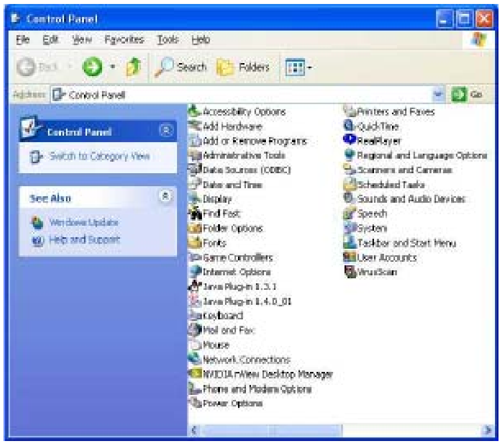
So, you obeyed Microsoft and spent a small fortune upgrading to Windows XP, did you? Well, in all their wisdom, Microsoft, feeling that that file access permissions were much too difficult a concept for home users to cope with, all users should be given administrator privileges by default(!) See their website if you don't believe me! I quote:
"In the simple file sharing model, Windows does not directly expose the complexity of managing file access control lists to the user. Instead, the user interface features an option called "make private" which, when selected for a folder, will modify the underlying access control for that folder so that other non-administrative users cannot access it. This feature only works if the file system is NTFS."
So, beware. In my opinion, learning how file access permissions work is a small sacrifice when compared to the alternative. But first…

Disabling Remote Assistance:

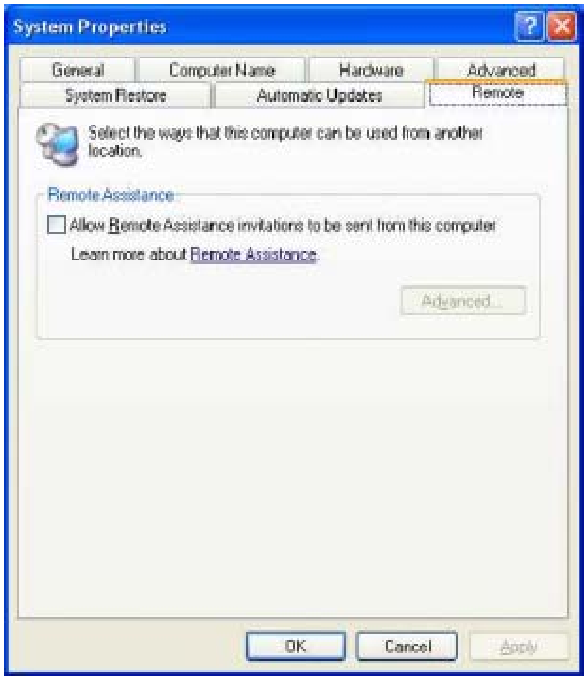
Windows XP Home edition contains a feature known as Remote Assistance, which I feel is a potential source of intrusion. To prevent this, make sure that you can see the System icon in the Control Panel by clicking on Switch to 'Classic View'. You will probably be in 'category view':


Control Panel
File Edit View Favorites Tools Help
Back
Search
Folders
Address Control Panel
Go
Control Panel
Switch to Classic View
See Also
Windows Update
Help and Support
Other Control Panel Options
Pick a category
Appearance and Themes
Printers and Other Hardware
Network and Internet Connections
User Accounts
Add or Remove Programs
Date, Time, Language, and Regional Options
Sounds, Speech, and Audio Devices
Accessibility Options
Performance and Maintenance

When you have changed over to 'classic view', your screen should look like this:



Double-click on the ‘System’ icon, and bring the ‘Remote’ tab to the front. Make sure that ‘Allow Remote Assistance invitations to be sent from this computer’ is not ticked:



Select the ways that this computer can be used from another location.

□ Allow Remote Assistance invitations to be sent from this computer

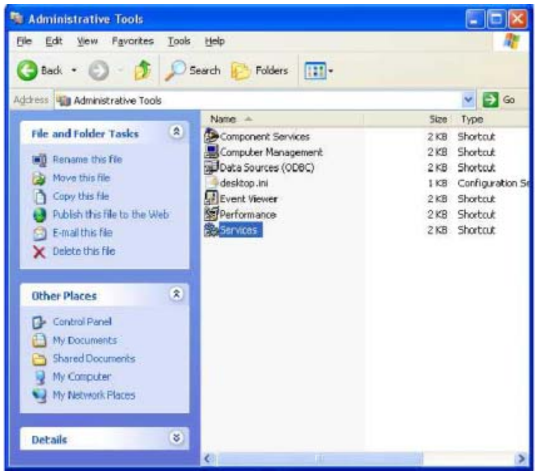
Learn more about Remote Assistance.

You are unlikely to need this service, and in any event, do you really want to advertise your availability to unknown (and possibly malicious) individuals?

Disabling Universal Plug and Play (UPnP, port 5000):

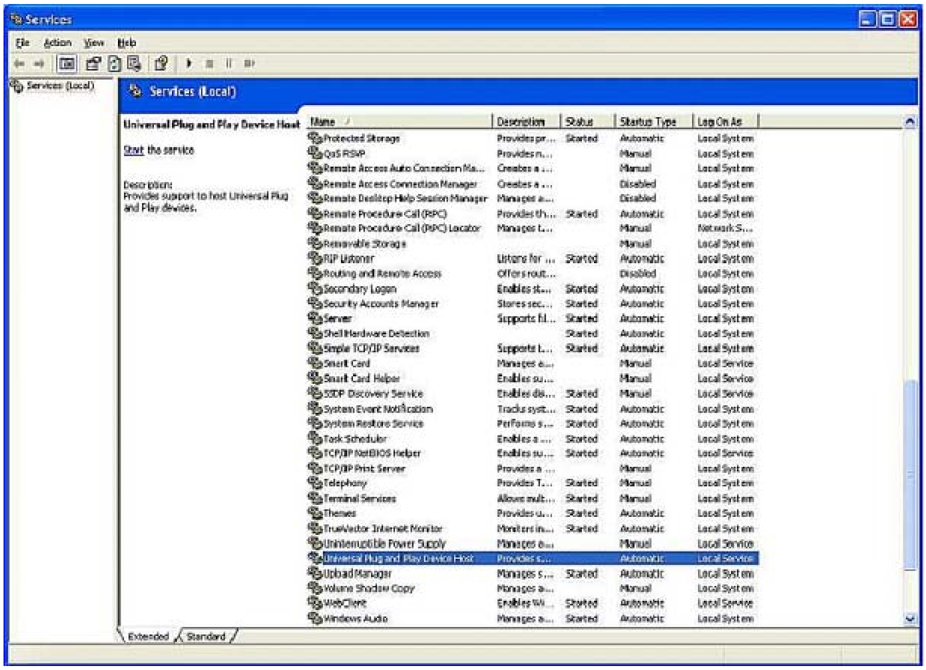
This is yet another example of an unnecessary server, which Microsoft has enabled by default, is accessible to the Internet, and already has known bugs which allow a system compromise (Denial/ Distributed Denial of service). Universal Plug and Play is a set of communications protocol standards that allow networked TCP/IP devices to announce their presence to all other UPnP devices on the network, and to then inter-operate in a flexible and pre-defined fashion. There is nothing wrong with this idea in itself, but devices utilising such technology are not currently widespread, and as

security was not really a consideration in development, it has some, already known, flaws.
(So even now Microsoft are supposedly addressing security issues, they still have failed to learn, through past experience, the vital security rule 'do not enable services which may well prove unnecessary the average user, as a ‘default setting’!).
Since you are unlikely to need UPNP in the foreseeable future, (I personally have yet to come across a single hardware device which supports it!!!); you should disable it . Open the Control Panel , make sure that you are switched to the 'Classic' view (see instructions above) and then double-click on Administrative Tools . Then double-click on the Services icon:



Name	Size	Type
Component Services	2 KB	Shortcut
Computer Management	2 KB	Shortcut
Data Sources (ODBC)	2 KB	Shortcut
desktop.ini	1 KB	Configuration Se
Event Viewer	2 KB	Shortcut
Performance	2 KB	Shortcut
Services	2 KB	Shortcut

Double-click on ‘Universal Plug and Play Device Host’. Click on ‘Stop’ .You have now stopped the service but not disabled it. (If you do not disable it, then it will simply start again next time you restart the computer!)



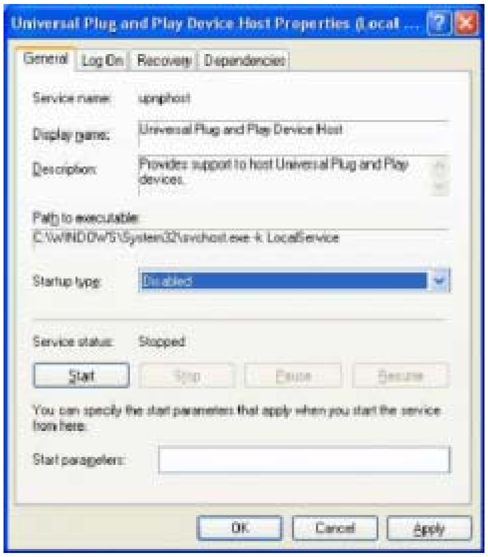
Universal Plug and Play Device Host

Start the service

Description:
Provides support to host Universal Plug and Play devices.

Name	Description	Status	Startup Type	Log On As
Protected Storage	Provides pr...	Started	Automatic	Local System
QoS RSVP	Provides n...		Manual	Local System
Remote Access Auto Connection Ma...	Creates a ...		Manual	Local System
Remote Access Connection Manager	Creates a ...		Disabled	Local System
Remote Desktop Help Session Manager	Manages a...		Disabled	Local System
Remote Procedure Call (RPC)	Provides th...	Started	Automatic	Local System
Remote Procedure Call (RPC) Locator	Manages t...		Manual	Network S...
Removable Storage			Manual	Local System
RIP Listener	Listens for ...	Started	Automatic	Local System
Routing and Remote Access	Offers rout...		Disabled	Local System
Secondary Logon	Enables st...	Started	Automatic	Local System
Security Accounts Manager	Stores sec...	Started	Automatic	Local System
Server	Supports fil...	Started	Automatic	Local System
Shell Hardware Detection		Started	Automatic	Local System
Simple TCP/IP Services	Supports t...	Started	Automatic	Local System
Smart Card	Manages a...		Manual	Local Service
Smart Card Helper	Enables su...		Manual	Local Service
SSDP Discovery Service	Enables dis...	Started	Manual	Local Service
System Event Notification	Tracks syst...	Started	Automatic	Local System
System Restore Service	Performs s...	Started	Automatic	Local System
Task Scheduler	Enables a ...	Started	Automatic	Local System
TCP/IP NetBIOS Helper	Enables su...	Started	Automatic	Local Service
TCP/IP Print Server	Provides a ...		Manual	Local System
Telephony	Provides T...	Started	Manual	Local System
Terminal Services	Allows mult...	Started	Manual	Local System
Themes	Provides u...	Started	Automatic	Local System
TrueVector Internet Monitor	Monitors in...	Started	Automatic	Local System
Uninterruptible Power Supply	Manages a...		Manual	Local Service
Universal Plug and Play Device Host	Provides s...		Automatic	Local Service
Upload Manager	Manages s...	Started	Automatic	Local System
Volume Shadow Copy	Manages a...		Manual	Local System
WebClient	Enables Wi...	Started	Automatic	Local Service
Windows Audio	Manages a...	Started	Automatic	Local System

Click OK to return to the Services page, where you will now see that the service is no longer shown as Started. Then double-click on the Universal Plug and Play Device Host line again and change the 'start-up type' to 'Disabled' from the dropdown menu.



Universal Plug and Play Device Host Properties (Local ...

Service name: upnphost

Display name: Universal Plug and Play Device Host

Description: Provides support to host Universal Plug and Play devices.

Path to executable:
C:\WINDOWS\System32\svchost.exe -k LocalService

Startup type: Disabled

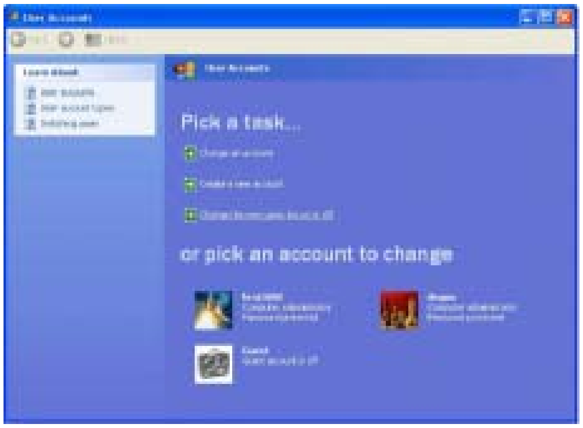
Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

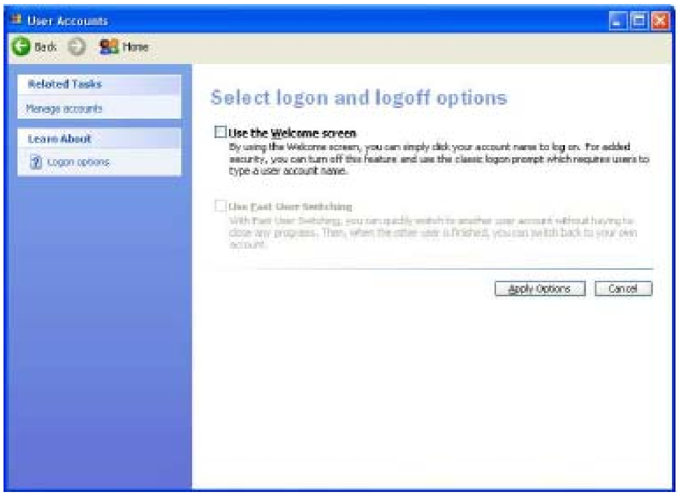
Start parameters:

Password protecting Your User Accounts:

If you currently have the 'Welcome screen logon' enabled you should disable it.(This presents every user as a small icon with their name beside it. Clicking on it enables users to login without entering a password, and is totally insecure. So much for Microsoft being committed to security – this is no better than Windows 9.X allowing you to bypass the login prompt by pressing escape!!!) You should disable this before attempting to password your accounts. Open 'User Accounts' in the Control Panel:



Then: Select 'Change the way users log on and off'. Make absolutely sure that the 'Welcome Screen' is *not* ticked and click on 'Apply Options':

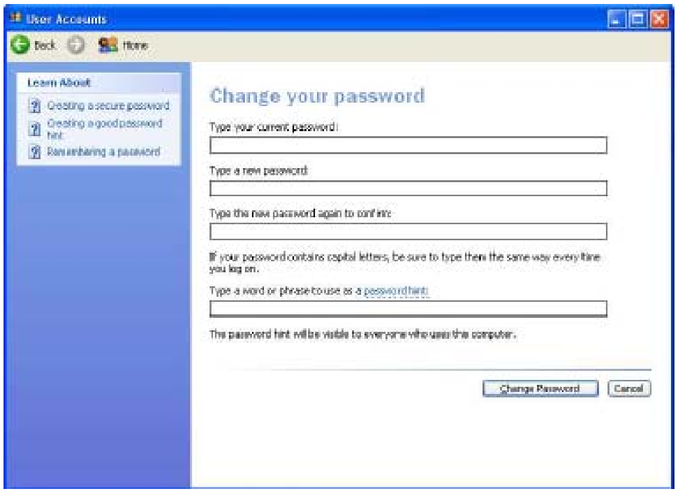


Select logon and logoff options

□ Use the Welcome screen
By using the Welcome screen, you can simply click your account name to log on. For added security, you can turn off this feature and use the classic logon prompt which requires users to type a user account name.

