Trinidad and Tobago Computer Society

Internet Security and Online privacy

version 2.1

October 2000

COPYRIGHT

LICENCE AGREEMENT

ACKNOWLEDGEMENTS

Trademarks: All terms mentioned in this document that are known to be trademarks or service marks are hereby acknowledged. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

References to companies/individuals and their products/services in this document are for information purposes only. They are not and should not be considered an endorsement or validation of the services and / or products offered by any of these companies or individuals.

DISCLAIMER

While every effort has been made to ensure the technical accuracy of the information contained in this document, **readers use it at their own risk**.

The author(s) and/ or the TTCS are **NOT** liable for any damages whatsoever (including without limitation, direct or indirect damages for personal injury, loss of business profits, business interruptions, loss of business information or other financial loss) arising from the use of, or inability to use, the information contained within this document.

Information in this document is subject to change without further notice.

TTCS contact information:

TTCS Website: http://www.ttcsweb.org

TTCS E-mail: ttcs@opus.co.tt

TTCS Postal Mail: P.O. Box 1211, Port of Spain, Trinidad, West Indies.

Table of Contents

Introduction

The previous edition of this document, Version 1.2 (released June 2000) was concerned with informing the home and small business user about how to secure their Internet access against intrusion by such malicious software as trojan horses, viruses and hostile scripts (aka “malware”). Research has shown that many Internet “technologies” are both a security and privacy threat to the home and small business user, as a result several additions have been made to the information contained in this document.

The present threat to Internet users is a combination of the old (e.g. trojans, viruses, hostile scripts) and the new (e.g. web bugs, confidential data being stored in plain-text cookies, unique identification numbers, ad-ware/spyware and unauthorised transmission of the user’s personal data). Most of the problems orginate in the methods by which online advertising companies (see Appendix E for a list of these companies) track and store data about Net surfers in order to compile statistics for more “effective” advertising. They claim it is to make the WWW a better place for everyone but so far they have only caused un-necessary worries for all Net users.

This document will seek to explain some of these problems and where possible, provide solutions. It is important to note that this document is about *informing* users about potential Internet threats. Everyone who uses the Internet is subject to their influence in one form or the other; the chances of being victimised by these “technologies” and “malware” are directly related to user awareness of their existance.

If you aware of their existance you can avoid being a victim!

Chapter 01: The Handout

Introduction

There are a variety of issues concerning Internet computer security for home and business users:

- Traditional viruses;
- Macro viruses which infect data;
- E-mail that contain viruses either as attachments or hostile scripts;
- Trojan horse programs that "phone home" with critical/confidential information or which allow un-authorised access to your computer;
- "Spyware" programs which: track your Internet travel and system contents without your knowledge; which may allow "spyware" companies to secretly install software on your machine without your knowledge; which track which files you download and the source of the download.
- Improper file and printer sharing settings in Windows 9.x networking.

Counter-measures

Traditional and Macro Viruses

- Update your anti-virus software as often as possible.
- Scan **ALL** files (executables, compressed files **AND** data!) from **ALL** sources **BEFORE** use.
- Avoid distributing known "infected" programs.
- Keep informed of the latest viruses and virus hoaxes.

E-mail Viruses:

- Be suspicious of **ALL** e-mail with unusual or blank subject lines from **ALL** sources.
- Delete **ALL** attachments from unknown sources! **NEVER** let curiosity get the better of you!
- **NEVER** forward copies of infected e-mail to friends, family, your e-mail address at work etc.
- **NEVER** forward copies of any sort of "spam" virus warnings to friends, family, work etc.
- If you have no choice but to accept attachments from strangers, scan **ALL** file attachments (executables, compressed files **AND** data!) from **ALL** sources with up to date, anti-viral software **BEFORE** using them.
- Do not use e-mail clients with known security flaws. NOTE: Using a different e-mail client is NOT a 100 percent guarantee against infection; virus creators can always create new viruses that exploit previously unknown loopholes in these alternative e-mail clients.
- Install the latest security patches to fix the security loopholes in your email client(s).
- Switch OFF all types of scripting (e.g. Java, Javascript, Active X) when ever possible.
- Use the ADD/REMOVE applet in Control Panel to UN-INSTALL the Windows Scripting Host in Windows 98.
- As an alternative, use a NON-WINDOWS based e-mail client.
- Use firewall technology to block the malicious scripts.
- Keep informed of the latest virus threats.

Trojans:

- Scan your downloads with up to date anti-virus software.
- Install and configure firewall software.
- Monitor your firewall logs for evidence of trojans "phoning home".
- Monitor your firewall logs for evidence of un-authorised access to your system.
- Avoid using, storing or distributing known "infected" programs.
- Keep informed of news related to trojans and their variants.

Spyware:

- Avoid using advertising sponsored software aka "adware" or other known "spyware".
- Install and configure firewall software.
- Monitor your firewall logs for evidence of spyware "phoning home".
- Monitor your firewall logs for evidence of unauthorised access to your system.
- Avoid using, storing or distributing known “spyware” programs.
- Keep informed of news related to spyware and adware.

Win 9.x file and printer sharing:

(Note: these tips apply to stand-alone machines which are used to access the Internet).

- "unbind" the Client for Microsoft Networks in Windows 95 networking and then un-install the service Client for Microsoft Networks (if you using a stand alone computer).
- Use only the networking components essential for Internet access.
- Probe/test your machine's ports for security loopholes at the Shields up website (http://grc.com).
- Install and configure firewall software.
- Monitor your firewall logs for evidence of scans and probes or access to your hard drive.
- Keep informed of news related to file and printer sharing loopholes.

Conclusion

The Internet has increased the channels by which your machine can be attacked and the danger presented by these security threats is directly proportional to:

- the value and sensitivity of the information on your computer

- the importance of your system to your life and livelihood.

The best defense against these cyber threats is **information**. Once you know what to expect, you can take relevant steps to avoid being a victim. Remember:

PREVENTION IS BETTER THAN CURE!!

Chapter 02: The Web Bug Menace

Web bugs are 1-pixel, transparent GIF files that are used to “help” Web sites and advertisers track Internet surfing habits. They are invisible to the human eye and can be placed anywhere on a web page.

The “bugs” are a widely used, virtually undetectable means of tracking Internet surfing habits similar in nature and function to the infamous “cookie”. Many Internet surfers are aware of the issues concerning cookies and their use as tracking devices so they usually switch off this service for improved speed and security. However, unlike cookies, web bugs cannot be seen on web pages, anti-cookie filters can not block them, firewalls do not block them and many web sites who use web bugs do not mention in their privacy statements/inform surfers that the site uses web bugs.

NOTE: Web bugs can track Net surfers even if the site does not have banner ads.
NOTE: **any** image format supported by a browser can be used as a web bug.

Web bugs can cross-reference information with existing cookies on a computer if they (the bug and the cookie) originated from the same site or advertising company. They can send the following information to the server

- The IP address of the computer that fetched the bug
- The URL of the page that “hosts” the bug
- The URL of the bug image
- The time the bug was viewed
- The type of browser that fetched the bug image
- A previously set cookie value

The bugs can also be used in email; e.g. spammers can send a bulk email newsletter containing HTML formatting, as well as web bugs which would allow the sender to determine how many people read the letter, how often they read it and if they forwarded it to anyone.

So, why are web bugs used in the first place? Here is a relevant quote from the chief privacy officer at DoubleClick (the dominant online advertiser/user of tracking technology):

QUOTE:

"Using traffic-log cookies or clear gifs is a way for advertisers to learn whether they're getting the most bang for their advertising dollar," said Jules Polonetsky, chief privacy officer at DoubleClick. "It's a tool that does not provide any personal information but allows the Web site to learn how users are visiting different areas of their site and learn which ads brought them to their site”.

END QUOTE

Comment: The advertising companies claim that cookies and other methods of tracking surfers e.g. web bugs, are useful to both consumers and Web sites. Given the potential for abuse of the information they collect, the companies have consistently said the information collected is kept

private and is the sole property of the company that is being advertised. The problem arises by the fact that “**the information … is the sole property of the company that is being advertised**”. Recently there have been cases where cash-strapped “dot.com” companies have resorted to selling or leasing their customer information (their “property”) to third parties (e.g. spammers, junk mailers, telemarketers) in an effort to raise cash. Some other companies have drastically altered their online privacy statements to allow such activity. (A good example of such behaviour was recently provided by Amazon.com). In other words, consumers have absolutely no guarentee that their personally identifiable data will not be abused in any way. It is a matter of trust and none of the online advertising/tracking companies have given Internet users any real reason to trust them.
End comment

The story does not end with Internet browsing, according to an August 2000 article written by Richard M. Smith, Chief Technology Officer of the Privacy Foundation, web bugs can be embedded in Microsoft Word, Excel 2000 and PowerPoint 2000 documents thus allowing the author to track the document . MS Word documents have the ability to link to an image file that is located on a remote Web server. Only the URL of the bug is contained in the document therefore Word has to obtain the image from the remote server every time the document is opened. This “linking” feature allows the remote server to monitor when and where a document file is being opened. The server would be able to record the IP address and host name of the computer that has opened the document. Web bugs in Word documents can also read and write cookies belonging to Microsoft’s Internet Explorer browser.

The following quote from the article provides a more detailed description:

QUOTE:

Microsoft Word from the beginning has supported the ability to include picture files in Word documents. Originally the picture files would reside on the local hard drive and then be copied into a document as part of Word .DOC file. However, begining with Word97, Microsoft provided the ability to copy images from the Internet. All that is required to use this feature is to know the URL (Web address) of the image. Besides copying the Web image into the document, Word also allows the Web image to be linked to the document via its URL. Linking to the image results in smaller Word document files because only a URL needs to be stored in the file instead of the entire image. When a document contains a linked Web image, Word will automatically fetch the image each time the document is opened. This is necessary to display the image on the screen or to print it out as part of the document. Because a linked Web image must be fetched from a remote Web server, the server is in a position to track when a Word document is opened and possibly by whom. Furthermore, it is possible to include an image in a Word document solely for the purpose of tracking. Such an image is called a Web Bug. Web bugs today are already used extensively by Internet marketing companies on Web pages and embedded in HTML email messages. When a Web bug is embedded in a Word document, the following information is sent to the remote Web server when the document containing the bug is opened:

- The full URL of the Web bug image
- The IP address and the host name of the computer requesting the bug