□ Use Fast User Switching
With Fast User Switching, you can quickly switch to another user account without having to close any programs. Then, when the other user is finished, you can switch back to your own account.

Next, go back into the Control Panel and pick 'User Accounts', and then select 'Change an account' .This will take you to a list of accounts. Select your own and then choose ‘Change my password’.



Change your password

Type your current password:

Type a new password:

Type the new password again to confirm:

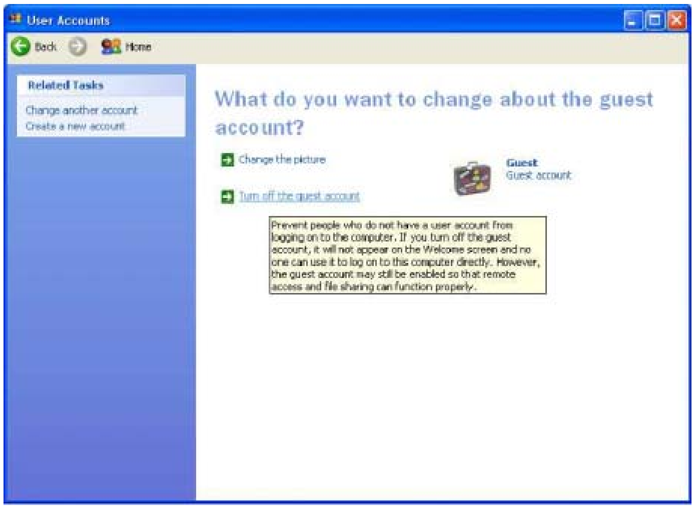
If your password contains capital letters, be sure to type them the same way every time you log on.

Type a word or phrase to use as a password hint:

The password hint will be visible to everyone who uses this computer.

Note: If you have not used passwords on your machine previously, your password will be blank. You should not enter anything on the ‘Type your current password:’ box i.e. leave it blank. You must now enter a new password (not less than six-eight characters for security, see also my suggestions for choosing a password) and not a dictionary word for instance, which is dead easy to guess, and then confirm it by entering it a second time on the line below.

Click on Change Password and you will have successfully password your account. You need to do this also for any other accounts you have on your computer except the Guest account. You should probably wish to disable this anyway, by clicking the guest account icon from the ‘User Accounts’ screen:



What do you want to change about the guest account?

Change the picture

Turn off the guest account

Guest
Guest account

Prevent people who do not have a user account from logging on to the computer. If you turn off the guest account, it will not appear on the Welcome screen and no one can use it to log on to this computer directly. However, the guest account may still be enabled so that remote access and file sharing can function properly.

From the next screen, choose 'Turn off the guest account'. Finally you may see an account called Owner from your User Accounts screen. This account is created if no user accounts were enabled when Windows XP was installed. This account must be password protected as well to fully protect your computer. You can also rename it, as this is good advice.

File & Printer Sharing:

Windows XP Home Edition always has 'Simple File Sharing' enabled. Windows XP Professional computers in a workgroup file sharing enabled by default. Windows XP Professional computers that are in a domain have only the classic file sharing and security interface. You configure file sharing by right clicking on a folder and selecting the 'properties' tab.
I strongly recommend that you disable 'simple file sharing' if you don't need it. Home users usually don't. If you really must use it, then alternatively you can also set the permissions to individual users given that you have adequate knowledge of the NTFS file system and the sharing permissions in order to use this facility.

Warning: By simply disabling 'simple file sharing', the file sharing protocol *is not disabled*. (I see, it's just so typical of Microsoft!). This means that all files in the 'My documents' folder, for example, *are still shared*. (Personally, I always found the insistence of Windows applications on wanting to save everything in this folder a wretched nuisance anyhow; as I prefer to organise *my* work in my *own* way.). Unless you still want to share this folder (to everyone on the Internet without a firewall!), you must disable the 'shared documents' facility also. And here's how:

Double-click the desktop 'my computer' icon;
On the 'tools' menu, click 'folder options';
Click the 'view' tab, and then click to deselect the 'use simple file sharing' check box to disable 'simple file sharing'.

To disable the ‘shared documents’ facility, you need to understand the access levels and their properties (permissions for various users), which are somewhat more involved than those of earlier versions of Windows NT:

Access Level	Name	Everyone (Local)	Owner	System	Administrators	Everyone (Network)
1	Private	None	Full	Full	None	None
2	Default	None	Full	Full	Full	None
3	Files Available Locally to Everyone	Read	Full	Full	Full	None
4	Read Access to All on Network	Read	Full	Full	Full	Read Only
5	Read/Write Access to All on Network)	Change	Full	Full	Full	Full

As you can see, care must be taken here! Note that when Windows XP is set up, the default level (2) is used. Remember that ‘Local’ users include a user who logon to a Windows XP Professional-based computer from a Remote Desktop (RDP) session. Note that without a firewall protecting your system, Level 4 allows read-only access to your files from the Internet, and level 5 also permits your files to be modified or deleted by *anyone on the Internet*! Remember that ‘full access means precisely that. Read only means that your files cannot be modified or deleted; however someone can still read the contents, or copy the files to examine later.

To set a folders access level-to-level 1, right-click the folder in Windows Explorer, and then click ‘sharing and security’. Select the ‘make this folder private’ check box, and then click OK.

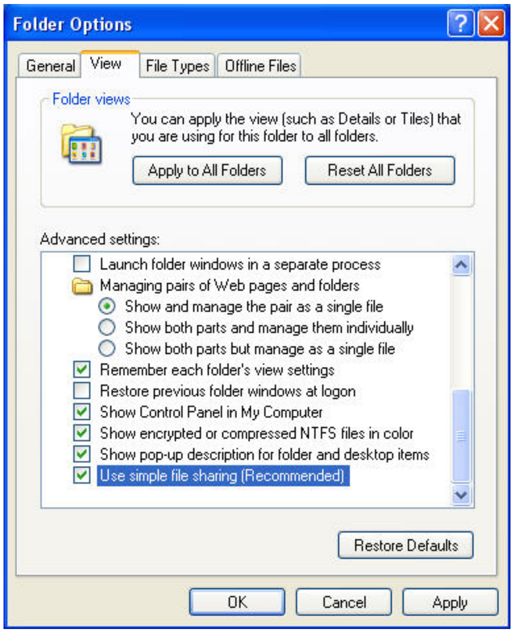
If you have recently upgraded to Windows XP, bear in mind the following points:

A Windows 2000 Professional computer that is upgraded to Windows XP Professional maintains its domain or workgroup membership. NTFS and share permissions are not changed at time of upgrade.

A Windows NT computer that is upgraded to Windows XP Professional maintains its domain or workgroup membership. NTFS and share permissions do not change with the upgrade.

A Windows 95, 98 or Windows Millennium Edition (Me) computer that has "per share" sharing permissions that is upgraded to Windows XP has 'simple file sharing’ enabled by default. Shares that have passwords assigned to them are removed, but shares that have blank passwords *remain shared after the upgrade.*

This is the ‘Folder Options’ dialogue box in Windows XP:

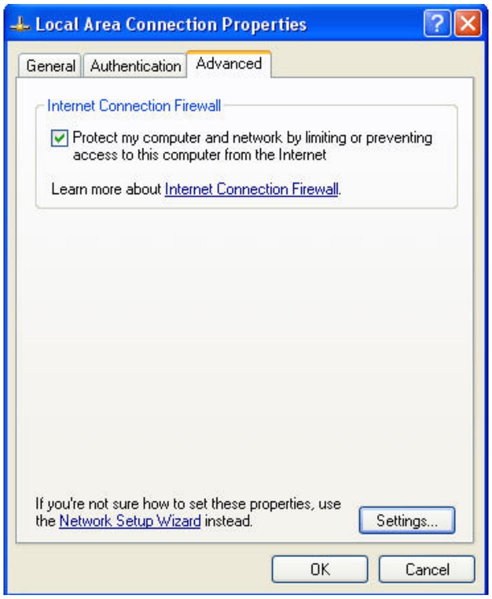


You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

- □ Launch folder windows in a separate process
- Managing pairs of Web pages and folders
  - ● Show and manage the pair as a single file
  - ○ Show both parts and manage them individually
  - ○ Show both parts but manage as a single file
- ☑ Remember each folder's view settings
- □ Restore previous folder windows at logon
- ☑ Show Control Panel in My Computer
- ☑ Show encrypted or compressed NTFS files in color
- ☑ Show pop-up description for folder and desktop items
- ☑ Use simple file sharing (Recommended)

Use Internet Connection Firewall (or preferably something better):
One of the few features of Windows XP that I really like is that it does at least come complete with it's own, very basic, firewall. This is called 'Internet Connection Firewall'. To enable ICF, right-click on an Internet connection in the 'network connections' wizard, click 'properties', and then click the 'advanced' tab, and the ICF check box:



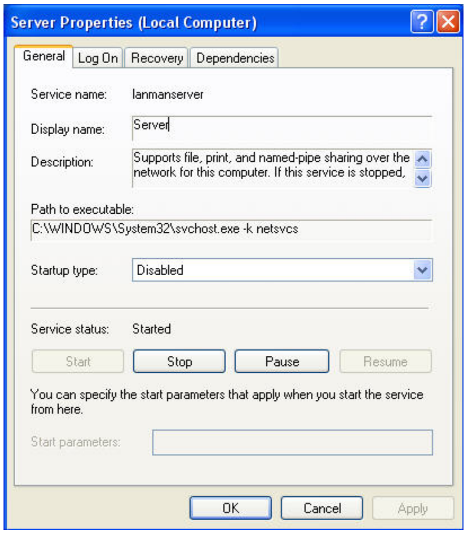
Local Area Connection Properties
General
Authentication
Advanced
Internet Connection Firewall
Settings...
OK
Cancel

☑ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.

If you're not sure how to set these properties, use the Network Setup Wizard instead.

If you are a home user, having a stand-alone PC connected to the Internet, I would also suggest that you disable the server services. You probably have no practical reason to leave them enabled and they represent an unnecessary source of susceptibility. This is found under the 'general' tab of the server properties wizard:



Server Properties (Local Computer)

Service name: lanmanserver

Display name: Server

Description: Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped,

Path to executable:
C:\WINDOWS\System32\svchost.exe -k netsvcs

Startup type: Disabled

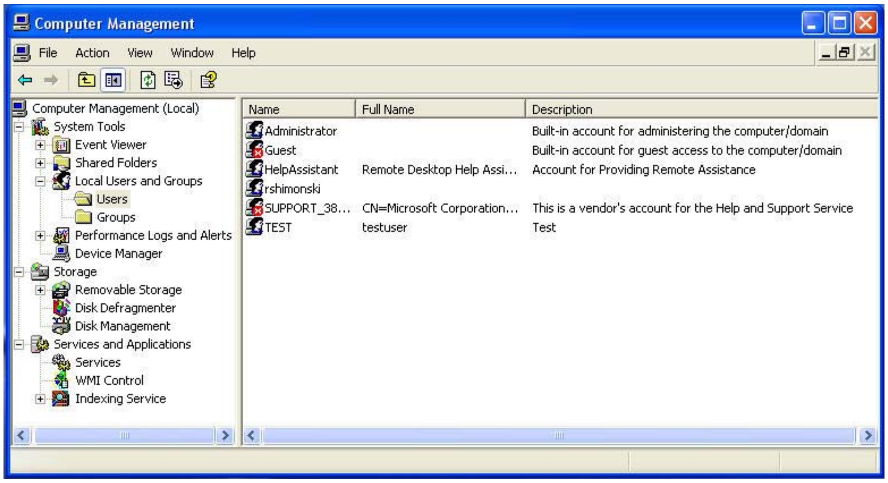
Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Warning! Internet connection Firewall is only a very basic Firewall. In particular, it *does not block or even monitor* outgoing connections. This implies that absolutely no protection is given against Trojan horses or ‘spyware’ which are intended to steal confidential information. For this reason, you may wish to replace ICF with a proper firewall which monitors all connections, whether incoming or not.

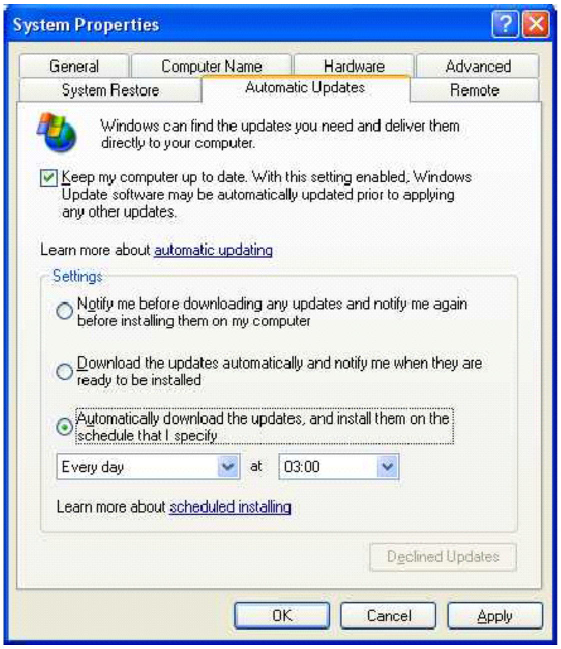
Also, remove any unused user accounts, using the ‘computer management’ wizard. In particular the guest account should be disabled if not genuinely needed, as for Windows NT/2000. You may also want to rename the administrator or ‘Owner’ account. Also, do not log in as an administrator except for purposes which genuinely require administrator access rights. You really do not need to do so for everyday usage – use your own user account instead. Logging in as an administrator when you don’t even need to leaves you open to a large number of unnecessary risks. And as for all operating systems, be sure to keep your antiviral software and system updates up to date. Remember that the updates are provided for a reason.
The above recommendations are Windows XP specific. However, the vast majority of the advice given for Windows NT and 2000 also applies to XP as XP is based on the earlier Windows NT operating system. The above information caters for the differences between Windows XP and it’s predecessors.



Name	Full Name	Description
Administrator		Built-in account for administering the computer/domain
Guest		Built-in account for guest access to the computer/domain
HelpAssistant	Remote Desktop Help Assi…	Account for Providing Remote Assistance
rshimonski		
SUPPORT_38…	CN=Microsoft Corporation…	This is a vendor's account for the Help and Support Service
TEST	testuser	Test

Configuring Windows Update Configure Windows XP to update your machine automatically:

Microsoft constantly issues patches and service packs for any software defects as they come to light, so I strongly recommend that you keep your machine updated regularly. The easiest way to do this if you have a permanent connection to the Internet, such as a broadband connection, and you normally leave your machine running, is to configure the machine to update itself and restart if necessary overnight - but be sure you save any open files when leaving the computer to it's own devices! To do this, right-click on the 'My Computer' icon, choose 'Properties' and select the 'Automatic Updates' tab. Select 'Automatically
download the updates', and install them at a convenient time, for example during the early hours. It is good advice to check for updates regularly, say every week or two.



Windows can find the updates you need and deliver them directly to your computer.

☑ Keep my computer up to date. With this setting enabled, Windows Update software may be automatically updated prior to applying any other updates.

Learn more about automatic updating

Settings

○ Notify me before downloading any updates and notify me again before installing them on my computer

○ Download the updates automatically and notify me when they are ready to be installed

● Automatically download the updates, and install them on the schedule that I specify

Every day at 03:00

Learn more about scheduled installing

If you normally shut down your computer overnight, or when not needed, then you are better off using the ‘Download the updates automatically and notify me when they are ready to be installed’ option. This is still convenient if you use a broadband connection.
Dial-up users are somewhat less vulnerable to hacking than broadband users, however they should still keep their computer updated, for example, once a month at minimum.