- A Web browser cookie (optional)

This information is typically saved in an ordinary log file by Web server software.Because the author of the document has control of the URL of the document, they can put whatever information they choose in this URL. For example, a URL might contain a unique document ID number or the name of the person to whom the document was orginally sent. These tracking abilities might be used in any number of ways. In most cases, the reader of a particular document will not know that the document is bugged, or that the Web bug is surreptitiously sending identifying information back through the Internet. One example of this tracking ability is to monitor the path of a confidential document, either within or beyond a company's computer network. The confidential document could be "bugged" to "phone home" each time it is opened. If the company's Web server ever recevied a "server hit" from an IP address for the bug outside the organization, then it could learn immediately about the leak. Because the server log would include the host name of the computer where the document was opened, a company could know that the organization that received the leaked document was a competitor or media outlet. All original copies of a confidential document could also be numbered so that a company could track the source of a leak. A unique serial number could be encoded in the query string of the Web bug URL. If the document is leaked, the server hit for the Webbug will indicate which copy was leaked. A serial number could be added to a Web bug in a document either manually — right before a copy of a document is saved — or automatically through a simple utility program. The utility program would scan a document for the Web bug URL and add a serial number in the query string. A Perl script of less than 20 lines of code could easily be written to do this sort of serialization. Another use of Web bugs in Word documents is to detect copyright infringement. For example, a publishing company could "bug" all outgoing copies of its newsletter. The Web bugs in a newsletter could contain unique customer ID numbers to detect how widely an individual newsletter is copied and distributed. A third possible use of Web bugs is for market research purposes. For example, a company could place Web bugs in a press release distributed as a Word document. The server log hits for the Web bugs would then tell the company what organizations have actually viewed the press release. The company could also observe how a press release is passed along within an organization, or to other organizations. In an academic setting, Web bugs might be used to detect plagiarism. A document could be bugged before it is distributed.An invisible Web bug could be placed within each paragraph in the document. If text were to be cut and pasted from the document, it is likely that a Web bug would be picked up also and copied into the new document To place a Web bug in a Word document is relatively simple. These are the steps in Word 2000:

1. Select the Insert | Picture | From File... menu command

2. Type in the URL of the Web Bug in the "File Name" field of the Insert Picture dialog box.

3. Select the "Link to File" option of the "Insert" button.

Access to the sender's server logs is required to monitor the movement of such Web bugs.

The Privacy Foundation ran simple experiments with Excel and PowerPoint files and found that these files can also be "bugged" in Office 2000. The Privacy Foundation continues to investigate this issue with regard to other software programs. The Privacy Foundation has set up a demonstration of a Web bug in a Word document. The demo document can be downloaded from the University of Denver Privacy Center Web site at this URL: http://www.privacycenter.du.edu/demos/bugged.doc

The document contains a visible Web bug. When the document is opened, the Web bug will show the host name of the computer that fetched the image. In addtion, a non-identifying Web browser cookie will be set on your computer. The cookie is non-identifying because everyone gets the same cookie value, which is simple test string. Demonstrations of "bugged" Excel and PowerPoint files are alsoavailable for download from the Privacy Center Web site:

http://www.privacycenter.du.edu/demos/bugged.xls
http://www.privacycenter.du.edu/demos/bugged.ppt

The use of Web bugs in Word does point to a more general problem. Any file format that supports automatic linking to Web pages or images could lead to the same problem. Software engineers should take this privacy issue into consideration when designing new file formats. This issue is potentially critical for music file formats such as MP3 files where piracy concerns are high. For example, it is easy to imagine an extended MP3 file format that supports embedded HTML for showing song credits, cover artwork, lyrics, and so on. The embedded HTML with embedded Web bugs could also be used to track how many times a song is played and by which computer, identified by its IP address.

END QUOTE

Solutions to blocking the “Word bug”

- Cookies should be disabled any time the Internet Explorer browser is called by applications such as Word, Excel, Powerpoint or Outlook.

- Personal firewall software such as ZoneAlarm can monitor your Internet connection and will warn you if a program attempts to access the Internet without your permisssion. If any of the non-Internet related MS Office Applications (e.g. Word, Excel, Powerpoint) attempt to access the Internet because of an embedded “bug”, ZoneAlarm can trap it.

Chapter 03: Netscape's Java Security Hole

This flaw is present in versions of Netscape running under Windows 95, 98, 2000 and Linux.

Note: the problem is fixed in version 4.75 and higher of the browser.

There is a security hole in Netscape's Java implementation, that could exposes the contents of machine's local hard drive to the Internet while the user is web surfing.

The security vulnerability takes advantage of a hole in the Java Virtual Machine used by Netscape browsers and could allow a malicious web site operator to turn the browser into a web server style applicaion **without the user's knowledge.** Once activated, this "web server" allows the malicious operator to view and download any file from the victim's local hard disk. At this time the malicious operator cannot modify or delete any of the victim's files. In Linux, the security flaw can only function if the victim is logged in as "root" while surfing the Internet.

NOTE: The Java security model is designed to protect the end user from such an attack. It places programs in a "sandbox" which prohibits the Java program from doing anything outside the boundaries of the "sandbox". This includes: reading or writing to local disks, making a network connection to any machine other than the host which provided the applet, etc.

The only protection from this security vulnerability is to disable the Java Virtual Machine.

How to disable Java

- Start Netscape Communicator.
- Select Edit,
- Select Preferences
- Select Advanced.
- Un-check "Enable Java"
- Un-check "Enable Java Script".
- Click "Apply".

Chapter 04: Generic spyware

A defination of spyware courtesy of Steve Gibson’s web site:

> Silent background use of an Internet "backchannel" connection MUST BE PRECEDED by a complete and truthful disclosure of proposed backchannel usage, followed by the receipt of explicit, informed, consent for such use.
>
> ANY SOFTWARE communicating across the Internet absent these elements is guilty of information theft and is properly and rightfully termed: Spyware.

The term “spyware” and the term “ad-ware” have is often considered one and the same but there is a difference between the two. Ad-ware is the term used to describe “advertiser sponsored software” whereas “spyware” is defined as **any** software that secretly uses an Internet connection to communicate with an undisclosed third party (note that adware can be spyware but not all spyware is adware!).

The concept of adware is simple: software authors can create high-quality, fully functional software (that is, no disabled features, no expiry date) and release it to the public for “free” (no registration fees, no purchase necessary) because they receive compensation (i.e. get paid) via the advertising support built into the program.

An adware program uses your Internet connection to download and store advertisments on your machine. These advertisments are then displayed when you run the host program. While the adware is online, it reports which advertisments have been displayed on your machine as well as which advertisments have been used (i.e. have you surfed over to the web site associated with the advertisment?) to the ”home base” server. The data is used to target the advertisments specifically to you. The spyware issue arose from the fact that in the “old days” (as little as one year ago) the majority of adware programs did not inform the user that they were indeed adware at anytime during the installation process or during regular use (only a few disclosed their true nature but only after they were already up and running on the host system). Then there were the technical problems: uninstalling the host application or registering the host application (to remove/disable the adware features) did not remove the adware components (i.e. DLLs, executables), or the related entries and settings in the system registry. Adware use of Internet connections was found to be responsible for operating system instablity and unexplained browser crashes. The situation was only made worse by the advertising/marketing companies (See Appendix E for a list of the more prominent companies). When approached for information, most denied their products were responsible for any sort of computer problems and refused to provide details on how they were collecting their demographic data, what specific data they were collecting and what use was being made of that data.

The term spyware was coined to describe this type of software because all of this activity was taking place without user knowledge. Even in cases where the software identified itself as “adware” most users did not know exactly what was going on with the adware evertime they went online.

We recommend that readers consult Steve Gibson’s website at: http://grc.com for further information/details on the subject of spyware and their related dangers.

Chapter 05: NetZip-based file-downloader spyware

This chapter is concerned with the following programs:

- Real Networks RealDownload,
- Netscape/AOL Smart Download
- NetZip Download Demon

The problem with these three programs is as follows:

QUOTE:

EVERY TIME you use one of these utilities to download ANY FILE from ANYWHERE on the Internet, the complete "URL address" of the file, along with a UNIQUE ID TAG that has been assigned to YOUR machine, and — in the case of Netscape's SmartDownload only — YOUR computer's individual Internet IP address, is immediately transmitted to the program's publisher.

END QUOTE

If you have old versions of these programs (i.e. if they were downloaded before August 2000) and are concerned with your online privacy, uninstall them and delete all copies immediately!

Important note: the Netscape browser's "Smart Update" feature is NOT related to the "Smart Download" program.

Note: according to Steve Gibson's website, as of late July 2000, Real Networks has indeed removed the "spyware" capabilities of the "Real Networks RealDownload " manager, thus the latest versions are supposedly "safe". However, as of this writing, there has been no official word from AOL or Netzip about what steps (if any) they have taken to de-toxify the spyware capablity of *their* download managers

This document is too small to accomadate the technical information required to assist readers with understanding the problems and implications of this new breed of spyware. We recommend that readers **consult Steve Gibson's website at: http://grc.com for further information on the subject of this and other spyware and their related dangers .**

Chapter 06: Anti-spyware software and techniques

The concept of having your Internet activities monitored without your knowledge by some anonymous tracking software for vaguely defined reasons can be overwhelming, however, there is hope and help for Internet users who which to regain control of their online time. As stated in the handout:

- Avoid using advertising sponsored software aka "adware" or progams known to be "spyware".
- Install and configure firewall software.
- Monitor your firewall logs for evidence of spyware "phoning home".
- Monitor your firewall logs for evidence of unauthorised access to your system.
- Avoid using, storing or distributing known “spyware” programs.
- Keep informed of news related to spyware and adware.

This is a basic approach to securing your system; the firewall can block the spyware or adware from "phoning home" and it can block external servers/users from making connections to software that is resident on your system however it does not remove the offending software, it components or its settings in the registry. A more technical approach is needed to completely rid your system of the spyware/adware.

The first step would to verify that the program is indeed spyware (See Appendix D for a list of some spyware).Within recent times, the online marketers have yielded to public pressure and are now including built-in utilities to remove the various components of their tracking software. The second step would be to use this utility (note: if the spyware replaced or altered system files or DLLs, the un-installer and other software will most likely NOT undo the damage). Aureate/Radiate has a utility available to remove its DLLs from a system. If the un-installer does not work properly or the tracking software does not have un-install capability or the un-installer has left residual files, you need to use a third party utility such as Opout (produced by Steve Gibson, available at http://grc.com, effective only against Aureate/Radiate related spyware) or the more powerful Ad-aware (freeware produced by Lavasoft at: www.lavasoft.de, which is effective against most of the current spyware).