To increase Win95/Win98/ME security:

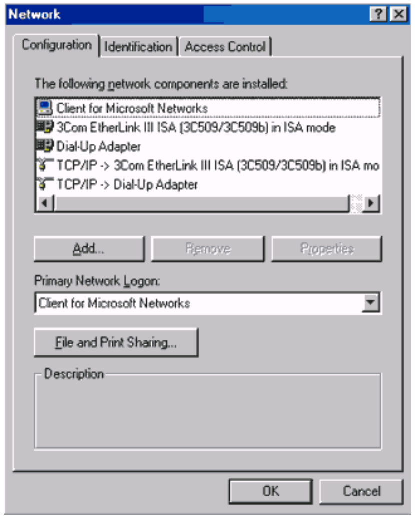
This advice is intended for a typical home computer user running Win9.X and accessing the Internet either via a modem, or via DSL or cable.
Well, how do I begin? The only real means to secure a PC running Windows 95, 98 or ME, is to exchange this horrendously insecure operating system and install Windows NT, 2000 or XP in it’s place. And then, you will need to convert the FAT file system to NTFS, in order to take advantage of the security features it has to offer. In all honesty all versions of Windows 9.X cannot be made secure. Security was never built into these versions of Windows, so don’t expect to make a good job of ‘tacking it on’ afterwards! You could write a thesis regarding what Windows 9.X leaves to be desired. There are numerous vulnerabilities, which include amongst other things, a complete lack of:

- File permissions;
- Password encryption (of which Windows 95 has none at all!);
- Registry protection;
- System file protection.

Little wonder then, that the best advice is to replace Windows 9.X outright.
The Windows 9x/ME operating system was never designed to be a "secure" system. Win95/Win98/ME have no auditing or logging capabilities. Additionally, it also only offers the FAT file system, which has no built-in security features.
Anyone with physical access to your computer has full access to every single file on your computer, and if you have your whole hard drive shared to the Internet via ‘file and printer sharing’, then so does every single user of the Internet!

(Warning – if you have file & printer sharing enabled, and your hard drive shared from the root directory, anyone on the Internet has full access to every single file & directory on your hard disk!!!). You really should upgrade to WinNT and use the NTFS file system, if you are using the computer for any serious or work-related purpose. The following suggestions will help improve security (but the above suggestion to upgrade to Windows NT or 2000 is far preferable). For the typical user:

Turn off file and printer sharing – remember what I said earlier. When sharing is turned on, the system creates a PRINTER$ share that allows remote systems to access printer drivers from the local system32 directory. Unfortunately, this allows remote systems to access non-driver files, such as the Win95 password file. Note that Windows 95 First Edition does not encrypt passwords at all! Turn off file sharing anyhow. As a home user, you probably don't need it. One means by which to do so is to right-click on the ‘network neighbourhood’ icon; this should bring up the ‘network’ dialogue box. Select the configuration tab and then the ‘file & print sharing’ icon:

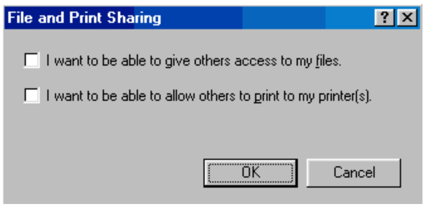


The following network components are installed:

- Client for Microsoft Networks
- 3Com EtherLink III ISA (3C509/3C509b) in ISA mode
- Dial-Up Adapter
- TCP/IP -> 3Com EtherLink III ISA (3C509/3C509b) in ISA mo
- TCP/IP -> Dial-Up Adapter

Primary Network Logon:
Client for Microsoft Networks

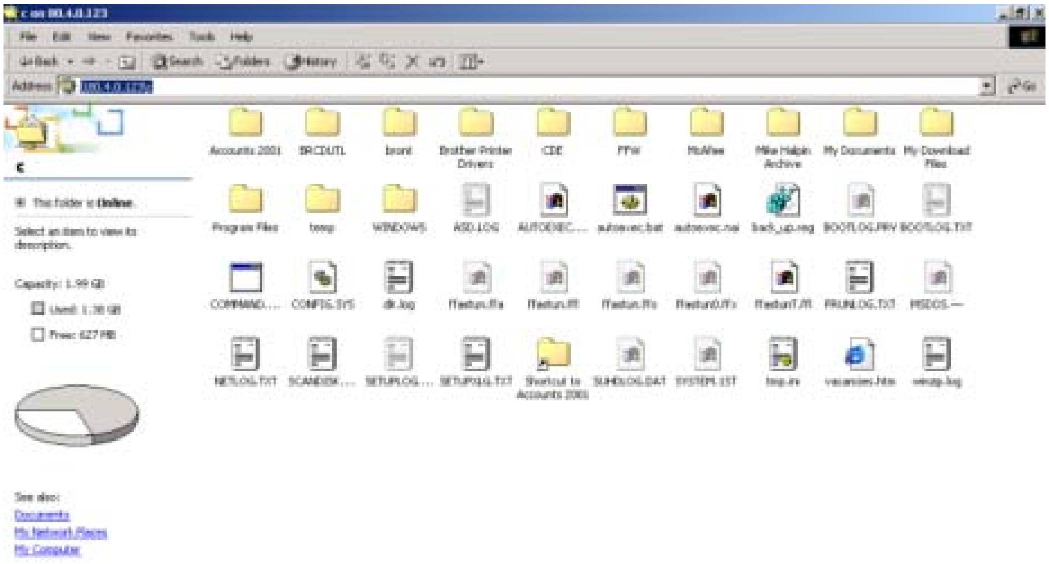
Ensure that you *de-select* both file sharing and printer sharing:



□ I want to be able to give others access to my files.

□ I want to be able to allow others to print to my printer(s).

If you absolutely *must* share files, make sure that you choose a strong password to protect your shared directories, and *only* turn it on for brief moments while you need to share the files, then turn it off again. Here is how your hard disk will appear to someone who has accessed it via the Internet, where your whole hard disk is shared *from the root directory*:



As you can see, if you have shared your whole hard disk, then all files and directories can be seen. It's just as though they were looking at the root directory of their own hard disk…

Win9.X also caches passwords in easily decoded formats, so you would probably wish to remove the password files. Go to MSDOS prompt, and type 'del c:\windows\*.pwl' . The password cache file will often be the first and most obvious one intruders look for. It has the same name as the user name(!), and poorly encrypts the cached passwords (not at all in Windows 95!). This however deletes dial-up networking passwords as well, so take care if you use dial-up networking.

Disable internal caching of passwords from the registry: Run:
REGEDIT /s \\MY_PDC\netlogon\nocache.reg
where "nocache.reg" consists of:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network]
"DisablePwdCaching"=dword:00000001
```

As always, take great care when using the registry editor! Do so only if you are adequately experienced to do so, as mistakes cannot easily be rectified later. It is good advice to back up your registry before making changes! I am not responsible for the result of any mistakes here!

Authentication:

Unless your computer is connected to a very secure network, *anyone* can logon to Windows 9.X as a new user - simply by typing a new user name at the logon prompt! Or an unauthorised user can just press the Cancel button at the logon prompt and start using the computer as the default user. Although you can't log onto a network by doing so, all files and settings on the workstation are fully accessible. To deal with this problem:

Make sure that the user profiles are enabled and created for each user, and that the 'include start menu' and 'program groups' in the 'user settings' option is enabled for each user - you can easily lock yourself out of your own computer by using this method if you don't!

Make sure you know how to reboot Windows in the 'safe mode', by pressing a hotkey (usually F8) during start-up. If something fails to produce the expected result, you can always reboot your computer in safe mode and correct the problem.
Run registry editor (Go to Start, select run and type RegEdit.exe). Please be very careful when using this tool, because if you do something wrong with it, you can mess up your registry and then you will find yourself reinstalling Windows all over afresh!

Find the following key in the Registry:

```
 HKEY_USERS
   .Default > Software > Microsoft Windows > CurrentVersion > Run
```

Create a new string value under this key and rename it to some other name. To create the
string value: right-click on 'run', select New > String Value from the shortcut menu, and then enter your new entry.

Now open the entry you've just created by double-clicking it in the right tab of the registry editor window and specify the following command as its value:

```
rundll.exe user.exe, EXITWINDOWS
```

From now on, whenever someone logs on by pressing Cancel on the logon prompt, or by entering a new user name in the logon screen, the session will be immediately terminated. The other user accounts may be used as usual. To restore the original setting, simply delete the entry you've created.

If you want to create a new user account, you should remove this entry before creating the account, and then restore the entry back after the new account has been created. Otherwise, the new user account acquires the settings of this invalid entry and is inaccessible.
I would strongly recommend upgrading to Windows NT or 2000 in preference to these measures. Use this method only where you are stuck with 9.X.

Disable MSDOS Mode:

Windows lets anyone press Ctrl+C during start-up. If the user is knowledgeable of MSDOS, they can then examine and modify or erase your files from DOS. To protect yourself from this susceptibility:

First, make a backup copy of the C:\CONFIG.SYS file on a start-up disk, in case anything goes wrong.
Make sure that you can actually boot the computer into DOS using this disk!
Then type ‘edit C:\CONFIG.SYS’ and add the following command at the very beginning of the file:

```
BREAK=OFF
```

Now save the config.sys file and reboot the computer. Note: Note that this setting also disables the Ctrl+C exit method for all programs running in the MSDOS mode. If you would like to prevent users from using the Restart in MS-DOS mode command (one of the shut down options offered by Windows 9.X), here is the method:
Run Windows Explorer and open the folder in which Windows is installed – normally C:\Windows). and locate the following item: Exit To Dos (Shortcut to MS-DOS Program). Highlight it.

Make a backup copy of this file just to be on the safe side. While it is highlighted, press Ctrl+C, and then press Ctrl+V. This should create a new file named ‘Copy of Exit To Dos’. If anything goes wrong, you can use it to restore the original copy of this file. While ‘Exit To Dos’ is selected, press Alt-Enter to open its ‘Properties’ dialog. Select the Program tab. Change the Cmd line field to read as follows:

C:\Windows\Win.com – Unless of course Windows is installed in a different folder, in which case specify the correct path. Then press OK to close the dialog box. Finally, try to restart the computer in the MS-DOS mode to test the new setting. After a time, Windows should re-start instead of MSDOS.

To prevent modification of dial-up networking settings:

This can be achieved by deleting or renaming the file RNAUI.DLL, located in the Windows\System folder. You may wish to keep a backup copy of this file elsewhere should you wish to modify them yourself later.

Windows 95 cannot in reality, be booted in a secure manner as the file system (FAT) does not have any security built in, as is the case for the NTFS file system offered by Windows NT/2000/XP.
Bear in mind also that at time of writing, versions of Windows up to and including 95 are no longer supported by Microsoft, and that implies no further service packs or updates are available. You should consider upgrading, preferably to Windows 2000.

To increase Macintosh security:

Macintoshes usually (by default) support very few services that can readily be hacked. In comparison, Windows machines are far more common, whether in the home or business environment, and although less common, UNIX machines have a lot more ‘interesting’ services running on them than the average Windows system (although not Netbios!). This is due to the fact that Macintosh systems are very much geared toward the ‘end user’, more than are Unix/Linux, or even Windows systems. Thus, Macintoshes are not particularly interesting to hackers. Beyond this point, I admittedly know of very few documented Macintosh Vulnerabilities. You may wish to check any documentation which comes with certain ‘add on’ software, e.g. web servers, which you may install, however. You may also want to disable file sharing for Macintosh where applicable.

To turn off file sharing for Macintosh:
Open the ‘Sharing’ control panel. In the File Sharing area of the window, make sure you see the message, "File sharing is off." You should see a Start button to the left of the status box. If there's a Stop button, then sharing is on. Click the stop button. When the dialog box appears, asking, "How many minutes until file sharing is disabled?" Select "0" and click OK. This will immediately turn off sharing. Note that future versions of the Mac OS (10 and higher) may vary in this respect.
Macintosh file systems come mid-way between those of Windows 9.X and NT in terms of their security. They cannot be booted from a secure centralised network source for example, and although the file system itself is more secure than that of Windows 9.X, it turns out that authentication measures *can* be evaded by those with adequate knowledge of the Macintosh OS.

To increase Unix/Linux security:

One of the problems with Linux in specific is that it is free. This brings with it a number of vulnerabilities. With Linux systems that are not ‘bolted down’ from a security point of view, or often those that are running older ‘known-to-be-vulnerable’ software, it can be unbelievably easy to find insecure Linux machines to hack into. While the average teenage hacker would not have access to their own machine running a Sun, operating system, for example, to work out how to crack into it, most will have access to a PC running Linux to experiment on. There are even a number of ready-made scripts or applications available for the ‘first time’ hacker, who don't as yet have the technical knowledge to hack into a system ‘from first principles’, but are certainly quite capable of running a proprietary program which does all the hard work for them! Linux and Unix versions vary in the services that they offer by default, and of course this will vary depending on what services you yourself choose to install. Hence you should check to see what is enabled. You may even wish to run a port scan on all 65536 ports, just to be certain.
Bear in mind that network services are offered in two ways; either as standalone daemon processes (usually for things such as samba (file sharing), nfs (file sharing), lpd (printing), httpd (web serving)), or as programs which are started from inetd.

Installing Services:

When installing Unix/Linux, only install the options and services that you actually need; you can always add extra components later, as under Windows. If you install all available options, you will end up with a large number of open ports which you need to avoid. Remember that as a general rule, as potential hacker can only exploit open ports, then fewer open ports you have accepting connections, the less susceptibility your system has to attack. This advice holds true for all operating systems. When installation is completed, use the 'netstat' and ‘rpcinfo’ commands to list all services running and their corresponding open ports. Disable any services which are running and which you don’t actually need. Red Hat Linux, for example, has quite a number of vulnerabilities which (by now) are well known amongst hackers. This is the reason you should ensure that any services you don’t explicitly require is disabled.
The first thing to realise when installing a Linux (or any other) operating system is that most distributions are not actually 100% secure ‘out of the box’. Most Linux distributions ship with default settings, which will helpfully set up systems such that they will happily run services which accept incoming connections, which include: telnet, file transfer protocol, remote shell, remote login, Imap email, pop-3 email, ntp (Network Time Protocol), nntp (Network News Services) and smtp (Email delivery relays). While this is set up with the intention to ‘get it up and running with the minimum of fuss, it leaves a lot to be desired from a security point of view! Each of these services will present a corresponding open port, which advertises it’s presence, and maybe a number of potential vulnerabilities, to all who may wish to exploit them. See the earlier ‘port scanning’ section and follow the directions relating to the Unix/Linux services, and disable any services you may be running and which you don’t actually need. For example, if you won’t be needing to receive incoming email on your system, then you can disable the smtp mail listener. If you really need to offer anonymous FTP, ensure that only anonymous downloads (and not uploads) are possible.
Remember, it is always wise to turn off any network services which you do not intend to use. Do however be aware that these services may vary between Unix and Linux, and between different versions of either. Consult the documentation which shipped with the variant you have.

Logging in as root:

Ensure that root can only login from the console of the local machine itself. Valid terminals allowed to log in as root are listed in the file /etc/security, or /etc/login.defs depending on the variant of Unix or Linux you are using. You will still be able to access root by using the ‘su’ command once you have logged in as a normal user. You should resist the temptation to log in as root, even where you are the only user of the machine: only login as root when you need to; don't carry out normal user tasks as root. This is the equivalent to my advice regarding logging in as administrator in Windows NT, 2000 or XP. When you don’t genuinely *need* root privileges, why take unnecessary risks? Create a lower privilege account for normal usage.
Be sure to secure your password file, as this is a favourite starting point for attacks on a Unix or Linux system. Try logging in as ‘anonymous’ from another machine, and attempt to take a copy of your password file (/etc/passwd). If you can copy this file, then so can absolutely anybody else! If you will be connected to the Internet, this is a very important point indeed. Also, beware packet sniffing – on an Ethernet, such as a

cable modem network, any other machine on the same subnet as yourself can potentially capture passwords, where you log into your machine remotely. So be careful when doing so! As mentioned previously, it is best not to log in as root remotely at all. Take care with the .rhosts file, and ensure that no-one else can access it remotely!

Unix/Linux file systems in general do not in themselves present a security problem. Given that root access is secured from unauthorised users of the system, and given that it can be guaranteed that the operating system is adequately patched and maintained, then non-root users can be adequately authenticated and constrained.

---

14) Use of a Firewall

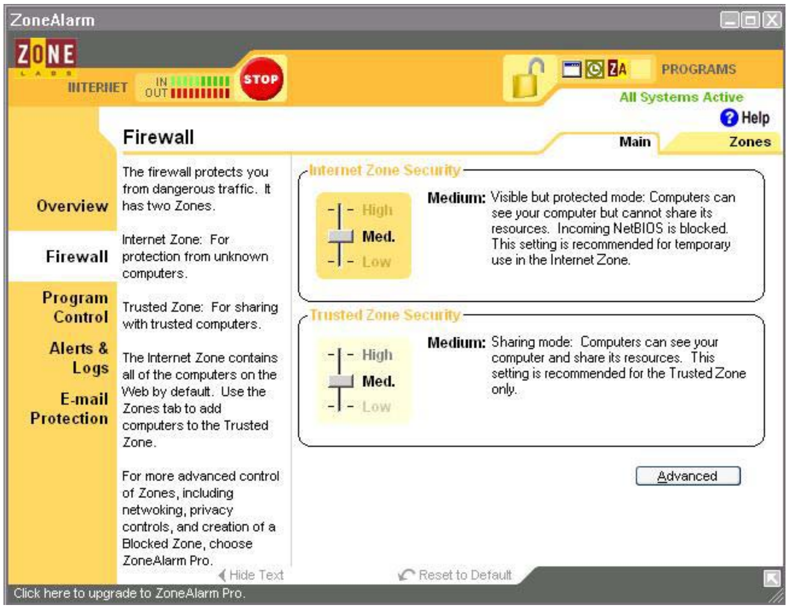
In the real world a firewall is simply a solid barrier between a vulnerable entity on one side and a hazardous entity on the other. For example, we would expect there to be a guard between a dangerous piece of machinery and it's operator. A network firewall performs exactly the same role, protecting the network inside the firewall from the outside Internet.
The simplest network 'firewall ' is, of course, not to have a network connection of any kind! This gives the best possible protection against hazardous network traffic, but unfortunately it also prevents all legitimate functionality offered by the Internet! A practical firewall must therefore allow connection, but must also have rules to enable it to distinguish 'friendly ' network traffic from 'enemy' traffic. Of course no computer can in itself truly understand the purpose behind a data packet, so most make simple decisions based on where the traffic is coming from and intended for, and what network service it appears to be requesting. A firewall might, for example, be set up to allow nothing but e-mail to pass to pass from the outside into a network, but allow both e-mail and web browser requests by internal users to pass out.
The rules that govern the firewall's handling of packets define what to do with the permitted traffic, but this leaves the question of what to do with the remainder. Firewalls can be set up either to let all undefined traffic through, a methodology known as default-permit, or block all undefined traffic, default -deny. If an event is unexpected, then it is clearly safest to assume that it is hazardous, at least until it has been investigated. Firewalls should ideally employ the 'default-deny' methodology, in order to block all traffic that they are not explicitly told to permit, as this is clearly the most secure option. Inevitably this will of course stop new, legitimate, traffic, (for example when a new service is set up to run on a network) but this conflict is much easier to resolve than the alternative of a default-permit strategy which allows the firewall to pass new, unknown traffic which later turns out to be hostile or destructive. In the event of unknown traffic being detected, the firewall can merely drop the packets, or can also, of course, log the event to permit later analysis to be carried out.

There are plenty of options regarding firewalls. It is important to remember that having a firewall should not make you complacent, nor should you rely on it as your only means of protection. However, it is an important means of protection which goes a long way to protecting your home computer against external threats. (It is a little like putting a lock on your door – it's an important first line of defence, but it is unwise to assume that it alone will foil all possible types of burglary!) A firewall protects your computer by enforcing restrictions on incoming traffic. Firewalls can also hide your computer's identity, so hackers' attempts to port scan your computer cannot return the type of information that makes intrusion easy. A firewall works by examining each data packet as it arrives to determine whether it complies with the ‘rules’ regarding what data can enter or leave your computer. When the firewall is installed, some rules are set my default, others may be added later.

‘Genuine’ packets (which are those allowed to enter or leave) are let through, whereas others are rejected. You can add an important layer of protection between your computer and the Internet by using a firewall system. Potential intruders scan computers on the Internet probing for an "open port", which they know how to exploit. A firewall can block unauthorised entry into your computer, as well as restrict outbound traffic. In addition, they can also log any intrusion attempts, such as port scans. As a general guide, I would suggest that a single attempt to access a single port (for example FTP or Telnet ports 21/23) is not suspicious, however an attempt to connect to multiple ports (for example 21,23,25,80,110,139,143) would suggest that someone is definitely a sign of someone probing for weaknesses. Where multiple ports are scanned on a number of occasions, this is a sure sign of someone trying to ‘break in’, this should be investigated.

When choosing a firewall, there are actually three types. The first, Personal (or software) firewalls are most suited for home users. They are cheap (a few can be downloaded for free!), costing around £20 sterling. Windows XP comes with a built-in firewall: the Internet Connection Firewall (ICF). Here are a few others to choose from:

Zone Labs Zone Alarm Pro (The control panel is shown below);
Symantec Norton Personal Firewall 2002;
McAfee Personal Firewall – Quite Popular;
Sygate Personal Firewall PRO;
Internet Security Systems’ Black Ice Defender - Highly spoken of;
Zero Knowledge Freedom Personal Firewall.



Firewall

The firewall protects you from dangerous traffic. It has two Zones.

Internet Zone: For protection from unknown computers.

Trusted Zone: For sharing with trusted computers.

The Internet Zone contains all of the computers on the Web by default. Use the Zones tab to add computers to the Trusted Zone.

For more advanced control of Zones, including netwoking, privacy controls, and creation of a Blocked Zone, choose ZoneAlarm Pro.

Internet Zone Security

High / Med. / Low

Medium: Visible but protected mode: Computers can see your computer but cannot share its resources. Incoming NetBIOS is blocked. This setting is recommended for temporary use in the Internet Zone.

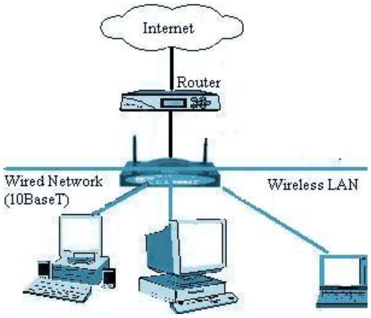
Trusted Zone Security

High / Med. / Low

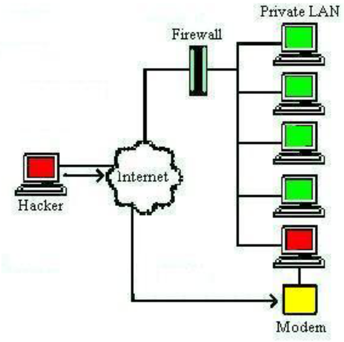
Medium: Sharing mode: Computers can see your computer and share its resources. This setting is recommended for the Trusted Zone only.

Click here to upgrade to ZoneAlarm Pro.

Hardware routers - Although not firewalls in the strictest sense, router hardware does masking your computer's IP address and port status to outsiders. They generally cost: around £50 and upwards, although you can connect more than one PC behind the router, making them a useful option for giving three or four PC's in a home network access via the same DSL or Cable Modem, using either wired or wireless networking. Many (For example the Belkin 'Gateway Router' I use on my own network) do offer a NAT firewall option, which should be used unless there is a very good reason not to do so). This is the typical configuration of one or more computers installed behind a router, and sharing a single cable modem connection to the Internet. The individual IP address of each computer on the private (home) network is concealed from the Internet; only the IP address of the router is visible to the Internet. This method allows more than one computer to use a single cable modem connection via the single IP address leased by your Internet service provider.

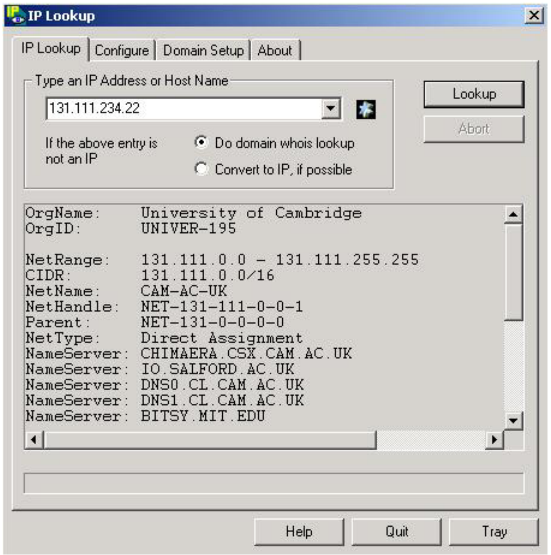


It is also possible to use a PC rather than a router, with two network cards installed; one to connect to the Internet via the cable modem, the other to connect this machine to the others in the private network. However, this method does expose the resources on this machine to the Internet, unless a firewall is installed on this machine. In addition, the use of a PC as both a router and as a workstation is very heavy on the machine concerned, particularly where it is running Windows.
Hardware firewalls cost around £250 and upward. They are also somewhat more complex to set up also, so they are not well suited to home users (they are normally used by business users having large numbers of computers behind the firewall).



An important point must be made here. If you are using a hardware firewall or router, bear in mind that if you do occasionally use a modem to dial out (for example to use any services which can only use the telephone network, such as websites which charge for usage, or when the broadband network is down) then this bypasses your hardware firewall or router. In this case, use of a software firewall is strongly recommended. (PPP stands for point-to-point protocol; this is used on dial-up connections.)

Setting up your firewall is not the end of your security worries. This is because new threats emerge all the time; for example new Trojan horses (which use different ports) will require new firewall rules to block them, in order to ensure security. It's a good idea to check for updates once a month – these can be obtained free from the vendor's website. Examine the logs from time to time, in order to find out who is trying to 'break in'. The IP address of the offending computer can be looked up, allowing you to inform the person's service provider. Most ISP's realise that it is bad for business to allow their services to be used for hacking, 'Spam mailing' and other forms of abuse which violate their acceptable use policy. You can generally complain using an email address such as abuse@serviceprovider.com - in which case, you may want to attach a copy of your firewall logs as evidence. You can obtain this information about a particular IP address using sites such as the American Registry of Internet Numbers (www.arin.net), or a 'lookup program' such as 'IPLookup' which can be obtained from http://www.softnik.com/products/iplookup/index.htm. Here is a screenshot of this in use:



Type an IP Address or Host Name: 131.111.234.22

If the above entry is not an IP

● Do domain whois lookup

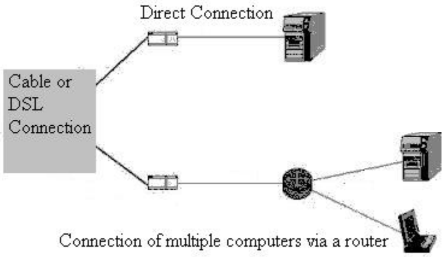
○ Convert to IP, if possible