If you are still experiancing problems or suspect an unlisted piece of software to be spyware; you can use the following software for a more in-depth analysis of your system:

DLLView: provides a list of: which DLLs have been loaded, all active processes, as well as the base, size, version information, complete path, and a time/date stamp for each DLL.

Regmon: monitors and displays all registry-related activity on a Win 9.x system.

TDImon: monitors TCP and UDP activity on the local system. It can be used for analyzing application network usage.

All software mentioned in this Chapter:

- ♦ Ad-Aware (check www.lavasoft.de for the latest version)

- Aureate DLL Uninstaller
- DLLView
- Opout (available only at http://grc.com)
- Regmon
- TDImon
- ZoneAlarm

is either freeware or at least free for personal use and can be downloaded from the ZDNET software library at:

http://www.hotfiles.com

Lists of known spyware can be found at:

www.lavasoft.de

http://www.infoforce.qc.ca/spyware

Most of the reputable download sites now place Ad-ware in a category separate from shareware and freeware.

A word of caution

Manually un-installing the advertising related components of an advertiser sponsored program maybe the only way to rid your system of security/privacy vulnerabilities but removing those components may cause the host program to either cease functioning or to crash while in use.

A thorough cleansing of your system may require editing the Registry.

Proceed with extreme caution! .

The Windows 9.x system registry is an essential component of the operating system. Any errors in this file can cause system crashes or even render the system unable to boot. Manual editing of the Registry is NOT recommended for in-experianced users.

If the spyware replaced or altered system files or DLLs, you may need to conduct a fresh installation of your operating system to ensure that the appropriate versions and components are properly re-installed. Remember to back up all essential data, passwords, dial-up settings etc **before** the actual re-install.

Conclusion: Why should I care?

Having read the previous material, you may be asking yourself: why should I care? After all, my anti-virus software is up-to-date and claims that my machine is not infected and the online advertisers/marketers claim they are only trying to make the World Wide Web a better place for everyone. It all appears harmless enough and if a little demographic data can help keep the Internet free, then it is an acceptable compromise.

You have no choice but to be concerned with what is happening because it is taking place without your knowledge! In addition to the privacy and security concerns created by this "malware" (e.g. trojans, viruses, spyware), there is the fact that most of them also hog your system resources and can cause operating-system and browser instability and crashes. People who use dial-up services to connect to the Internet will be particularly hard hit since the trojans/ad-ware/spyware waste precious online time to retrieve advertisments and report to "home base". Remember **you** are paying for the online time and other people have technically hijacked it for their own use.

Yes advertising helps to sponsor Internet content but why do advertisers/marketers require such detailed information about users? Then there are the methods by which the demographic data is collected. Not too long ago, (as little as one year ago) few people knew of the existance of the technology (e.g. web bugs, spyware) used by advertisers to track users movement on the Internet. Once you had cookies and scripting languages switched off you were supposed to be safe. That is no longer the case. They (advertisers/marketers) have now implemented technologies that circumvent these safeguards in order to continue tracking your movements and collecting informaton about you. You are nothing more than a block of data in an online database just waiting to be sold to the highest bidder. It is bad enough that they collect the data "behind your back" but there have been cases when confidential/personally identifiable data has been transmitted to "home base" in plain text! In other words it could have easily been intercepted and read by third parties. There have even been cases where credit card numbers were transmitted as plain text.

In the real world, you would be extremely un-comfortable, perhaps even frightened if you were constantly followed by unknown people who recorded everthing you said and did; you would not appreciate other people eavsdropping or generally being inquisitive about your personal matters; you would take every possible precaution to ensure that your personal/confidential data does not fall into the wrong hands; you would be angry if, someone sold information about you to advertisers and then you were bombarded with junk mail and telemarketing calls trying to sell you products you neither need nor requested.

So why do you accept it when you connect to the Internet?

At the moment, these tracking technologies and the data they collect are being publicly used by online advertisers and marketers whose stated claim is to be more effective and efficient with advertising thus maximising the advertising expenditure of their clients.

The issue is not so much the technology, **but rather how the technology and the data it collects, is used and by whom**.

It is not difficult to envision a scenario whereby governmental authorities or unscrupulous businesses implement such technology for their personal "profit" at the (financial) expense of the average user and perhaps even at the expense of basic civil and human rights.

Appendix A: What is a firewall?

A firewall is a piece of computer software or hardware (Note: it can also be a combination of both hardware and software) that is designed to defend a private network (or stand-alone computer) against unauthorised access. The most common application for firewalls are to defend confidential Internet databases and "member-only" areas on Internet sites. The basic mission of a firewalls is to screen incoming (most common use) or outgoing messages (especially if the data/email originates on a corporate network) to ensure that the data conforms to specfied security criteria in order to prevent the intake of "malware" or loss of confidential information.

Firewalls use some or all of the following techniques:

Packet Filter: The firewall examines each packet entering or leaving the network and accepts or rejects the packet based on rules established by the system administrator. Packet filtering is effecient and most importantly, transparent to users. Note: it is vulnerable to Denial of Service (DoS) attacks.

Application Gateway: This technique is used for allow or deny access by specific applications. It is commonly used to block unauthorised FTP and Telnet access to corporate networks.

Circuit-Level Gateway: The firewall is used verify a connection that uses a specific protocol (e.g. TCP/IP or even UDP). Once a connection has been established and verified, data packets can be transferred over the client/server connection without need for further verification.

Proxy Server: This technique is used to intercept **all** messages entering and leaving the network. The messages are then checked before being forwarded to their respective recipients. The proxy server is the only point of contact with the external world and hides the network address. Thus if there was an attempt to break into the network, the attacker would only be able to access the proxy.

Firewalls can also employ additional techniques such as encrytion, packet sniffing and IP tracing to further enhance the security of the protected network.

Appendix B: What are TCP/IP ports?

A TCP/IP "port" refers to any one of the 65,535 possible addresses that a computer, running TCP/IP software, can use to communicate with the outside world. Each address (port number), has the potential to allow outsiders to access your system. There are internationally accepted conventions for running specific applications on specific ports. A common example is web server software. By defualt, web servers use port 80 and it would be monitored by the software for connection requests. Therefore, if you are running a web server on your system port 80 has to be “open”, however, if you are not running a web server it should not be “open”/accessible.

If you tested your system for security loopholes at the Shields Up web site (http://grc.com), you would have been informed as to which TCP ports on your system are open and thus vulnerable to attack. If you need to determine why a given port is open on your system and if it can be safely closed, the Shields Up web site provides easy and clear explanations of the necessary concepts, and detailed instructions for making configuration changes. NOTE: A quick solution would be to install firewall software such as Zone Alarm from Zone Labs (www.zonelabs.com).

The Shields Up website performs TCP port scans of your system as well as probes for well-known vulnerabilities such as open file sharing access. A port scan is a piece of software which queries the ports of a given system by tranmitting TCP/IP commands that will generate a response if the port is open ("listening)". A port can only be opened and kept open by software that is running on your system e.g. a web or FTP server, a chat client such as ICQ or a malicious Trojan horse. There is no simple way to close TCP ports; if you are concerned about open ports, you need to identify which program(s) are keeping them open and whether or not you need to have such programs running in the background.

A major security concern is the Trojan horse server e.g. "Back Orifice"; These servers open their own ports to communicate with intruder scanners. If you see any non-standard ports open on your system and there is no apparent reason for such activity, you may have a Trojan horse hiding in your system. An up-to-date anti-virus program should be aware of the latestTrojan horse programs and should able to remove them.

One of the most abused TCP/IP security loopholes is your Win95/98 file and print sharing access. If you use a stand-alone machine and if you do not need to share files on a LAN/over the Internet, these capabilities should be turned off. You can disable them by unbinding “File and Printer Sharing” from TCP/IP, in your computer's Network Neighborhood.

Appendix C: Useful websites

Anti-spy/pro-security sites:

Richard Smith's Technology of Spying Pages: www.tiac.net/users/smiths/privacy/index.htm

Steve Gibson's website: http://grc.com
(contains info on: windows network sharing, spyware and firewalls)

Privacy Foundation http://www.privacyfoundation.org/
(info on all sorts of internet based ad-tracking and spying)

Privacy Power http://accs-net.com/smallfish/index.htm
(info about the companies who create spyware and the methods used by each spy technology)

CounterExploitation (warning: adult language): http://cexx.org/main.htm

Voice of the Republic (warning: adult language): http://www.voiceoftherepublic.com

Anti-hoax sites:

Computer Emergency Response Team	www.cert.org
Warnings about virus hoaxes from F-Secure	http://www.F-Secure.com/virus-info/hoax/

Note: the antivirus vendors maintain lists of all known viruses and virus hoaxes. You can check their sites to determine if the virus/trojan is real or fake.

Anti-virus vendors:

InoculateIT Personal Edition v5.1	http://antivirus.cai.com/
McAfee	www.mcafee.com
Norton anti-virus	www.symantec.com

Miscellaneous :

Spyware removal software (freeware): www.lavasoft.de/free.html

Download Mage (non-spyware download manager): http://lctek.tripod.com/dnloadmage/

Personal firewall software: www.zonelabs.com

Another personal firewall: www.sybergen.com

Website about cookies: http://cookiecentral.com

Un-install the Win98 Scripting Host http://www.F-Secure.com/virus-info/u-vbs/uninstall-vbs.html

ZDWebopedia (online glossary of computer terms and technology): http://www.zdwebopedia.com

News sites:

CNBC: www.cnbc.com
CNET: www.cnet.com
CNN: www.cnn.com
Fox News Channel: www.foxnews.com
MSNBC: www.msnbc.com
News.com: www.news.com
Techtv (formerly ZDTV): www.techtv.com

Search engines:

Ask Jeeves: www.ask.com
Altavista: www.altavista.com
Google: www.google.com
Hotbot: www.hotbot.com
Lycos: www.lycos.com
Northern Light: www.northernlight.com
Yahoo: www.yahoo.com

Freeware/Shareware sites:

Cnet : www.shareware.com
TUCOWS: www.tucows.com
ZDNET software library: www.hotfiles.com