```
OrgName:    University of Cambridge
OrgID:      UNIVER-195

NetRange:   131.111.0.0 - 131.111.255.255
CIDR:       131.111.0.0/16
NetName:    CAM-AC-UK
NetHandle:  NET-131-111-0-0-1
Parent:     NET-131-0-0-0-0
NetType:    Direct Assignment
NameServer: CHIMAERA.CSX.CAM.AC.UK
NameServer: IO.SALFORD.AC.UK
NameServer: DNS0.CL.CAM.AC.UK
NameServer: DNS1.CL.CAM.AC.UK
NameServer: BITSY.MIT.EDU
```

One important point to be made here is that more competent hackers will tend to use IP spoofing, which means faking their IP address, or else they relay their attacks via other compromised systems. This is obviously in an attempt to make the actual source of the attack difficult to trace. Another point is that some probes your firewall logs may be the result of worms or Trojan horses trying to propagate; for instance I repeatedly get a number of probes against my web server from other machines which are already compromised, probably without their owner's knowledge.

Computers that are attached to a cable modem system are, as explained previously, somewhat more susceptible to hacking because they offer a fast, 'always on' connection to the outside world. This, combined with the fact that Windows, by default, has 'file & printer sharing' enabled, makes unprotected systems into a hackers dream come true. There is also the fact that IP addresses change infrequently (if at all), which means that your computer needs only to be discovered once. You cannot easily hide your IP address from other computers. Did you know that every email you

send has this unique number contained within the header? It is very difficult to remove this; which at least makes tracing Spam mailers relatively easy.
Anyhow remember that whether you have one computer accessing the Internet directly via a cable modem, or you are using one computer as a hub for others, you need to turn off file sharing on any machine connected directly to the cable modem, or if you really do need it, then make sure you use a firewall. Remember that ports 137 through 139 are so tempting to hackers that there are a number of port scanners (such as the Legion Scanner featured earlier) which probe for nothing else. Below: configuration of a single computer connected via a cable modem (which requires a software firewall), and of multiple computers to a single cable modem via a router.



Warning! Remember that although a firewall is an important defence against hacking and intrusion; do remember that it should never be your only means of protection! Remember also that as new threats emerge all the time, for example new Trojan horses, your firewall must be updated regularly to take this into account.

Another warning regarding firewalls is necessary here:

There are a number of personal firewalls available, having a hiding mechanism which they refer to as 'stealth mode'. In stealth mode, the firewall causes the host PC just to drop incoming connection attempts to a closed port, rather than sending a negative acknowledgement to the sending machine (NAK). This is in an attempt to make it appear as though no computer exists at that IP address. It is also true that it slows down a hacker's probes - a port scanner must wait for a set time to ensure that no reply is forthcoming across the Internet.

Unfortunately, this can however cause many problems. The Internet standard (RFC 1122), which governs the operation of TCP/IP - the protocol of the Internet - has a directive regarding ICMP Echo requests (pings) used to determine whether a host is currently reachable: 'Every host MUST implement an ICMP Echo server function that receives Echo Requests and sends corresponding Echo Replies'. Now, stealth mode is in obvious violation of RFC 1122 and you may additionally experience some difficulties which include, but are not limited to, the following:

- Slow web connection in cases where the remote web server uses ICMP to determine the time delay in the network path;

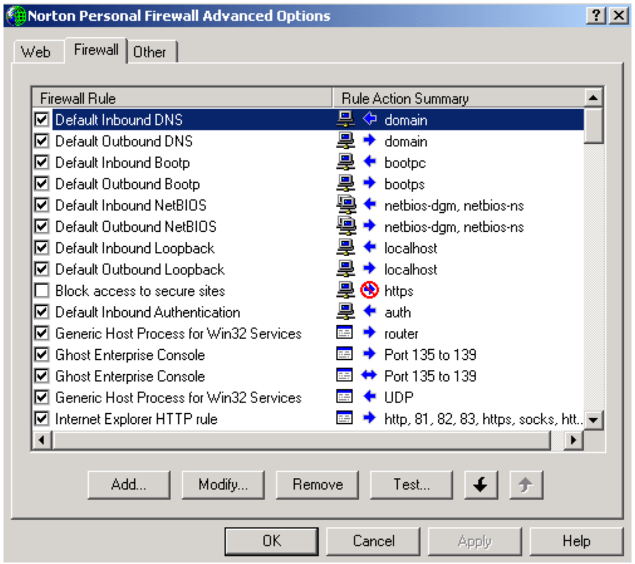
- Difficulties where technical support teams belonging to your service provider when troubleshooting connection problems, where your PC does not respond to pings or trace-routes - how do you remotely distinguish this situation from a faulty connection?;

- Some games and file sharing applications use ICMP echo requests to test the availability of hosts, as do many utilities;

- Difficulties with DHCP lease acquisition (which allows IP address allocation and/or renewal): some DHCP servers check the presence of your machine on the network, in particular where dial-up connection is used. Note that some may be fooled into thinking that your IP address is not in use, and allocate the same address to another machine - this causes an address conflict.

So you best advised not to apply stealth techniques at your firewall. For example, use the medium (rather than the high) setting in the Zone alarm control panel. Internet connection firewall (which comes with windows XP) by default blocks ICMP Echo. You should disable this rule. For other firewalls, you need to view their default settings and ensure that the option to block ICMP echo requests is cleared. This is how in Norton Personal Firewall:

Select the options tab, then ‘advanced options’. Use the ‘firewall’ tab and if a ‘default block’ option is present, highlight it, click remove. After confirmation (really remove this rule?), click apply, and exit. In my own case, I have already cleared the option.



Firewall Rule	Rule Action Summary
☑ Default Inbound DNS	← domain
☑ Default Outbound DNS	→ domain
☑ Default Inbound Bootp	← bootpc
☑ Default Outbound Bootp	→ bootps
☑ Default Inbound NetBIOS	← netbios-dgm, netbios-ns
☑ Default Outbound NetBIOS	→ netbios-dgm, netbios-ns
☑ Default Inbound Loopback	← localhost
☑ Default Outbound Loopback	→ localhost
□ Block access to secure sites	https
☑ Default Inbound Authentication	← auth
☑ Generic Host Process for Win32 Services	→ router
☑ Ghost Enterprise Console	→ Port 135 to 139
☑ Ghost Enterprise Console	↔ Port 135 to 139
☑ Generic Host Process for Win32 Services	← UDP
☑ Internet Explorer HTTP rule	→ http, 81, 82, 83, https, socks, htt..

A common objection to allowing ICMP Echo Replies is that it gives away information to hackers. There is no evidence in itself that a hacker has been aided by the presence of an ICMP Echo request. Most port scanners do not rely on ICMP echo in any way.
If you can use ‘stealth mode’ without blocking ICMP echo responses, feel free to do so. Feel free to apply stealth to all ports you do not use – except port 7, which is used to respond to echo requests. If you want to really annoy a hacker, this is an excellent method! This is because, whereas a response to an attempted connection to an ‘un-stealthed’ port is sent, indicating whether the port is open or closed, if instead *no*

response is sent at all, the port scanner is slowed down considerably as it waits in vain for a response…

15) Spyware

'Spyware' is a term used to describe illicit software placed on your PC without your knowledge or consent. It may be used for any number of purposes, ranging from recording which websites you visit (by companies trying to gain marketing information) to programs such as 'key loggers' which record every character you type, in order to be collected by the programs user later. Some programs of this type are on offer commercially for various purposes such as for parents wanting to remotely oversee their children's usage of the computer from work, for example. Many are used by employers to ensure 'appropriate' use of computing facilities (personally I do not agree with this – so never trust your boss whilst at work!). There are also many shady (Trojan horse) programs which may be placed on your system without your knowledge. These may constantly bombard you with advertisements constantly whilst you are online, or may also be secretly monitoring the software components you have installed. Even if you manage to remove these components, backups will be hidden elsewhere and the program will later be replaced. Many of these programs have no visible affect; they instead leak your personal information back to the programs owner using stealth. One program which is able to detect these is Lavasoft's ad-aware, which can be configured to run automatically after logon. It can automatically remove the offending Trojans for you. It even scans your registry for you – note that it can only remove registry keys if you are logged in as an administrator in Windows NT or 2000. It will be able to delete all files associated with malware of this kind – however take care, it has been known to inadvertently remove some necessary DLL files also.

WARNING: be careful with files such as advpack.dll and amcompat.tlb; their name suggests they are part of such a malware installation, however they are actually Windows components, which if removed, my cause Windows components to function improperly.

There are many other keystroke-logging program detectors available – 'Spycop' is one such program which is well spoken of. Another possible means to detect many such programs which are running – if you obtain a port scanner, and run a port scan on all ports 1 through 65536 on IP address 127.0.0.1 (this corresponds to 'localhost', namely the machine you are actually running it on) and noting which ports are open. Take note of which are suspicious, i.e. those which you do not recognise. A list can be found at http://www.iana.org/assignments/port-numbers, which you can check against to determine which are genuine. There should normally be no more than a handful at most – as I have already stressed, you really should not have any more open ports than you need.

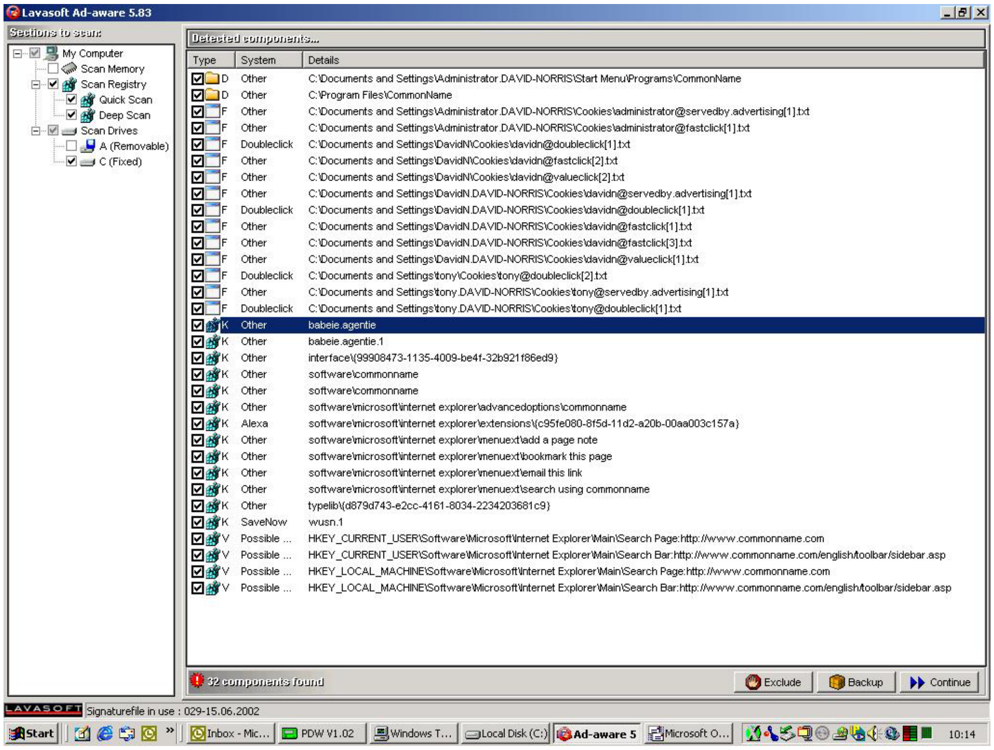
I would strongly advise that you disable cookies where possible (See earlier). Cookies are small text files which record your visits to websites. Cookies can be disabled in either Internet Explorer or Netscape Navigator, and you may also want to set-up your firewall to block them (I know that most firewalls allow you to do this). From a storage point of view alone you may wish to avoid cookies (I once discovered 1.5GB – yes gigabytes!) had accumulated over a period of several months.

Unfortunately, not all cookies are bad, they add functionality to some Web services, so as a compromise between security and convenience, at least purge them regularly. By default they are saved in c:\windows\cookies (Windows 9.X) or C:\Documents and Settings\Username\Cookies (Windows NT/2000).

There are additionally many free software applications which can locate and remove program components which have been placed on your system without either your knowledge or your consent. For example, I am sad to say that many 'freeware' programs, for example, now come with this kind of malware included, and these components can usually be removed without affecting the components you want. Now I do recognise that the software vendors need to cover development costs, however one really does not want to have their personal details sent to advertisers behind the scenes, nor does one want to be bombarded by multiple browser windows which appear faster than you can close them, whenever you run Internet Explorer, wasting bandwidth and maybe eventually even crashing your system when it runs out of memory.

One free program which scans your disk drives and registry for these components is Ad-Aware by Lavasoft. It's free to download, and can be configured to run at logon. Note that it can only remove registry keys, and scan the entire hard disk, if you are logged in as an administrator in Windows NT, 2000 or XP. If you are not logged in as an administrator, you can right-click on it's icon and use the 'run as' option to run it as though you were logged in as an administrator (you will need to know the administrator password to do this). (Bear in mind that as I have already stressed, it's not a very good idea to log in as an administrator for normal computer usage, as this leaves you open to may vulnerabilities such as Trojan horses and unauthorised use of the machine. Remember that anyone, or any program, has full-unrestricted access to the entire system whilst you are logged on as an administrator! Log in as an administrator only when you actually need administrative access).

Here is a screenshot of Ad-Aware in action. It has, somewhat astonishingly, found 32 separate components on this sweep. This just demonstrates how extreme this problem can be. (Just how much of your personal information can 32 components leek out without you even being aware?). Scan your system regularly for this kind of malware if you care about your privacy!



Type	System	Details
☑ D	Other	C:\Documents and Settings\Administrator.DAVID-NORRIS\Start Menu\Programs\CommonName
☑ D	Other	C:\Program Files\CommonName
☑ F	Other	C:\Documents and Settings\Administrator.DAVID-NORRIS\Cookies\administrator@servedby.advertising[1].txt
☑ F	Other	C:\Documents and Settings\Administrator.DAVID-NORRIS\Cookies\administrator@fastclick[1].txt
☑ F	Doubleclick	C:\Documents and Settings\DavidN\Cookies\davidn@doubleclick[1].txt
☑ F	Other	C:\Documents and Settings\DavidN\Cookies\davidn@fastclick[2].txt
☑ F	Other	C:\Documents and Settings\DavidN\Cookies\davidn@valueclick[2].txt
☑ F	Other	C:\Documents and Settings\DavidN.DAVID-NORRIS\Cookies\davidn@servedby.advertising[1].txt
☑ F	Doubleclick	C:\Documents and Settings\DavidN.DAVID-NORRIS\Cookies\davidn@doubleclick[1].txt
☑ F	Other	C:\Documents and Settings\DavidN.DAVID-NORRIS\Cookies\davidn@fastclick[1].txt
☑ F	Other	C:\Documents and Settings\DavidN.DAVID-NORRIS\Cookies\davidn@fastclick[3].txt
☑ F	Other	C:\Documents and Settings\DavidN.DAVID-NORRIS\Cookies\davidn@valueclick[1].txt
☑ F	Doubleclick	C:\Documents and Settings\tony\Cookies\tony@doubleclick[2].txt
☑ F	Other	C:\Documents and Settings\tony.DAVID-NORRIS\Cookies\tony@servedby.advertising[1].txt
☑ F	Doubleclick	C:\Documents and Settings\tony.DAVID-NORRIS\Cookies\tony@doubleclick[1].txt
☑ K	Other	babeie.agentie
☑ K	Other	babeie.agentie.1
☑ K	Other	interface\{99908473-1135-4009-be4f-32b921f86ed9}
☑ K	Other	software\commonname
☑ K	Other	software\commonname
☑ K	Other	software\microsoft\internet explorer\advancedoptions\commonname
☑ K	Alexa	software\microsoft\internet explorer\extensions\{c95fe080-8f5d-11d2-a20b-00aa003c157a}
☑ K	Other	software\microsoft\internet explorer\menuext\add a page note
☑ K	Other	software\microsoft\internet explorer\menuext\bookmark this page
☑ K	Other	software\microsoft\internet explorer\menuext\email this link
☑ K	Other	software\microsoft\internet explorer\menuext\search using commonname
☑ K	Other	typelib\{d879d743-e2cc-4161-8034-2234203681c9}
☑ K	SaveNow	wusn.1
☑ V	Possible ...	HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Search Page:http://www.commonname.com
☑ V	Possible ...	HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Search Bar:http://www.commonname.com/english/toolbar/sidebar.asp
☑ V	Possible ...	HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\Search Page:http://www.commonname.com
☑ V	Possible ...	HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\Search Bar:http://www.commonname.com/english/toolbar/sidebar.asp

32 components found

Signaturefile in use : 029-15.06.2002

16) Mobile Computing Security (Windows CE 3 and higher)

If you own a Pocket PC (Which runs Windows CE) as I do, and are wondering what security features it supports, here is a general guide. I am chiefly referring to Pocket PC 2002 (Windows CE 3.1). I cannot currently offer any specific advice for other portable computers, such as those which run the Palm Operating System.
Windows CE 3.0 does not support all of the security features of desktop Windows versions, particularly those of NT. Other than the obvious security vulnerabilities of mobile devices, such as physical theft, the Pocket PC does attempt to address some of the potential threats. This is what a Compaq Ipaq running Pocket PC 2002 (Windows CE 3.1) looks like:

On many occasions I have heard rumours of viruses for the PPC; as yet these are unfounded, although I do feel that with the PPC becoming ever more popular, it is only a matter of time before viruses do begin to appear. One thing is certain however, viruses affecting the desktop PC *cannot* affect the Pocket PC; due to the fact that the PPC does not use an Intel compatible processor; my Ipaq uses the Strongarm processor, others are the SH3, SH4 and MIPS. However, do note that any virus-infected desktop files which end up on a Pocket PC via synchronisation (Unconverted), or via inbox or other network connections *can* become active when transferred to a desktop PC!

Built-in Security Features of the Pocket PC Running PPC 2002

Passwords can be assigned under the 'settings menu'. PPC 2002 allows either a simple 4-digit number to be assigned, as in PPC 2000, or a strong alphanumeric password, which I recommend if any confidential information is stored. You can also set the Pocket PC to display the password entry screen if the device is not used for an interval ranging from 1 minute to 24 hours. There is also an option for 0 minutes which does this only when the device is first turned on. Please note that for each incorrect attempt to enter a password, you must wait for a longer and longer interval before you can retry. This is in order to discourage a 'brute force attempt' to guess the password, as on the VAX-Alpha system I once used at university. Also, if you forget your password, your only option is to perform a herd reset of your device – *caution!*

Virtual Private Networking

Your pocket PC supports connection to a VPN running on a Windows NT, or Windows 2000 server. It does not appear to support servers running other operating systems, deliberately, I shouldn't wonder? Certicom VPN (www.certicom.com) does support some additional services. The VPN service supports automatic connections to internal resources whenever the user is connected to the Internet, and they access an internal network resource. This is implemented by checking the host name. If the host name has a period (-) in it, then the request is sent to the Internet otherwise, otherwise it is instead sent over the VPN to the internal network. Therefore you cannot access the Internet via the VPN.

Website Encryption

Pocket Internet Explorer can access websites with 128-bit encryption. Unfortunately, most web sites check the version of the web browser to see if the version is 4.0 or higher. Since Pocket Internet Explorer on the Pocket PC is version 3.02, this causes most secure websites to block access to them. One solution is RegKing 2002 (www.doctorce.com/regking.htm), which allows users to change the web browser version to Internet Explorer 5.0 on Windows CE. This is not foolproof; it does work in the majority of cases.

Email Security

User authentication is provided using Secure Password Authentication (SPA) which MSN and Microsoft Exchange support. This feature allows remote users to send e-mail through a server without opening that e-mail server up to Spam mail.

Security Facilities not provided at Time of Writing

Many desktop PC applications include additional encryption support for connection via modem connections, for email services, passwords protected files (Such as Word, Excel and Access documents), and memory encryption. The Pocket PC may only have limited access to network resources.
The Pocket PC does not currently support the ability to encrypt all data sent over a modem connection, which means that the data is susceptible to packet sniffing. The 128bit high encryption pack for desktop PC's does have the ability to encrypt all data sent via a modem. There is no support provided for the Pocket PC at time of writing.
The Pocket PC does not as yet support SSL (Secure Socket Layer) encryption for email (IMAP/POP3 & SMTP). Some companies use SSL to prevent unauthorised access to the email server.
As yet the pocket PC does not encrypt files stored in 'Main memory'. However, Pocket PC 2002 does support Secure Digital (SD) cards, which allow built-in encryption of files stored on the card.
The Pocket PC does support 40 and 128 bit encryption as per the 802.11b standard. However, this is not a particularly good encryption standard.
The Pocket PC does not support encryption of individual files such as Word, and Excel documents. It does not as yet synchronise or open password protected files, as Pocket Word & Excel do not support password protection.

---

17) Content Filtering

Be Warned: It is a (relatively) well-known fact that the Internet contains material which is not suitable for minors. It has to offer a wealth of information which parents have little or no control over. However, the Internet is also an exciting recent development that is offering much useful educational content. The recent availability of non-metered, broadband access to the Internet means that children can potentially learn about the modern world at minimal cost, in an enjoyable way which, to them, is a world away from copying down words from the school blackboard. At the same time that we are providing our children with access to this valuable media, we need some means by which to protect them from stumbling across objectionable material. However, the means by which this can be accomplished is far from certain. One difficulty is that the English language alone has many words which have more than meaning when pronounced differently; take the word 'lead', as in dog walking, or lead, the metal. Also there are many words which have different meanings when used in a different context, for example the word 'bitch' is far from objectionable when used by a dog breeder, yet is more often used in a derogatory context. How is censoring software to know the difference? Take for another example the word 'breast'. To determine the questionable context of this word would require considerable diagnosis, which is extremely difficult and costly to build into a product. The simplest approach is 'keyword blocking', in which the software refers to its database for words known to cause offence. However, this simplistic approach gives rise for many ‘cases of mistaken identity’. For example, take the word ‘naked’. It is often, for example, used by astronomers in the phrase ‘the naked eye’, meaning without the use of optical aids such as telescopes or binoculars. One product I tested refused to let me view many pages belonging to the Royal Greenwich Observatory! Simply comparing the content of WebPages and other files for objectionable content is obviously overly simplistic! I have heard of at least one piece of software which does nothing more than simply hide the offending words for the viewer. Not only does this *not* filter out the images (except where their links contain offending character strings, for example in the filename), the reader has no idea that the text has been altered, sometimes completely changing the meaning of the sentence. For example, if the word ‘homosexual’ is present in the database, then the sentence “The Catholic church is opposed to all homosexual marriages" appears to the reader as, "The Catholic church is opposed to all marriages." This may appear somewhat amusing, but it represents a real problem particularly from the educational point of view! Alternatively, it may be best to remove the offending page altogether.

A more sophisticated approach is to block individual web pages by specific URLs. Typically the software vendor runs automated web crawlers to search continually for suspicious pages, which will be added to the vendor’s database. Although less flawed, there are means by which the technically competent may bypass them altogether. For example, when my university tried to ban students from accessing sites such as www.napster.com, I soon learnt that by instead entering the IP address of the respective server, I could circumvent the blockers. Before long I had a list with a number of sites complete with their IP address. In any event, the fact that the Internet is still growing exponentially raises the question of how the vendors can possibly keep pace with all the sites as they appear. Additionally, as new pages may appear all the while, it is necessary to continually update the software, as in the case of firewalls and antiviral software. This can unfortunately be rather a drawback, but as a home user, spare a thought for the school network administrator, for whom this is a far bigger administrative task!

In practice, most packages use a combination of filtering and blocking techniques, and the experienced user can choose which of these are best for their pattern of usage. It is somewhat difficult to give advice here as the individual packages differ quite considerably. You must consult the documentation which ships with the product. It is best to give the children their own login accounts (you can do this in Windows NT, 2000 or XP), so their settings can be treated separately. I would recommend doing this for other reasons also.

All things in consideration, my view is that even though the filters will never be perfect, I would say that they do go some way to giving you some peace of mind. However, it must be borne in mind that no content filter is a substitute for direct parental supervision! You can get some further safety advice regarding children’s use of the net at www.netaware.org, which is dedicated to children’s safety whilst online. Another good site is www.internetwatch.co.uk.

Here are a few general ‘common sense’ guidelines which children should *always* be made familiar with:

- Tell your children they should never give out their real names or other personal information about themselves, your family or financial details whilst using ‘chat rooms’. They might just as well give out your house keys to everyone at school.
- Instruct your children that they should never; ever arrange to meet with someone they've met online. Remember that they may not be what they make themselves out to be!
- They should *never* give away passwords for email/site logons, or user accounts on your own computer(s), even to people they know.
- Let your children know that if they run into anyone who uses abusive or foul language online, they should not respond and immediately log off. They should also be taught to inform you of any such difficulties they encounter whilst online.
- Put your computer in the living room or another communal area that the entire family uses. This makes supervision easier.
- Occasionally view the ‘history’ list to keep checks on which sites they are visiting.

---

18) Frequently Asked Questions about Safe Internet Use

Q: I’m already protected from viruses – I have an antiviral package installed. Surely I’m safe now?
A: Antivirus Protection is important. After all, home computer users are statistically the least likely to keep their antiviral software updated – and new viruses are written all the time! Remember that by permitting viruses to spread you are placing others at risk beside yourself. However, antiviral software can only provide virus protection (which as only as up to date as your virus definitions list – hence the need to update regularly). But there are other threats, such as hackers, and antiviral software alone will not help here.
Q: Surely my home computer contains no data of interest to hackers?
A: Actually, there’s likely to be plenty of information they might seek. For example, your bank account and credit card numbers, which you entered when you set up software such as Microsoft Money or purchased goods online for instance, could use to defraud you. And you may have your name, address and identity saved somewhere, along with other useful information (for example, if you have made up a CV!), which could be used to make up false passports, for example.
Q: Surely there are only a very few people with the knowledge to hack into other peoples computers?
A: Yes, this is true. However, quite a number of such people have written programs allowing anyone do become a ‘trainee hacker’. The Legion Netbios Scanner for example, which is featured in this book? If you use a search engine, you will find any number of sites offering these in abundance. Visit www.astalavista.com for example. And remember that ‘security tools’ double as ‘hacking tools’, and vice versa! Here is Astalavista’s homepage, for example:

ASTALAVISTA SECURITY GROUP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://www.astalavista.com/
Go Links
astalavista group
Home | Become a Member | Text File Archive | JavaScripts | Astalavista Directory | Tutorials Library | Trojans & Virus | Anonymity/Privacy | Downloads | Features | Art Works | Security TOOLBOX V.1.0
ASTALAVISTA MEMBER ZONE
ENTER the bright side of the underground
We guarantee highest security... from $ 3.00
Does It Take To Start A Wave?
Australia Agrees To Build Nuclear Plant - On Earthquake Fault Line
Teenager Arrested For Stealing 6-Pack Gets 10 Years in Prison
Astalavista - Worldwide underground intelligence
Underground Search
Search
[more] [The List]
Inside Astalavista
News and Updates

FEEDBACK: Hi folks, What do you think of the website, how can we improve? Your suggestions and comments are welcome. please send us some feedback Submit! Thanx for staying with us.

HOT: ASTALAVISTA.NET! Your search for answers is over! Astalavista has created the largest security archive on the net that is completely free of advertising. Our .net site rocks the security world just like the .com site rocked the underground ! Already more than 4100 active members. Webmasters join our new WEBMASTER-CASH program !

09/13/02 Clean Trash Email UnBomber - By swth
09/12/02 Port Listener Update V1.1 by Cozz
09/12/02 Date Generator
09/11/02 Packet Storm 1.3 - By Subby
09/11/02 Protecting Files/Folders in Windows.
09/09/02 UPX simple batch GUI by Benji
09/09/02 ASCII Folder Deletion - By Harshal
09/09/02 Anonymous EBomber
09/09/02 Force Trojan 1.61
09/06/02 Wireless Security & Hacking - By Dr.T
09/06/02 netbios tutorial - By TsHy
09/05/02 Spam Killer - By Hirosh

Q: Surely nobody can hack into my computer – I'm only using a dial-up (Modem) connection; and that only on occasion?

A: It is far more difficult to access somebody's computer if they use dial-up access. It's slower, so they cannot copy large amounts of data in the time you are connected. Also, finding you is harder as your IP address is different each time you are online; it's a little like trying to 'hit a moving target'. But it can be done, and what's more, small files can be copied, such as your CV which is likely to be a small <100kb document. This contains much of the information they need. And they can certainly plant a Trojan horse which will alert them of your IP address whenever you *are* online, should they want to return later for any reason! In this case, it simply doesn't matter that you only use dial-up access.

Q: If I only use the Internet to send the odd email, why would they bother with me? I'm not doing anything interesting!

A: Your computer is often less well protected than a corporate system (see below), and if you use a broadband 'always on' connection, your computer's on much of the time, and rarely checked, you may not notice anything out of the ordinary for quite some time. This makes your computer prime hacking territory.

Q: Isn't it only business or government systems that are targets for hacking?

A: It all depends on the hacker's motive. Politically motivated hackers tend to prefer government systems; disgruntled former employees wish to take their revenge on their previous employer. 'Profiteers', who wish to commit fraud, are likely to simply choose the easiest target, which is very often the home user. Remember that corporate users are likely to have invested a great deal of money and expenditure securing their networks. They usually turn out to have extensive intrusion detection systems and audit trails, as well as hardware firewalls, making them harder to successfully hack.

Q: Am I any safer as I am using an Apple Macintosh?

A: It is true that Mackintoshes are generally of less interest, they offer fewer services than PC's running either windows or Linux/Unix, however, there are doubtless some open ports available, for example if you run a server of any kind. And there are a few Mackintosh-specific hacking tools available. Furthermore, there are viruses, which cater for either PC or Macintosh systems; there are for example some macro viruses, which infect WinWord or MacWorld documents equally well. So don't be complacent!

Q: Surely doesn't my Internet service provider provide some firewall or antiviral protection for me when I'm online?

A: This is where the Internet and corporate networks are *very* different. A corporate network provides access to a relatively small number of known (and trusted) individuals. A fair degree of security normally exists between the corporate intranet and the outside Internet. The Internet, however, is free for all. ISP's rarely do provide much protection (except for their abuse department). For the most part, securing your computer is your own responsibility. Although they may, for example, provide some minimal screening for email-borne viruses, it is still a good idea to use your own anti-virus software.

---

19) Backing up the Windows Registry

This advice pertains mainly to those of you still using Windows 9.X. Note that the Windows NT registry is protected from unauthorised modification to some degree as only an administrator may modify it.

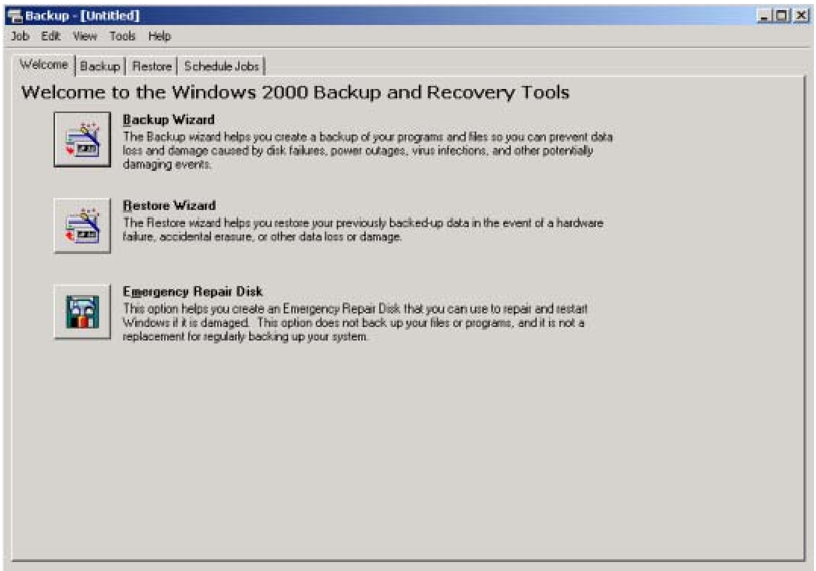
The Registry is a very important part of Windows. It is where Windows stores and manages information about hardware and software installed on your computer. Whenever you install new software or hardware, the changes are saved to the registry. This is why, in Windows NT/2000/XP, you need to be logged in as an administrator to make changes to the system registry, as the registry is protected from unauthorised modification. The registry consists of a number of files. To backup the registry, you must make safe copies of its constituent files. The following two files are the vital components of the registry; they are always present in the Windows folder (usually, C:\Windows, for Windows 95/98/ME.):
System.dat contains mostly information about the hardware configuration of the computer. User.dat contains mostly information about the software installed on the computer. In addition, if user profiles are enabled, the user-specific parts of the registry are stored in separate User.dat files, a separate file for each user. (These files are usually located in folders C:\Windows\Profiles\username.) Whenever a user logs on the system, Windows uses these to load each user's settings.

It is my advice backup the Windows' registry before making any important changes to your system -.
you can backup the Registry by making copies of the files discussed in this section. If you need to restore the Registry, replace its existing files with the copies you have saved during backup. There are many tools that can be used for this purpose. Search Windows Help or Microsoft online support web site for System Restore, Registry Checker, ERD or Emergency Repair Disk for more information on registry maintenance.

You can back up the registry with the Registry Checker tool. To run it, press the Start button on the Windows taskbar, then choose Run and enter SCANREG as the command line.
For more information about the Registry, please consult your Windows Help files.

To back up your registry in Windows NT/2000/XP:

Run the backup program (located under the start menu: Start > Programs > Accessories > System tools > Backup). You should see a dialogue box like this:



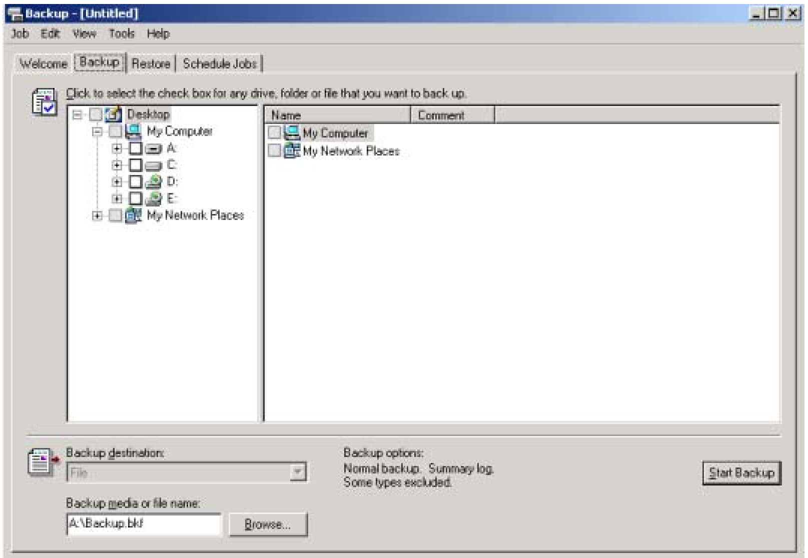
Welcome to the Windows 2000 Backup and Recovery Tools

Backup Wizard
The Backup wizard helps you create a backup of your programs and files so you can prevent data loss and damage caused by disk failures, power outages, virus infections, and other potentially damaging events.

Restore Wizard
The Restore wizard helps you restore your previously backed-up data in the event of a hardware failure, accidental erasure, or other data loss or damage.

Emergency Repair Disk
This option helps you create an Emergency Repair Disk that you can use to repair and restart Windows if it is damaged. This option does not back up your files or programs, and it is not a replacement for regularly backing up your system.

(At some point I'd also recommend creating a start-up disk, if your computer does not support booting from CD-ROM; most newer PC's do). Choose the backup wizard:



Click to select the check box for any drive, folder or file that you want to back up.

Backup destination: File

Backup media or file name: A:\Backup.bkf

Backup options:
Normal backup. Summary log.
Some types excluded.

Select the directories you wish to back up, and the 'Also back up the registry to the repair directory' option. This will allow you to repair your system should your registry or other files become corrupted. Note that your target drive will need adequate free space to store your backup! You can back up an entire hard disk to another drive of the same capacity, if you have two hard disks installed. Note: here I am referring to two physical hard disks. Remember my earlier warning about backing up to a logical drive which is part of the same physical drive! It is worse than useless, as it merely places you in a false sense of security.

20) Prepare for the Worst – Risk Management

Here are some basic methods to plan ahead for foreseeable disasters. By 'preparing for the worst', I'm implying that if you wait around long enough, you may well regret it…

- Install anti-virus software (And keep it up to date);
- Run an antiviral scan *at least* once per month
- Ensure that your system is password protected;
- Virus scan all incoming diskettes and e-mails for viruses (your software can be configured to do this automatically 'behind the scenes';
- Avoid commonly used, blank or 'obvious' passwords;
- Change your passwords as regularly as is practical;
- Give any other users of your system only as much access as they really need (In particular, never administrative privileges!)
- Regularly backup all-important data, including the Windows registry. (How often? How much are you prepared to loose if your hard disk were to fail tomorrow?);
- Keep your backups somewhere away from your computer; for example at another address;
- Verify that your backups are free of defects such as file corruption;
- Make sure that your equipment is physically safe, for example in a lockable room;
- It is best to back your important data up before hardware or software upgrades;
- Don't use software from disreputable sources (You may get 'more than you bargain for'!);
- Verify that you are suitably insured (Where appropriate);
- Don't be complacent – keep to these rules!
- Remember that adherence to these guidelines could make all the difference between minor inconvenience and significant loss or damage!

What do I do if I believe my system has <u>already</u> been compromised?