Appendix D: List of known spyware programs

Note: new spyware is being created and distributed every day and this list is literally the "tip of the iceberg". This list was originally compiled by: Gilles & Yves Lalonde. Please check their website for updates: http://www.infoforce.qc.ca/spyware

100% Word Search Free
123Search
2MinuteWarning
3d Anarchy
3D Frog Man Demo
3D Maze Man Demo
3D-FTP
3rd block
Abe's FTP Client
Abe's Image Viewer
Abe's MP3 Finder
Abe's Picture Finder
Abe's SMB Client
Absolute Yukon Solitaire
Access Diver III
Aces and Kings Solitaire
Acorn Email
AcqURL
ActionOutline Light 1.6
Active 'Net
Add URL
Add/Remove Plus
Add/Remove Plus!
AddAce
Address Rover 98
Admiral VirusScanner
Advanced Call Center
Advanced Maillist Verify
AdWizard
Alchemist Demo
Alive and Kicking
alphaScape QuickPaste
Appload Notify
ASP1-A3
Auction Explorer
Aureate Group Mail
Aureate SpamKiller
AutoFTP PRO
AutoWeb
AxelCD

Balloon Pop Demo
Banner Crafter
Beatle
Binary Boy
BinaryVortex
Bingo Demo
Bingo Master Demo
Blast Thru Demo
Blue Engine
BuzMe
BookSmith : Original
buddyPhone 2
Business Letter Punch
Calypso E-mail
CamGrab
Capture Express 2000
Cascoly Screensaver
CDDB-Reader
CDMaster32
ChanStat
Charity Banner
Chat PicPluck
Cheat Machine
Check & Get
Check4New
Chinese Checkers Demo
ChinMail
Clabra clipboard viewer
Classic Peg Solitaire
Clean and Tidy
CoffeeCup Free HTML
ComTry Music Downloader
Connect ?
Crazy Drake Demo
Crazy Puzzle Demo
CrushPop
Crystal FTP
CS Telnet
CSE HTML Validator Lite
Cursor Maker
CuteFTP
CuteFTP 3.0
CuteFTP 3.0 beta
CuteFTP/Tripod
CuteMX
CutePage
Danzig Pref Engine
DateTime
DB to HTML Express

Debt Relief
Delphi Component Test
Delphi Tester
Develop Critical Thinking Skills
Dialer 2000
DigiBand NewsWatch
DigiCams - The WebCam Viewer
Digital Postman
Digital Postman
DirectUpdate
DL-Mail Pro 2000
DNScape
Doorbell 1.18
dotCool Builder
Download Minder 1.5
Download Wonder
DownLoader v.1.1
Dweebs Demo
Dwyco Video Conferencing
EasySeeker
EconForecast
EmmaSoft ChatCat
EmmaSoft dBrow
EmmaSoft KeepLan
EmmaSoft Soundz
eMNGma
EnvoyMail
Essay-Punch
Extreme Animals Demo
Extreme Bugs Demo
Extreme Dinosaurs Demo
Extreme Orchids Demo
EZ-Forms FREE
File Mag-Net
File Sniffer
FileSplit
FlashGet 0.76 and newer
FlexSpex
Folder Guard Jr.
FourTimes
Free Picture Harvester
Free Solitaire
Free Solitaire
Free Spades
Free Submitter Pro
FreeImageEditor
FreeIRC
FreeNetMon Web3000
FreeNotePad
FreeSite

FreeWebBrowser
FreeWebMail
FreeZip!
FTPEditor
Galactic Invasion Demo
Galaxy of 3D TetriMania Demo
Gardener Demo
Garret Demo
GetRight
Glowing Bugs Demo
Go!Zilla
Go!Zilla WebAttack
GovernMail
Grafula
Grammar Fitness Suite
Gunther's PasswordSentry
Gypsee
HangWeb
hesci Private Label
Hexx Wars II
Home Buyer's Calculator Suite
HTML Translator
HTTP Proxy-Spy
Huey v1.8 Color Picker
Iban Technologies IP Tools 3.1
Idyle GimmIP
Idyle GimmIP
iFind Graphics
Image Carousel
Image Site Grabber
imageN
InboxSpecialist
Infinite Patience
InfoBlast
InnovaClub
InstallZIP
Intergalactic Exterminator Demo
Internet Tree
Internetrix
InterWebWord Companion
IPLAY
iSolitaire
IVOX
IVOX ICQ
JetCar
JFK Research
jIRC
JOC Email Checker
JOC Web Finder
JOC Web Spider

KVT Diplom
LapLink FTP
Lexicon Demo
LineSoft Download
Link Crafter
LivePaper
Loan Calculator Plus
LOL Chat
Ludo Safari Demo
Mahjongg Master 2 Demo
Mahjongg Masters Timesink
Mail Them
MailAlert
Meracl FontMap
Meracl ImageMap Generator
Midnight Oil Solitaire
MidWaviPro
Mini Golf Demo
MirNik Internet Finder
More Space 99
MouseAssist
MP3 Album Finder
MP3 Album Finder
MP3 Fiend
MP3 Grouppie
MP3 Mag-Net
MP3 Renamer
Mp3 Stream Recorder
MP3INFO-Editor
Mr. Cool
MSi-Clip
MultiSender
Music Genie
MX Inspector BIG AD
My Genie Patriots
My Genie SE
My GetRight
NeatFTP
Nebula Fighter Demo
Net CB
Net Scan 2000
Net Vampire
Net Vampire
Net-A-Car Feature Car Screensaver
NetAnts
NetBoard
Netbus Pro 2.10
NetCaptor 5.0
Netman Downloader
NetNak