The first rule is not to panic. It is usually the case that your system has been compromised for some days, weeks, or even months before you realize it. If anything heinous were going to happen, such as your hard drive being wiped, it would probably have happened by now. It is more worrying when you consider what may have been copied from your system. If your bank details could potentially have been taken, for example, then inform your bank *without delay* – you will be liable for any losses *until* you inform the bank of the problem. If you find that your computer has been compromised, you should isolate it from the Internet immediately by disconnecting either the modem or your network cable, and contact the police where appropriate, for example if you believe that the machine has been used to aid or abet a criminal activity such as fraud. If you decide to involve the police, then do not continue to use the machine, and under no circumstances delete anything – you may remove evidence. A compromised machine may contain valuable clues to the identity of the attacker, and the data accessed. So do not delete any files or reinstall the operating system until the computer has been examined. If it is at all possible, don't even switch it off, since valuable evidence may be volatile, i.e. memory resident. Just remove the network connection immediately, and then seek expert advice.

---

21) Probe types for a particular port number – what the hacker's are looking for…

This Information attempts to provide an insight into what a hacker is probably looking for when your firewall logs a probe for a particular port. Note that there are other reasons for a firewall alert: 'normal' Internet activity, such as an incoming trace-root can sometimes appear as though someone is port scanning your system. This is why a single 'probe' for a single port number is nothing to be concerned about, however, a probe for multiple ports is a real danger signal; it gives away the fact that someone is intentionally carrying out a scan in order to discover vulnerabilities which could identify an 'open gateway' into your system. Note that this list is not exhaustive in detail, is merely attempts to de-mystify the most common probes seen in firewall logs.

Port 0: Most commonly used to help determine the operating system. This works because on some systems, port 0 is not 'valid' and will generate a different response according to the operating system's method of handling invalid port connection attempts.

Port 1: tcpmux Indicates someone searching for machines running the 'IRIX' operating system. Irix is the only major vendor that has implemented tcpmux, and it is enabled by default on Irix machines alone. No threat exists to Windows, Unix/Linux, or Macintosh machines.

Port 7: Ping (ICMP Echo); Normal activity (Usually). Used to test connectivity. May be used by service providers for troubleshooting. Ensure that your firewall allows your system to reciprocate. Recent versions of Windows/Unix should handle echo requests safely (older versions were vulnerable to DOS attacks – the 'ping of death').

Port 11: This is a UNIX service which will list all the running processes on a machine and who started them. This gives an intruder a huge amount of information that might be used to compromise the machine, such as indicating running programs with known vulnerabilities, or user accounts. Unless you are running Unix, no risk is present.

Port 19: This is a service that simply sends random data. This is for testing purposes. Can be used in a DOS (Denial of service attack).

Port 21: FTP. The most common attack you will see are hackers looking for "open anonymous" FTP servers. These are servers with directories that can be written to and read from without authentication! Hackers can use these machines for transferring such materials as 'warez' (pirated programs etc) and illegal pornography.

Port 22: Secure Shell. A more secure version of Telnet (as it encrypts passwords etc before sending them). It has some bugs which can be exploited however.

Port 23: Telnet. The intruder is looking for a remote login. Much of the time intruders scan for this port simply to find out about what operating system is being used. In addition, if the intruder finds passwords using some other technique such as packet sniffing, they will try out the passwords here. See also SSH above.

Port 25: SMTP. Mail 'Spammers' (those who send unsolicited mail, often containing objectionable material) are looking for SMTP servers that allow them to "relay"

Unsolicited Bulk Mail (Spam), from one unknown system to another. This is one of the most frequently encountered, and unpleasant, problems inherent in the Internet at time of writing. Since spammers keep getting their accounts shut down, they use dial-up connections to connect to higher bandwidth e-mail servers, and then send a single message to the relay with multiple recipient addresses. The relay then forwards the rubbish to all the victims.
Port 53: Domain Name Service. Hackers may be attempting to do carry out zone transfers (the copying of all domain names from a domain to 'map' networks for reconnaissance. Hackers are increasingly exploiting this to pierce firewalls, as many do not log DNS (port 53) access.
Port 67/68: DHCP. These machines are asking you for an address assignment from a DHCP (dynamic host connection protocol) server. You can hack into a DHCP server by specifying yourself as the local router, then carry out a wide range of 'man-in-the-middle' attacks. DHCP is set up by default on some Unix systems, even though most users don't need it.
Port 69 TFTP (Trivial file transfer protocol). Many Unix systems in particular, support this protocol in conjunction with BOOTP in order to download boot code to a diskless system (Once commonplace). However, they have successfully been miss-configured to provide any file from the host system, such as password files. They can also be used to write files to the system. If you run Unix, disable this as you probably don't need to run it.
Port 79: Finger service. Hackers are trying to discover information regarding the operating system and the users of the system. For this reason, many people shun the Finger service, hence it is less useful for legitimate purposes than it once was.
Port 80: HTTP. Hackers may be curious about a web-server you are running whether or not you do so intentionally. They may hope to discover information, or mount a denial of service attack – MS Information server in particular has a history of vulnerabilities. Disable if not needed.
Port 109: POP2 email is not nearly as popular as POP3 (POP stands for Post Office Protocol), but many servers support both (for backwards compatibility). Many of the vulnerabilities that can be exploited on POP3 can also be exploited via the POP2 port on the same server, so if you don't need POP2, don't run this server at all.
Port 110: POP3. Used by clients accessing e-mail on their servers. POP3 services have many known vulnerabilities, such as buffer overflows in the username or password exchange (meaning that hackers can break in at this stage before actually logging in). There are other buffer overflows that can be executed after successfully logging in. Also, passwords can be captured in transit via packet sniffing.
Port 113: ident. This is a protocol that runs on many machines that identifies the user of a TCP connection. Windows and in particular Unix/Linux systems may give away too much information in this way. Note that if you do stealth this port using your firewall, you may well perceive slow connections to e-mail servers on the other side of the firewall, as the mail server tries to query this information, before timing out and proceeding with the service. Many firewalls support sending back a negative acknowledgement as part of the blocking procedure, which will prevent delayed connections.
Port 119: NNTP. Network News Transfer Protocol, carries USENET traffic. This is the port used when you access newsgroups. Hackers may be hunting for open USENET servers. Most ISPs restrict access to their news servers to only their own customers. Open news servers allow posting and reading of messages from absolutely

anybody, and may be used to access newsgroups blocked by someone's ISP, to post anonymous messages, or to post Spam.
Port 135: MS RPC end-point mapper: Hackers can scan the machine on this port in order to find out things such as whether MS Exchange Server is running. Although this risk is small at time of writing, it may increase over time.
Port 137 NetBIOS name service. A very common probe. Reveals the user information, such as who is logged on and to which domain or workgroup. May also be sent by remote Windows systems, so not necessarily an attempted intrusion.
Port 139 NetBIOS File and Print Sharing. This is one of the most serious and easily exploited security risks, as mentioned in detail earlier! Some shares are unintended (as people do not realise that Windows file sharing shares their files not just to their home network, but also to the entire Internet if a directly connected machine is used as a fileserver! The Nimda worm deliberately looks for open file shares in order to propagate. Avoid using a machine used as a gateway or router as a fileserver!
Port 143 IMAP: These suffer from the same security problem as POP3, numerous IMAP servers allow buffer overflow attacks. Many servers of around 2-3 years of age (1999-2000) are vulnerable if left un-patched.
Port 161: SNMP (Simple Network Management Protocol): A very common port for intruders to probe for. SNMP allows for remote management of systems. Many vulnerabilities are known; these allow for buffer overflow attacks and unauthorised ‘management’ of your system, such as forced re-booting of your system, if left exposed to the Internet.
Port 445: NetBIOS File and Print Sharing. This is similar to port 139, only uses TCPIP alone. Some ISP’s block port 139 to safeguard their customers, however few currently block port 445. Hackers can exploit this to bypass port 139 blocking.
Port 1024 , and possibly quite a few numbers higher. This is the first port number in the dynamic range of ports. Many applications will use any dynamically assigned port for a connection, so they ask the operating system to assign the next available dynamically assigned port number. The first application on your system that requests a dynamic port may well be assigned port 1024. As more applications request dynamic ports, the operating system will assign higher port numbers in the dynamic range. For example, a web-server will move an established port 80 connection to a dynamically assigned port in order to leave port 80 free for the next HTTP connection.
Port 5632: pc Anywhere. This is a client program, which for example, allows one to access their home computer from work. Hackers may scan looking for machines running PC anywhere, so look at the source IP address to determine whether it is known to you or not!
Port 6346: Gnutella: If connections are attempted to this port, you are probably using a dial-up connection with dynamically assigned addressing. Perhaps the last user of this IP address was running Gnutella, and other Gnutella clients are attempting to re-establish the connection. Games which allow remote network play via the Internet also use higher port numbers. This is nothing to worry about.
Port 33434 – 33600: Apparent probes within this range alone may be the result of an incoming trace root. Some Unix trace root versions use ports within this range. Note that Windows trace root programs use ICMP echo (ping) only. This is not generally a threat, even if they appear alarming when first encountered.

22) Computing Security Glossary

Here is a brief description of some words, praises & abbreviations found in networking documents. These I re-ordered from notes made whilst researching the topics presented. It is not intended to be exhaustive in detail, but should help in explaining the computing jargon and phraseology which I felt unable to avoid using.

A

Active Attack
An attack which results in an unauthorised state change, such as the manipulation of files, or the adding of unauthorised files
Administrative Security
The management constraints and supplemental controls established to provide an acceptable level of protection for data.

AIS
Automated Information System - any equipment of an interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data and includes either software or hardware.
Alert
A message describing an event. The nature of the alert can be determined from event logs.
Anomaly Detection
A scheme where an intrusion is detected by looking for activity that is different from the system's normal behaviour.
Application Level Gateway
(Firewall) A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.
Assessment
Audits and Inspections; an analysis of the vulnerabilities of a system. Information acquisition and review process designed to assist a customer to determine how best to use resources to protect information in systems.
Assurance
A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy.
Attack
An attempt to bypass security measures on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the susceptibility of the computer system and the effectiveness of any existing countermeasures.

Audit

The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Audit Trail

In computer security systems, a chronological record of system resource usage. This includes user logins, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorised.

Authenticate

To establish the validity of a claimed user or computer.

Authentication

To positively verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.

Authentication Header (AH)

A field that immediately follows the IP header in an IP packet and provides authentication and integrity checking for the packet. Examined by firewalls to determine whether to accept the packet or drop it.

Automated Security Monitoring

All security features needed to provide an acceptable level of protection for hardware, software, and classified, sensitive, unclassified or critical data, material, or processes in the system.

Availability

Assuring information and communications services will be ready for use when expected.

B

Back Door

A hole in the security of a computer system deliberately left in place by designers or maintainers. Synonymous with trap door; a hidden software or hardware mechanism used to circumvent security controls.

Bomb

A general synonym for a system crash, normally through software or operating system failures.

Breach

The defeat of security controls which could result in damages. A violation of controls of a particular information system such that information assets or system components are unduly exposed.

Buffer Overflow

This happens when more data is put into a buffer or holding area than the buffer can handle. Attempted deliberately in a buffer overflow attack. This is sometimes also due to a mismatch in processing rates between the producing and consuming processes. This can result in system crashes or the creation of a back door leading to system access. This is a more serious problem in programs written in some programming languages than in others.

Bug
An unwanted and unintended property of a program or firmware, causing a malfunction.

C

C&C
Command and Control
C&C attack
Prevent effective C&C of adversary forces by denying information to or destroying the adversary C&C system.

C&C-protect
Maintain effective command and control of own forces by turning to friendly advantage or negating adversary effort to deny information to, influence, degrade, or destroy the friendly C&C system.
CGI
Common Gateway Interface - CGI is the method that Web servers use to allow interaction between servers and programs.
CGI Scripts
Allows for the creation of interactive web pages. They also tend to be the most susceptible part of a web server (besides the underlying host security).

Check_Password
A hacking program used for cracking VMS passwords.

Chernobyl Packet
Also sometimes called a Kamikaze Packet. A network packet that induces a broadcast storm and network failure. Typically an IP Ethernet packet that passes through a gateway with both source and destination Ethernet and IP address set as the respective broadcast addresses for the sub networks being gated between.
Circuit Level Gateway
One form of a firewall. Validates TCP and UDP sessions before opening a connection. Creates a handshake, and once that takes place passes everything through until the session is ended.
Compromise
An intrusion into a computer system where unauthorised disclosure, modification or destruction of sensitive information may have occurred
Computer Abuse
The wilful or negligent unauthorised activity that affects the availability, confidentiality, or integrity of computer resources. Computer abuse includes fraud, embezzlement, theft, malicious damage, unauthorised use, denial of service, and misappropriation.
Computer Fraud
Computer-related crimes involving deliberate misrepresentation or alteration of data in order to obtain something of value.

Computer Network Attack
(CNA) Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (DODD S-3600.1 of 9 Dec 96)
Computer Security
Technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of information managed by the computer system.
Computer Security Incident
Any intrusion or attempted intrusion into an automated information system (AIS). Incidents can include probes of multiple computer systems.
Computer Security Intrusion
Any event of unauthorised access or penetration to an automated information system (AIS).

Confidentiality
Assuring information will be kept secret, with access limited to appropriate persons.
COPS
Computer Oracle and Password System - A computer network monitoring system for Unix machines. Software tool for checking security on shell scripts and C programs. Warns of Weaknesses.

Countermeasures
Action, device or other measure that reduces the susceptibility of an automated information system. Countermeasures that are aimed at specific threats and vulnerabilities involve more sophisticated techniques as well as activities traditionally perceived as security.
Crack
A popular hacking tool used to decode encrypted passwords. System administrators also use Crack to assess weak passwords by novice users in order to enhance the security of the AIS.
Cracker
One who breaks security on an AIS.
Cracking
The act of breaking into a computer system.
Crash
A sudden, usually drastic failure of a computer system.
Cryptanalysis
Definition 1) The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including clear text.
Definition 2) Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.
Cryptographic Hash Function
An algorithm that computes a value (referred to as a hash word) from a particular data unit in a manner that, when a hash word is protected, manipulation of the data is detectable.
Cryptography
The art of science concerning the principles, means, and methods for rendering plain text unintelligible and for converting encrypted messages into intelligible form.

Cryptology
The science dealing with hidden, disguised, or encrypted communications.

D

DARPA
Defence Advanced Research Projects Agency.
Data Driven Attack
A form of attack that is encoded in innocuous seeming data which is executed by a user or a process to implement an attack. A data driven attack is a concern for firewalls, since it may get through the firewall in data form and launch an attack against a system behind the firewall.

Demon Dialler
A program which repeatedly calls the same telephone number. This is benign and legitimate for access to a BBS or malicious when used as a type of denial of service attack.
Denial of Service