NetScoopFinance
NetSetter Netsetter
Netsonic Pro 2.5
NetSuck 3.10.5
NetTime Thingy
Network Assistant
NeuroStock
NewsBin
News-Lynx
NewsShark
NewsWire
NfoNak
NotePads+
Notificator 1.0b
Octopus
Of The Day Quizzer
Oxide Demo
Paragraph Punch
Patriot Slots
Pattern Book
PCDJ PHAT
People Seek 98
Personal Auction Track
Personal Search Agent
Personal Stock Monitor SE
Photocopier
Photocopier
Photocopier 2.01 Timesink
PicPluck
Pictures In News
Ping Thingy
PingMaster
PKZip
Planet.Billboard
Planet.MP3Find
PMS
Powerzip 2000 Lite
ProtectX 3
ProxyChecker
Puzzle Master Demo
QuadSucker/Web
Quadzle Puzzles
QuikLink Autobot
QuikLink Explorer
QuikLink Explorer Gold Edition
QuoteWatch
QuoteTracker
QuoTracker (V. 1.1.5 - 1.1.7b)
QWallet
RahJongg Demo

Raptor Call of the Shadows Demo
Real Audioplayer 7.0 (Comet Cursor)
Real Estate Web Site Creator
Recipe Review
ReGet
ReGet 1.6
Resume Detective
RingSurf
RoboCam 1.10
Rosemary's Weird Web World
RubberDuck H30+
SaberQuest Page Burner
SafeNet Mail
SBJV
SBWcc
Scout's Game
ScreenFIRE
ScreenFIRE - FileKing
ScreenFlavors
Screenpik
Sea Battle
Shakespeare Punch
Shizzam
ShortKeys Lite
Simple Submit
SimpleFind
SimpleSubmit v1.0
Simplicity Personal Organizer
Site Select
SK-111
SL4 Historical Montage
Smart 'n Sticky
SmartBoard 200 FREE Edition
SmartSum calculator
SonicBurn Free
Sonic Mail
SonicMail
Sound Agent
Space Central Screen Saver
Speedy Eggbert Demo
Splash! Siterave
SSScanner
SSSiter
SSSpider
Star Miner Demo
StartDrive
Static FTP
StayOn Pro
Stock Profit Spread Calculator 32
StockBrowser

Subscriber
SunEdit 2K
Superball Challenge Demo
SuperIDE
Surf Saver
Sweep
SweepsWinner
System Agent
Tagger
TetriMania Master Demo
Text Transmogrifier
The Mapper
TheNet
TI-FindMail
TIFNY
Time Zone Converter
Tools 3.1
Total Finger
Total Whois
Tracking The Eye
Trade Site Creator
Trade Trakker
Tray Note Plus
TsAdBot
TS-Image Mapper
Tunnel Blaster Demo
TWinExplorer Standard
TypeWriter 1.0
uICE
UK Phone Codes
Vagabond's Realm
VeriMP3
Vertigo QSearch
Virtual Access
Visual Cyberadio
Visual Surfer
VOG Backgammon Main
VOG Backgammon Table
VOG Chess Main
VOG Chess Table
VOG Reversi Main
VOG Reversi Table
VOG Shell
VOG Shell
VOG Shell History
W3Filer
War Demo
Web Coupon
Web Page Authoring Software
Web Registrant PRO

Web Resume
Web SurfACE
WEB2SMS
Web-Cam VCR
WebCamVCR
WebCopier
Web-N-Force
WebSaver
Website Manager
WebStripper
WebStripper
WebType
Whitehouse Mambo Parody
WhizFolders Organizer
Whois
WhoIs Thingy
Win A Lotto
WinEdit 2000
Word Connect Demo
Word Search Mania Demo
Word+
Wordwright
WorldChat Client
Worm
Writing about Reading
Writing for Business
www.cyber-gold.com/free.htm (Comet Cursor)
www.devgames.com
xBlock
Your ESP Test
Zion
Zip Code Finder
Zip Express 2000

Appendix E: Online advertising/marketing companies

This is a list of companies who use web based tracking and data collecting technologies to profile Net surfers for advertising/marketing purposes. Source: the "Privacy Power" pages located at: http://accs-net.com/smallfish/index.htm
This site provides further information on these companies such as:

- How the company collects its data
- Its privacy policy (if any)
- Its business associates (which companies benefit from the data collection)

123Banners

AdForce (Imgis)

Advertising.com (Teknosurf)

AppNet (i33)

Avenue A (iballs.com)

Be Free (BFAST)

Bluestreak

Burst Media (BURST!)

Commission Junction (CJ.com, track4)

Cybereps

Doubleclick

Engage

eXTReMe Tracking

L90 (AdNet Strategies, Latitude 90)

STATSnet sprl (Net-Trak)

TRUSTe

ValueClick

WebSideStory (Hitbox)