Actions which prevent an AIS from functioning in accordance with its intended purpose.
Derf
The act of exploiting a terminal which someone else has absent minded left logged on.
DES
See Data Encryption Standard
DNS Spoofing
Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.

E

Encapsulating Security Payload (ESA)
A mechanism to provide confidentiality and integrity protection to IP packets.
Ethernet (Packet) Sniffing
This is listening with software to the Ethernet interface for packets that interest the user. When the software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like usernames or passwords.

F

False Negative
Occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behaviour.
False Positive
Occurs when the system classifies an action as anomalous (a possible intrusion) when it is in fact a legitimate action.

Fault Tolerance
The ability of a system or component to continue normal operation despite the presence of hardware or software faults.
Firewall
A system or combination of systems that enforces communication rules between two or more networks. Essentially a Gateway that limits access between networks in accordance with security rules. The typical hardware firewall is an inexpensive micro-based Unix box kept clean of critical data, with many modems and public network ports on it, but just one carefully watched connection back to the rest of the cluster.
Fork Bomb
Also known as Logic Bomb - Code that can be written to recursively spawn copies of itself, eventually crashing a host system.

H

Hacker
A person who enjoys exploring computers and how to stretch their capabilities. OR
A malicious or inquisitive meddler who attempts to discover information by poking around. A person who enjoys learning the details of programming systems and how to stretch their capabilities, as opposed to most users who prefer to learn the minimum necessary to use them.
Hacking
Unauthorised use of, or attempting to circumvent or bypass the security mechanisms of an information system or network.
Host
A single computer or workstation connected to a network
Host Based
Information, such as audit data from a single host which may be used to detect intrusions.

I

Information Assurance (IA)
Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DODD S-3600.1 of 9 Dec 96)
Information Security
The result of any system of policies and/or procedures for identifying, controlling, and protecting from unauthorised disclosure, information whose protection is authorised by executive order or statute.
Integrity
Assuring information will not be accidentally or maliciously altered or destroyed.
Intrusion
Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
Intrusion Detection
Techniques which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts

either manually or via software expert systems that operate on logs or other information available on the network.

IP Splicing

An action whereby an active, established, session is intercepted by an unauthorised user. IP splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorised user. Primary protections against IP splicing rely on encryption at the session or network layer.

IP Spoofing

An attack whereby a system attempts to impersonate another system by using it's IP network address.

K

Key

A symbol or sequence of symbols (or electrical or mechanical correlates of symbols) applied to text in order to encrypt or decrypt

Keystroke Monitoring

A specialised form of audit trail software, or a specially designed device, that records every key struck by a user and every character of the response that the AIS returns to the user.

L

LAN

Local Area Network - A computer communications system limited to no more than a few kilometres (more usually metres) and using high-speed connections (typically 10 to 100 megabits per second). A short-haul communications system that connects ADP devices in a building or group of buildings within a few square kilometres, including workstations, servers, bridges, switches, and gateways.

Leapfrog Attack

Use of userid and password information obtained illicitly from one host to compromise another host.

Letter bomb

A piece of email containing live data intended to do malicious things to the recipient's machine or terminal. Under UNIX, a letter bomb can also try to get part of its contents interpreted as a shell command to the mailer. The results of this could range from silly messages being sent to a denial of service attack.

Logic Bomb

Also known as a Fork Bomb - A resident computer program which, when executed, checks for a particular condition which triggers an unauthorised system event.

M

Mail bomb

An email sent to generate massive amounts of email to a single system or person, with the intent to crash the recipient's system. Mail bombing is regarded as a serious offence in most countries.

Malicious Code

Hardware, software, of firmware that is intentionally included in a system for an unauthorised purpose; e.g. a Trojan horse, worm or virus.

Malaria
General term for damaging, illicit programs which appear on a system without the user’s knowledge or consent.
Malware
A general term for malicious software. This covers viruses, Trojan horses and spyware, for instance.
Metric
A random variable x representing a quantitative measure accumulated over a period.
Mimicking
Also known as with Impersonation, Masquerading or Spoofing.
Misuse Detection Model
The system detects intrusions by looking for activity that corresponds to a known intrusion techniques or system vulnerabilities. Also known as Rules Based detection.
Mockingbird
A computer program or process which mimics the legitimate behaviour of a normal system feature (or other apparently useful function) but performs malicious activities once invoked by the user.
Multi-host Based Auditing
Audit data from multiple hosts may be used to detect intrusions.

N

Nak Attack
Negative Acknowledgment - A penetration technique which capitalises on a potential weakness in an operating system that does not handle asynchronous interrupts properly and thus, leaves the system in an unprotected state during such interrupts.
Network
Two or more machines interconnected for communications.
Network Level Firewall
A firewall in which traffic is examined at the network protocol(IP) packet level.
Network Security
Protection of networks and their services from unauthorised modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side effects. Network security includes providing for data integrity.
Non-Repudiation
Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

O

OSI
Open Systems Interconnection. A set of internationally accepted and openly developed standards that meet the needs of network resource administration and integrated network utility.

P

Packet
A fragment of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Packet Filter
Inspects each packet for user defined content, such as an IP address but does not track the state of sessions. This is one of the least secure types of firewall.
Packet Filtering
A feature incorporated into routers and bridges to limit the flow of information based on pre-determined communications such as source, destination, or type of service being provided by the network. Packet filters let the administrator limit protocol specific traffic to one network segment, isolate email domains, and perform many other traffic control functions.
Packet Sniffer
A device or program that monitors the data travelling between computers on a network
Passive Attack
Attack which does not result in an unauthorised state change, such as an attack that only monitors and/or records data.
Passive Threat
The threat of unauthorised disclosure of information without changing the state of the system. A type of threat that involves the interception rather than the alteration of information.
PEM (Privacy Enhanced Mail)
An IETF standard for secure electronic mail exchange.
Penetration
The successful unauthorised access to an automated system.
Penetration Signature
The description of a situation or set of conditions in which a penetration could occur or of system events which in conjunction can indicate the occurrence of a penetration in progress.
Penetration Testing
A type of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, that may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users.
Perimeter Based Security
The technique of securing a network by controlling access to all entry and exit points of the network. Usually associated with firewalls and/or packet filters.
Perpetrator
The entity from the external environment that is taken to be the cause of a risk, namely the hacker.
Personnel Security
The procedures established to ensure that all personnel who have access to any classified information have the required authorizations as well as the appropriate clearances.

Phage
A program that modifies other programs or databases in unauthorised ways; especially one that propagates a virus or Trojan horse.

PHF
Phone book file demonstration program that hackers use to gain access to a computer system and potentially read and capture password files.

PHF hack
A well-known and susceptible CGI script which does not filter out special characters (such as a new line) input by a user.

Phracker
A person who combines phone phreaking with computer hacking.

Phreak(er)
A person fascinated by the telephone system. Usually A person who uses his knowledge of the telephone system to make calls at the expense of another.

Phreaking
The art and science of cracking the telephone network.

Physical Security
The measures used to provide physical protection of resources against deliberate and accidental threats, such as fire and theft.

Piggy Back
The gaining of unauthorised access to a system via another user's legitimate connection.

Ping of Death
The use of Ping with a packet size higher than 65,507 bytes. This is an example of an invalid input which will possibly cause a buffer overflow and denial of service.

Plaintext
Unencrypted data.

Port
An arbitrary number assigned to a particular service location. An open port corresponds to a running service listening for connections from other computers.

Port Scan
A methodical means to probe for open ports, in order to determine which services are running on a target machine, and/or whether these offer an open ‘gateway’ into another Internet user’s computer.

Private Key Cryptography
An encryption methodology in which the sender and recipient use the same key, which must be kept secret. This methodology is usually only employed within small user groups.

Probe
Any effort to gather information about a machine or its users for the apparent purpose of gaining unauthorised access to the system at a later date. Port scanning is an example of probing.

Procedural Security
See Administrative Security.

Profile
Patterns of a user's activity which can detect changes in normal routines.

Promiscuous Mode
Normally an Ethernet interface reads all address information and accepts follow-on packets only destined for itself, but when the interface is in promiscuous mode, it reads all information (sniffing), regardless of its destination.
Protocol
Agreed-upon methods of communications used by computers. A specification that describes the rules and procedures that all entities making up the network should follow to perform activities on a network, such as transmitting data. If they use the same protocols, products from different vendors should be able to communicate on the same network.
Prowler
A daemon that is run periodically to seek out and erase core files, truncate administrative log files, erase lost and found directories, and otherwise clean up.
Proxy
A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it. A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.
Public Key Cryptography
Type of cryptography in which the encryption process is publicly available and unprotected, but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text.

R

Reference Monitor
A security control concept in which an abstract machine mediates accesses to objects by subjects. In principle, a reference monitor should be complete (in that it mediates every access), isolated from modification by system entities, and verifiable. A security kernel is an implementation of a reference monitor for a given hardware base.

Replicator
Any program that acts to produce copies of itself, namely a worm, a fork bomb or a virus.
Retro-Virus
A retro-virus is a virus that attempts to wait until all possible backup media are infected too, so that it is not possible to restore the system to an uninfected state.
Rexd
This Unix command is the Sun RPC server for remote program execution. This daemon is started by inetd whenever a remote execution request is made.
Risk Assessment
A study of vulnerabilities, threats, likelihood, and consequences, to access effectiveness of security measures.
Risk Management
The process to identify, control, and minimise the impact of uncertain events. The objective of the risk management program is to reduce risk and obtain and maintain DAA (Designated Approving Authority) approval.

Rootkit

A hacker tool that captures passwords and message traffic to and from a computer. A collection of tools that allows a hacker to provide a backdoor into a system, collect information on other systems on the network, mask the fact that the system is compromised, and much more. Rootkit is a classic example of Trojan Horse software. Rootkit is available for a wide range of operating systems.

Router

An interconnection device that is similar to a bridge, but serves packets or frames containing certain protocols. Routers link LANs at the network layer.

Routing Control

The application of rules during the process of routing so as to choose or avoid specific networks, links or relays.

RSA Algorithm

RSA stands for Rivest-Shamir-Aldeman. A public-key cryptographic algorithm that assumes that the factoring of the product of two large prime numbers is difficult.

Rules Based Detection

The intrusion detection system detects intrusions by looking for activity that corresponds to known intrusion techniques (signatures) or system vulnerabilities. Also known as Misuse Detection.

S

Secure Network Server

A device that acts as a gateway between a protected intranet, and the outside Internet.

Secure Shell

A completely encrypted shell connection between two machines protected by very long password.

Security

A condition that results from the establishment and maintenance of protective measures that protect against external threats.

Security Architecture

A detailed description of all elements of a system that relate to security. A security architecture describes how the system is put together to satisfy security requirements.

Security Audit

A search through a computer system for potential security problems or vulnerabilities.

Security Countermeasures

Countermeasures that are aimed at specific threats and vulnerabilities.

Security Domains

The sets of objects that any particular has the ability to access.

Security Features

The security relevant functions, mechanisms, and characteristics of AIS hardware and software.

Security Incident

Any act or event which deviates from the security rules enforced.

Security Kernel

The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept. It must mediate all accesses, be protected against modification, and be verifiable as correct.

Security Requirements
Types and levels of protection necessary for equipment, data, information, applications, and facilities.
Security Service
A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.
Security Violation
An instance in which a user or external person circumvents or defeats the controls of a system to obtain unauthorised access to information contained.

Server
A system that provides network service such as disk storage and file transfer, or a program that provides such a service. A kind of daemon which performs a service for the requester, which often runs on a computer other than the one which the server runs.
Sniffer
A program to capture data across a network. Used by hackers to capture usernames and passwords. Is also used legitimately by network operations and maintenance personnel to troubleshoot network problems.
Spam
To crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.
Spoofing
Pretending to be someone else. Attempting to gain access to an AIS by pretending to be an authorised user. Impersonating, masquerading, and mimicking are forms of spoofing.
SSL (Secure Sockets Layer)
A session layer protocol that provides authentication and confidentiality to applications.
Subversion
Occurs when an intruder modifies the operation of the intrusion detector to force false negatives to occur.
SYN Flood
When the SYN queue is flooded, no new connection can be opened.

T

TCP/IP
Transmission Control Protocol/Internetwork Protocol. The suite of protocols the Internet is based on.
Tcpwrapper
A software tool for security which provides additional network logging, and restricts service access to authorised hosts by service.
Term Rule-Based Security Policy
A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

Terminal Hijacking
Allows an attacker, on a certain machine, to control any terminal session that is in progress. An attack hacker can send and receive terminal I/O data while a user is on the terminal.
Threat
The means through which the ability or intent of a threat agent to adversely affect a system can be perpetrated. A potential violation of security.
Threat Agent
Methods and things used to exploit a susceptibility in an information system, operation, or facility; fire, natural disaster and so forth.
Threat Assessment
Process of formally evaluating the degree of threat to a system and description of the nature of the threat.
Topology
The physical map or plan of the network.
Trace Packet
In a packet-switching network, a unique packet that causes a report of each stage of its progress to be sent to the network control centre from each visited system element.
Traceroute
An operation of sending trace packets for determining information; traces the route of UDP packets for the local host to a remote host. Normally traceroute displays the time and location of the route taken to reach its destination computer.
Trojan Horse
An apparently useful and innocent program containing additional hidden code which allows the unauthorised collection, exploitation, falsification, or destruction of data.
TTY Watcher
A hacker tool that allows hackers with even a small amount of skill to hijack terminals. It usually has a graphical user interface.

V

Vaccines
Program that injects itself into an executable program to perform a signature check and warns if there have been any changes, such as through virus infection.
Virus
A program that can "infect" other programs by modifying them to include a possibly evolved, fully functional copy of itself.
Vulnerability
Hardware, firmware, or software flaw that leaves an AIS open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorised access to information or disrupt critical processing.
Susceptibility Analysis
Systematic examination of an AIS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

W

WAIS

Wide Area Information Service - An Internet service that allows you to search a large number of specially indexed databases.

WAN

Wide Area Network. A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks.

War Dialler

A program that dials a given list or range of numbers and records those which answer with handshake tones, which might be entry points to computer systems.

Worm

Independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads.