Computing & Networking Services

Computing & Networking Services
255 Huron Street, Room 345
Toronto, Ontario, M5S 3J1

UTORProtect

BEST PRACTICES

Your guide for protection your data and computer

Tuesday, November 12, 2002

Version: 1.0

Table of Contents

Section 1

Introduction

Information protection and computer security have become increasingly important issues to many computer users. Computer viruses have become more sophisticated and as more and more users leave their computers connected to the Internet 24x7, attacks by hackers have increased dramatically.

If you are using your computer to conduct research or to complete assignments or for business, then it is important that you take the necessary precautions to protect the data and information that is stored on your computer. The University expects that any institutional data stored on computers, whether on campus or at you place of residence, must be protected.

The University is increasingly taking a pro-active approach to data protection. For example, an institutional license for anti-virus software makes this software available at no cost to all students, faculty and staff. This should reduce instances of infections that generate a lot of unnecessary traffic on our networks as well as protect data and information from being inadvertently divulged to unauthorized individuals. Another initiative is a service that enables departments to backup network servers.

As part of the UTORProtect Program initiated by Computing & Networking Services, this Best Practices document was developed in order to assist all users associated with the University to protect their computers and the data and information stored on computers.

This document is intended to assist students, faculty and staff to determine how best to protect their computers. It is not intended to address technical issues nor is it a detailed “how to” or “do it yourself” technical reference document.

If you have any comments on the content or if you have any suggestions on how we can improve this document, please feel free to contact Computer Security Administration in Computing & Networking Services by email at security.admin@utoronto.ca.

Section 2

Malicious Programs

Viruses, Worms, Trojans, Spyware

Malicious programs, often referred to as "Malware" includes computer Viruses, Worms, Trojans, Spyware, and other programs written specifically to spy on network traffic, record private communications, execute unauthorized commands, steal and distribute private and confidential information, disable computers, erase files, etc., etc.

Some programs, such as Kaza, Napster, and others, although not intended to compromise computers, expose computers they are installed on to attacks from hackers.

This section addresses the various types of malicious programs.

Viruses

The threat of virus infections has increased dramatically in the past three to four years. Before the advent of e-mail attached viruses, virus were spread through exchange of infected media and this limited the potential damage that a virus could result in. When e-mail borne viruses appeared on the scene, the threat increased considerably. The sophistication of virus code has also contributed to the problem, as has the popularity of the Internet. Now viruses spread much faster and can potentially cause more damage than in the past.

In the past, a virus infection could result in loss on data on the infected computer and the inconvenience created by corrupted software on the infected machines. New forms of virus code have added the threat of loss of confidential information and individual privacy.

Computer users are well advised to protect their computers from the threat of virus infections. Many organizations now require that their users use virus detection programs. The University, through its program that makes virus software available at no cost to the University community has made virus protection a de facto requirement for all users connected to University networks, whether on campus or off campus. Users who fail to protect their computers may be prevented from accessing University networks and services available through those networks.

What can viruses do?

The possibilities are almost limitless, but viruses can: erase data on your computer; encrypt files; delete directory structures; prohibit you from using your computer; send files stored on your computer to contacts in your address book without your knowledge; and much more.

How does anti-virus software work?

The anti-virus program contains a database of virus signatures (strings of code that identify a virus program, much like a fingerprint). These signatures are utilized by the anti-virus software to identify files that may contain a virus. When the anti-virus program searches for viruses, it lets you know when it finds a match. The anti-virus program can look for viruses in files that you open, copy, save, or modify. It can also block

harmful files that you unknowingly download from the Internet and can scan your email attachments before they are downloaded on your computer.

Best Practices

- Install a copy of the Symantec anti-virus program on your computers and make sure that the software is always up to date.
- Make sure that your anti-virus software is always running and that it is set up to automatically start up when the computer is rebooted.
- Before clicking on any e-mail attachment, make sure that the attachment is something you were expecting – do not blindly click on any attachment. Scan for viruses before opening the attachments even if you know the source.
- Before using media given to you by someone else, scan it for virus infections. Viruses can be transmitted on all readable media including diskettes, CDs, USB memory cards, and other types of memory media such as SmartMedia.
- Scan all files you receive as e-mail attachments before opening them.
- Configure you anti-virus program for maximum protection.
- As a general rule, you should only download files from trusted sites.
- Back up important files regularly.
- Password-protect shared directories.
- Make sure that your Operating System and any software you use is up-to-date. Install patches made available from vendors of your software.
- If you receive an e-mail about a virus from a friend or colleague, do not forward it to anyone. More often than not, these messages turn out to be a virus hoax. These virus hoaxes cause a lot of unnecessary use of resources when users blindly forward such messages to all their friends and colleagues.

Section 3

Operating Systems

Windows 98

Step 1: Use a good password.

This is your first line of defence. Use a strong password to protect the login to your computer. Please refer to the Accounts, Passwords & PINs for password guidelines.

Step 2: Create a login screen for Windows 98

Although it's one of the weakest features of Windows 98, creating a login account still prevents computer-illiterate snoopers from playing with your desktops. They won't know that this feature is just a bluff and that all they have to do to bypass the login screen is to press [Esc]! To create a login screen, follow these steps:

- Go to Start | Settings | Control Panel.
- Click the Passwords icon in the Control Panel window.
- On the Change Passwords tab, choose the Change Windows Password box.
- Enter the information that's requested. If you're setting a password for the first time, leave the Old Password area empty.

As mentioned earlier, the downside is that it doesn't really add much security. Anyone who hits [Esc] can get to the desktop.

Step 3: Add a screen saver password

If your desktop's security is so important that you're bothering with BIOS and login passwords, then you won't want to leave your computer vulnerable every time you step away from your office. Why not add a screen saver password to keep curious eyes off of your desktop? You can do so by following these steps:

- Right-click on some blank desktop real estate.
- Select Properties.
- Choose the Screen Saver tab from the Display Properties dialog box.
- Choose a screen saver (if you haven't already) and adjust its delay value to a time period that's reasonably brief—three to five minutes would be fine.
- Check the box next to Password Protected, click change, and add or change your password. If you set a password length restriction earlier, it will be enforced here.

The downside is that if you don't reset the screen saver first, it tends to start up when you're in the middle of a download or an upgrade.

Step 4: Turn off file and printer sharing

There isn't much point to protecting your desktop if every user on the network has access to your files. You need to prevent general network access to your hard disk by removing file and print sharing from network properties. If you right-click a folder and choose Properties when sharing is enabled, the resulting dialog box will contain a tab called Sharing. When sharing is removed, that tab will disappear.

If a folder is shared, it will appear on the network with the name you give to it in this tab. You can specify access as read-only, full, or password-dependent. You have an option of specifying one password for read-only access and another password for full access. When you turn on a share, the folder icon changes. In Windows Explorer, shared folders appear to be offered by a hand with the palm up. This scheme is referred to as share-level security.

Although you may have good reasons for sharing resources on your network, there are a few drawbacks to using share-level security. First, the share information is stored on your workstation, and anyone who gains access to the computer can modify the shares. Second, shares aren't authenticated. Again, anyone on the network who obtains the password can access your resources. Third, share-level security provides only one password per folder. Put this aspect together with the lack of authentication, and there isn't any way to secure your folders at the user level. Finally, unlike Windows NT or Windows 2000, when it's running NTFS, you can't protect files—just folders.

To remove file and printer sharing, go to the Control Panel and click the Network icon. In the Configuration Tab, scroll down the network components list to File And Printer Sharing For Microsoft Networks. Highlight that option and click the Remove button. Afterwards, your hard drive will become much more secure.

The downside is that you will lose your ability to share your resources on the network.

Exceptions

If you absolutely must share the contents of a folder with members of a workgroup or domain, opt for user-level security instead of share-level security. Although you can't protect resources down to individual files and your shares are still stored on your computer, you can authenticate users against a list of authorized accounts on a Windows NT or NetWare server. To enable user-level security, follow these steps:
Make sure that you've installed file and printer sharing.

- Click on the Network icon in Control Panel.
- Select the Access Control tab and choose User-Level Access Control.
- In the box below, fill in the name of the Windows NT domain or workstation that has user accounts (if it's not filled in already).

To share a folder, highlight it in Windows Explorer and right-click. Select Properties and click the Sharing tab. You can keep the same share name or revise it. Then, click Add. The Add Users dialog box will open. It contains a list of all of the groups and users on the Windows NT domain or workstation that you selected. Select a user or group and click one of the buttons marked Read Only, Full Access, or Custom to move the user or group to that level of access.

Custom access needs to be defined before you can save it. When you close the Add Users dialog box, the Change Access Rights dialog box will open. Check a box that corresponds to the access that you want the user or group to have. You can allow custom users to read, write, create, and delete files; change file attributes; list files; and change their own access control.

Sometimes a user who tries to log on to your shared resources may receive an Access Denied message. The user, who may have more than one workstation, may be coming in through a different domain. If a trust relationship hasn't been established between the two domains, then access isn't possible.

Step 5: Turn off remote administration

Remote administration allows specified groups or users, such as the IT department or help desk staff, to access your personal computer and make changes from a central location. Remote users can browse and manage shared resources, manage the file system, edit the registry, and monitor the performance of the remote computer. Although it's convenient for the IT staff, you may want to turn off remote administration

when your computer needs to be extra secure. To do so, double-click the Passwords icon in Control Panel, click the Remote Administration tab, and uncheck Enable Remote Administration Of This Server. Please note that the change won't take effect until the next time you boot.

Step 6: Disable password caching

When you're asked for a password in Windows 98, you're given the choice of having the OS remember the password for you so that you don't have to fill it in next time. Once you check the Save Password box, your password is encrypted in a file with the extension .pwl. If someone gains access to your desktop, this person can send and receive your e-mail and access any other resources for which the passwords are cached. Password caching makes you vulnerable. On the other hand, some of us have so many passwords that we would have to possess a remarkable memory just to recall all of them.

If you can store all of your passwords in your head, then feel free turn off password caching. Doing so will protect your desktop against many threats. To turn off caching, follow these steps:

- To open the registry, click Start | Run and type *Regedit*.
- Navigate to this key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network.
- Add a new DWord value called DisablePwdCaching.
- Give a value of 1 to enable this feature.

You also can disable password caching by creating or modifying a system policy with the System Policy Editor (Poledit.exe).

The downside is that you have to remember each password.

Conclusion

When it comes to security, every enhancement is a trade-off. To gain more security, you lose a certain measure of convenience. You'll want to weigh the gains in security against your losses in user-friendliness and IT administration before you make drastic changes to your machines.

Windows NT

(Placeholder)

Windows XP

Like Windows 2000, XP uses the NT File System (NTFS). As an Administrator, you control your XP system. You can create users, who can be administrators or just normal users. Policy can be created to limit which applications can be executed by any user. For standalone XP, this is done through the Local Security Settings.

AUTHENTICATION

Windows XP's standalone version lets the user choose a blank password, but then institutes certain default limitations. You cannot log in remotely to an account with no password, but rather only at the console, which is sensible. A new feature, Fast User Switching (FUS), permits you to log in as a

completely different user, and then switch between multiple user contexts without backing out of any applications that are running. FUS won't work when a user hasn't chosen a password.

Defaults for passwords are located in the Local Security Settings. In the standalone version, settings such as password lengths and number of failed login attempts are found here. Except for the number of failed logins being set to 10 and passwords expiring after 42 days, all other password features are set to zero or disabled. Thus, someone can enter a blank password, or recycle their old password when it expires. Password complexity checks are also disabled.

While blank passwords sound okay for home users, there's a bit more to XP and passwords than logging in or switching between user contexts. We need to discuss some other security features before it becomes apparent that having a blank password is a really, really bad idea in XP.

ENCRYPTION

Like Windows 2000, XP professional includes the Encrypting File System (EFS). Unlike Windows 2000, EFS is enabled by default, so as soon as you begin creating files with XP, they're encrypted. This is transparent to the user, although Explorer can control this behavior on a per-file or folder level. You don't need to enter the encryption key, as XP dose this for you.

XP also encrypts Cached Files, a technique that permits you to use up to 10 percent (by default) of your hard disk space to hold files that would normally be stored on a remote file share. You can then disconnect from the network, go home (or travel), and still access these files. The Windows Mirroring system will reconcile the file changes you've made with the Windows 2000 or XP file shares when you reconnect with the network. Encrypting these cached files is a great idea, as your notebook might be stolen (or if your evil genius of a son or daughter happens upon them while using your XP system).

XP also supports file sharing with Web Developing, Authoring, and Versioning (WebDAV), which uses HTTP to access remote files through firewalls. EFS can keep your remotely stored files encrypted, and when teamed with WebDAV, has the added value of storing and transmitting the data without decrypting. (In comparison, while accessing files using regular file sharing, the data is decrypted before it's sent across the network.) While WebDAV with EFS is a powerful feature, it also sends chills up the spine of any corporate security person even remotely aware of using Web tunneling to move internal files offsite-and encrypted to boot!

Credential Management stores various credentials for you, including public key certificates. It will also manage Kerberos keys, the default authentication mechanism for Windows 2000 and XP within a domain. You can store other usernames and passwords here as well, by asking (when prompted) that the Credential Manager “remember the password.” In this way, the Credential Manager becomes a single-sign-on agent.

The keys that encrypt your stored private key, other passwords, and EFS are based on two things: secrets that remain fixed for XP, and your password. If you've chosen a blank password, you've also chosen a null seed for the key that encryptsmany important things. Even choosing a weak password is a very bad idea if you plan to rely on any of these features. XP supports passwords longer than 14 characters (the old limit imposed by the user interface in Windows 95/98/NT), so you can use a passphrase instead.

XP includes a policy option of using reversible encryption for storing passwords. This is a very bad idea, as passwords are typically stored as hashes, a value based on the password that is not reversible.

Domain users can opt to use smartcards for authentication, which is a big improvement over passwords. By adding a smartcard reader to your desktop or notebook (they come in PC Card or CardBus packages), you've added something you have (the smartcard) to something you know (the PIN that unlocks it). Smartcards can often store your private key as well as any certificates, making them more secure than online storage. Smartcards do have their weaknesses: Keystroke monitors can collect your PIN, for example, but even then they still need the card.

Even if you do use a smartcard, XP unfortunately subverts it with one of its intrinsic properties: You can hibernate instead of shutting down. That means that when you restart your computer, you're right where you left off. It also means that if you hibernate, and the janitor powers on your system, he or she is also right where you left off. I tried this in the standalone version, and assume that it works the same way in domain installations.

NETWORK SECURITY

Windows XP (and Windows 2000) includes support for IPSec, the Internet standard for encrypting network communications. XP's IPSec support seems very complete, permitting the use of shared secrets (the most common method in many VPN products), as well as certificates and Microsoft Kerberos (the Kerberos variant where Microsoft has added proprietary extensions, so that the Key Distribution Server must reside on Windows 2000.

For home users, XP offers two useful features designed to compete with the Small Office/Home Office (SOHO) firewall vendors. The Internet Connection Sharing (ICS) feature enables your XP system to act as a Network Address Translator (NAT) for other systems in your local network. ICS includes a DHCP server that assigns addresses to members of your local network and transparently routes packets through your XP system to your ISP. ICS can bring up dial-up connections on demand, and can hang up the modem temporarily so that you can use the phone, yet resume the Internet connection afterward.

The Internet Connection Firewall (ICF) uses information collected by ICS to provide limited firewall capabilities. ICS must keep track of traffic that leaves your network in order to NAT. ICF uses this information to control which IP packets can enter your network-if a packet attempting to enter your network doesn't match at least one outgoing packet, it's blocked. ICF provides a simple form of firewall-essentially just NAT-and also won't permit you to set up a public server behind it.

REMOTE CONTROL

XP sports a new feature called Remote Assistance, which allows you to send a message to a “friend” (using Windows Messenger or Outlook Express) that invites them to take remote control of your XP system. With XP's complexity, you might really need configuration help, but providing a remote control capability can be dangerous. When someone consented to let me be his or her “friend,” XP actually failed to pass through the local, Linux-based firewall, while complaining about a failure to resolve the hostname (which was resolvable using nslookup under XP).

With any luck, many of XP's features that appear dangerous at first glance (just like Remote Assistance) will prove benign. Microsoft has taken strong steps to improve desktop security with XP, and we can only hope that it works.

Windows 2000

(Placeholder)

LINUX

(Placeholder)

Mac OS

(Placeholder)

Patches & Fixes

(Placeholder)

Section 4

Firewalls

Personal Firewalls

Securing personal computers has become an important issue because of computer viruses and the increase in hacking activities. If you are using a service such as that provided by cable companies, your risks are much higher especially if you are connected to the Internet continuously.

Personal Firewalls are programs that control access to your computer by restricting and allowing certain packets from external hosts via configurable rules (originating port, destination port, originating host, etc). This enables the user to block denial of service attacks and other hostile Internet attacks.

Installing a personal firewall can be quite easy but you must keep in mind that in most cases firewalls will require a deeper understanding of networking, operating systems and software. Since most firewalls are able to block incoming as well as outgoing connections, you have to be aware of what services/programs are being blocked. If you don't, you may find that services and programs that used to work before the firewall was installed may stop working.

Many personal firewalls can be set to notify you when they are about to block a connection. This is a good feature but may also be annoying after a while. If you decide to turn the notification feature off, you may run the risk of not knowing why a program or service stops working all of a sudden. On the other hand, this notification process may be confusing since you have to determine whether to allow/disallow a particular connection.

If you are considering acquiring and installing a personal firewall, use the checklist below for evaluating the software:

- System requirements
- OS support (Windows 9x, NT, 2000, Macintosh, Unix)
- Ethernet NIC support, Adapter compatibility
- Compatibility with NDIS or other (e.g., IPsec VPN) adapters that are part of your desktop
- Packet filtering
- Port filtering
- URL filtering and blocking
- Anti-virus measures
- Intrusion detection features
- Logging and reporting

When deploying personal firewall software, one big concern is compatibility with existing software. Ask the software vendor for information on know compatibility issues.

You should consider what may happen if the personal firewall software is itself attacked. Experience has shown that applications connected to the Internet can and do crash. When personal firewall software crashes, it could leave the host laptop or desktop unprotected, or causes the host itself to crash. Personal firewall software is in its infancy, and vendors are still hastily publishing patches as new exploits are discovered. Investigate your prospective vendor's track record; be diligent in applying new patches and

appropriately cautious about where you install this software.

ZoneAlarm

Web Site: http://www.zonelabs.com

Cost: Free for personal/non-commercial usage

Description: An easy-to-use firewall for PC users that also features application control, multiple security levels, auto-blocking of Internet traffic when the system is not in use, protection from VBS viruses, and more.

Platforms: Windows 98/Me/NT/2000 and XP

Support: On-line support from the ZoneAlarm web site.

ZoneAlarm Pro

Web Site: http://www.zonelabs.com

Cost: You can also purchase a more feature-rich version, ZoneAlarm. Please check the ZoneLabs web site for current pricing.

Description: ZoneAlarm Pro offers multiple security levels, auto-blocking of Internet traffic when the system is not in use, and protection from VBS viruses. It also protects against Internet-borne threats like worms, Trojan horses, and spyware. It also blocks Ads and controls cookies.

Platforms: Windows 98/Me/NT/2000 and XP

Support: On-line support from the ZoneAlarm web site.

Tiny Personal Firewall

Web Site: http://www.tinysoftware.com/pwall.php

Cost: Free for personal use

Description: Tiny Personal Firewall (TPF) is a powerful and free utility designed to protect home cable and DSL connections. TPF provides multi-layer security protection in controlling which applications are allowed to transmit and receive data.

Platforms: Windows 9x, ME, 2000, NT4.0 and XP

Support: On-line support from the TinySoftware web site.

Norton Personal Firewall 2002

Web Site: http://www.symantec.ca/

Cost: (Please check the Symantec web site for current pricing)

Description: Automatic firewall configuration sets up appropriate firewall rules for the most common Internet applications. Verifies that Internet-enabled applications are authentic — not "spyware" or Trojan horse programs. Blocks confidential info in AOL & MSN instant messaging applications

Platforms: XP Home/XP Pro/2000 Pro/NT WS/Me/98

Support: On-line support from the Symantec web site.

Best Practices

- Disable any unnecessary services on your machine.
- Deny all traffic by default and only enable those services that are needed.
- Enable firewall logging. If you have to report an intrusion, you will probably be asked to supply logs from your firewall.
- Apply any patches released by the firewall vendor.
- Monitor your logs regularly.
- Look for patterns within the logs. If you decide to investigate an intrusion attempt do so right away. If you delay in reporting an intrusion attempt, the administrator of the network form where the intrusion originated may not have the logs available to investigate the incident.
- Do not bother reporting normal network traffic events, such as Pings.
- If the firewall has password protection to enable changes to configuration, make sure you use it.
- Firewalls do not protect data and information sent over the Internet. If you are worried about the protection of personal or confidential information, encrypt the data.

Section 5

Backup & Recovery

Can you afford to loose your data? Without data from a back up source, there is no way to recovery following some sort of incident such as hardware or system malfunction, human error (deleting a file by mistake) or a virus infection that results in loss of data.

At a minimum, consider backing up your documents. This is easier to do if you store all your documents in the "My Documents" folder. There are various types of media you can use for backing up your data. These included floppies, CDRWs, DVDs, Zip media, USB drives, and tape. Which medium you use depends on how much data you are trying to backup and the peripherals you have installed on your computer.

Storage capacity of various media:

Diskettes	1.4MB
CDRWs	605-850MB
DVDs	3-17GB
Zip Disks	100MB – 20GB
USB Drives	32MB – 1GB

Best Practices

- Take regular backups of your data.
- Make sure your backups work. Remember, if you back up garbage, you'll restore garbage.
- Store backup media in a safe and secure place, preferably at a different location from your computer.
- Store backup media in a data safe or in a place that is not susceptible to extremes of temperature, humidity, etc. CDRs are a good and cheap medium for data backup from a personal computer. Tape backup is good for both local restores, and off-site disaster recovery.
- Consider the following types of backups. Full backup of your system – this usually includes your entire system and all its files. Incremental backups - only the files that have changed since the last full or incremental backup are backed up. Differential backups – only files that have changed since the last full backup are backed up. Differential backups are faster to restore from. To use this sort of scheme, you will need to have backup software installed on your computer.
- Use a backup rotation scheme so you have backups from different dates available for recovery.
- Make duplicate backup copies and rotate one off-site weekly.
- Include every hard disk in your backup process, including mobile PCs.
- Always use 'verify' to insure files have been correctly written to tape, try restoring a few

Section 6

Accounts, Passwords & PINs

Accounts, passwords and PINs are provided to users to enable them to access protected or restricted systems. Accounts, passwords and PINs are issued to individual users are not intended to be shared for any reason. Many protected systems are compromised because of misuse and abuse of accounts, passwords, and PINs. Maintaining the confidentiality of passwords and PINs is the sole responsibility of the users to whom they are issued.

Best Practices

- Never share your account, password or PIN with anyone else, including relatives, friends, colleagues, supervisors or the network/system administrators.
- When you are assigned a temporary password or PIN, make sure you change it right away.
- Never use passwords or PINs that are easy to guess or that can be somehow associated with you.
- Do not use **obvious** (e.g., names of persons, pets, relatives, cities, streets, your LogonID, your birth date, car license plate, etc.), **trivial** (e.g., dictionary words like 'secret', 'password', 'sex', 'computer', etc.), or **predictable** (e.g., days of the week, months, or a new password that has only one or two character different from the previous one you used) passwords and PINs.
- Do not write down or store passwords and PINs on your computer or computer media unless absolutely necessary. If you absolutely have to, make sure that the paper the information is written on is stored in a secure and safe place or if stored on your computer or computer media it is encrypted.
- Never use the same password twice. In fact, good access control systems prevent you from choosing a new password that is similar to your old one. When you are selecting a new password, choose one that is quite different from your previous password.
- Passwords should be changed frequently. The shorter the life of a password, the better it is. Some systems force users to change their password at predetermined intervals.
- Passwords should be at least four characters in length. If the system allows a password longer than four characters, then it is recommended that you use a minimum of six characters. Longer passwords are harder for others to guess.
- Passwords should contain a combination of alphabetic, numeric and special characters.
- Avoid using any dictionary words.
- Use a combination of characters including numbers, letters, special characters and mix upper and lower case characters.

Examples of Good Passwords (Please do not use these specific examples)

- Use a word with one or two digits embedded in it.

  Examples:

  HOU32SE, MON42DAY, TAB87LE2

- Make up an acronym based on a nursery rhyme, a favourite song or movie, or a sentence.

  Examples:

  MHALL - **M**ary **H**ad **A** **L**ittle **L**amb
  MDHF# - **M**y **D**og **H**as **F**leas**#**
  OTGDY - **O**nly **T**he **G**ood **D**ie **Y**oung
  TERM2 - **Term**inator **2**

- Use a three character pronounceable word suffixed or prefixed with a one- or two-digit suffix or prefix.

  Examples:

  DAM56, WAR34, 56DIG

- Make up nonsense words that mean something to you by combining the first syllables of two words. However, avoid using standard abbreviations like "jan, feb, mar, etc." as part of your password.

  Example:

  PUBPOL - **P**ublished **P**olicy

- Drop vowels or drop everything but the first 6 letters of a long word or two words.

  Examples:

  CLNDSK1 - clean desk
  DEDICA5 - dedication
  HOMEWO# - home work

- Use special characters like #, $, and @. These too, can be inserted anywhere.

  Example:

  UNI$VER - university

- Misspell a word, drop a couple of letters or add some.

  Examples:

  MISTIFI@ - mystify
  CELLEB - celebrate
  RNYDY$ - rainy day

- Be creative! And, try to choose a pattern that has meaning for you but that no one else can guess. For example, you might use upcoming events in your life. If you, or one of your children has a major essay to write next month, you might create a password reflecting that event.

  Example:

  MAJESS - Major essay
  4CUZZ029 - 4th cousin, twice removed

- Another pattern could be to choose meaningful words with a minimum of 10 letters and always use only the first 6 letters. Then add a special character as one of the characters

  Examples:

  ANNIVE$ - anniversary
  UNBEND# - unbendable
  @UNBEND - unbendable
  UN#BEND - unbendable

Note: Some systems have restrictions as to which special characters can be used as part of a password. For example, ACF2 will only allow #, @, and $ as part of the password.

- The best password is one which is a random combination of numeric and alphabetic characters.

  Example:

  48KK439V

- On systems which allow both upper case and lower case letters, use a combination of upper and lower case characters for your password.

  Example:

  4*hk8LP9

- Finally, please remember that there is no need to share IDs and passwords. Anyone who needs and qualifies for access to a computer system should submit a request for his or her own LogonID and password.

Section 7

E-Mail

Risks

There are many risks associated with the use of e-mail. The risks include information leakage, data integrity violations, repudiation, malicious code, SPAM, and others. Following is a brief overview of the major issues.

Information Leakage

- Many employers and online services retain the right to archive and inspect messages transmitted through their systems.
- Either party might accidentally send an e-mail message to the wrong person.
- E-mail might be left visible on an unattended terminal.
- E-mail can be printed, circulated, forwarded, and stored in numerous paper and electronic files.
- E-mail is discoverable for legal purposes.
- A person authorized to access the information might use it for an unauthorized purpose or disclose it to an unauthorized party.
- Confidential information might be obtained by an unauthorized entity from discarded media.
- E-mail may be vulnerable to computer hackers who could then transmit the information for illegitimate purposes.
- Phony e-mail could dupe legitimate users into voluntarily giving up sensitive information.

Data Integrity Violations

- E-mail is easily intercepted and altered without detection.
- E-mail can be used to introduce viruses into computer systems.
- An impostor can forge e-mail addresses.

Repudiation

- A party to the communication could falsely deny that the exchange of information ever took place.

Malicious Code

Over 11,000 different computer viruses exist to date and some 300 new ones are created each month. Their effects range from negligible, to bothersome, to destructive. The danger of viruses transmitted through macros, another common form of virus transmission, is that they allow the user to continue working and sharing documents. This way, the virus spreads faster, infecting more and more users. One such macro virus, known as Melissa, reared its ugly head on March 26, 1999. Melissa forced organizations the world over - among them Microsoft and Intel - to suspend all e-mail transactions. The spread of this virus resulted in productivity loss. Similar destructive viruses include the Chernobyl and the Explore Worm, both of which wipe out files, resulting in data loss.

Most viruses and other malicious code programs are delivered through e-mail messages as attachments.

SPAM

Most e-mail users receive SPAM - or unsolicited commercial mail – almost daily and unwanted mail is on the increase.

As well as consuming bandwidth and slowing down e-mail systems, SPAM is a frustrating time-waster, forcing users to sift through and delete mounds of junk mail. It also proves irritating and offensive to recipients who feel their privacy has been invaded. However, there is a third aspect to SPAM: it constitutes a security hazard.

Spammers can use a corporate mail server to send out their unsolicited messages, often bringing trouble upon the unwitting organization. Virgin Net recently underwent such an experience when one of its subscribers apparently used its network to send out 250,000 junk messages. As a result of this individual's actions, Virgin Net was put onto the Real-time Blackhole List (RBL), an undesirable listing that leads other ISPs to reject mail coming from that company.

The University does not have a policy on blocking or filtering for Spam. The University does not currently investigate or take any action on Spam received by faculty, staff or students.

What should you do? Either filter the Spam using your e-mail program or simply delete it.

Filtering Spam in MS Outlook

- Choose **Organize** from the drop-down menu **Tools**.
- Click the **Junk E-Mail** tab.
- Turn on the **Automatically Move *Junk* messages to *Deleted Items*** option.
- To add a message to the junk filter, right-click a message and choose **Junk E-Mail** from the menu.

  The sender's e-mail address will be added to the filter and when messages from that e-mail address are read into your in-box they will be automatically moved to the **Deleted Items** folder. You can edit the addresses included in your junk e-mail filter by going to **For more options click here**.

Filtering Spam in Netscape

- Right click on the **From** address and choose **Create Filter from Message...** from the drop-down menu.
- Make sure that the **Perform this action:** in the bottom part of the **Filter Rules** window is set to **Move to folder**.
- Click on the down arrow of the next box.
- Choose **Local Folders** and then choose **Trash**.
- Click **OK** to finish the filter setup.

  The sender's e-mail address will be added to the filter and when messages from that e-mail address are read into your in-box they will be automatically moved to the **Trash** folder. You can edit your filter rules by choosing **Message Filters…** from the **Tools** menu.

Handling Harassing or Threatening E-mail

If you receive a harassing or threatening e-mail message from a specific individual, we recommend you take the following steps:

Step 1

The sender should be told that you do not want to receive any further communications and you should reply to sender with a message similar to the following:

> *"I do not wish to receive any further communications from you of any sort."*

You do not need to explain why, just that you want the communications to stop. Keep a copy of the original e-mail you received as well as the response you send. This is required if any further action is taken to track down the sender. If the content or any circumstances surrounding the message cause you to have concerns for your safety, the University of Toronto Police Service should be contacted immediately.

Forward a copy of the e-mail message to Computer Security Administration at security.admin@utoronto.ca. They are responsible for keeping track of such incidents as well as for initiating investigation of such incidents. Optionally, if you feel it would be helpful, you may choose to cc or bcc a copy of the message to the University of Toronto Police Service. To reinforce the request for non-communication, you many choose to inform the sender you are contacting these university authorities as follows:

> "A copy of this e-mail is being forwarded to the University of Toronto Police Service and Computer Security Administration. Further communication of any sort will result in immediate notification to University authorities and the Police"

Note: Computer Security Administration can provide assistance in taking the necessary steps to resolve such incidents. It is a good idea to keep copies of all messages sent and received. And remember, you don't want to get into a shouting match or a protracted exchange of messages with the individual who sent you the message.

Step 2

If the sender persists on communicating with you please notify Computer Security Administration and the University of Toronto Police Service right away and ask for further assistance.

Computer Security Administration	**University of Toronto Police Service**
Computing & Networking Services	416-978-2323
416.978.1354	
416.978.1267/5551	
E-mail: security.admin@utornto.ca	
Web: http://www.utoronto.ca/security	http://www.utoronto.ca/police/

Other Risks

- The sender may assume, but doesn't necessarily know, that his/her message was delivered.
- The recipient might not check his messages within the time frame the sender expects.
- The attachments embedded in the e-mail might be in a format the recipient's software can't read.
- E-mail can be misinterpreted. Without verbal and nonverbal feedback, the sender can't confirm that his/her messages are understood.

Best Practices

- Understand the risks associated with using electronic mail to discuss personal, confidential or sensitive information.
- Double-check the recipient's address before sending a message.
- Communicate via e-mail only those things you're comfortable having forwarded.
- Avoid using e-mail for particularly sensitive matters.
- Avoid using e-mail for time sensitive messages.
- Take time to make sure the message is clear and concise, and cannot be misconstrued.
- Be careful about leaving programs operational and/or documents visible when your computer is unattended.
- Make use of screen savers with private passwords or automatic sign-off.
- If you receive any harassing or threatening e-mail, report it to Computer Security Administration at security.admin@utoronto.ca. Make sure that you include the e-mail headers from such messages, as this is the only way that the origin of the message can be traced.
- Ensure that your e-mail client is set to check for new mail no more frequently than once every 10 minutes (600 seconds), or longer if that's acceptable.
- Empty your inbox regularly to avoid exceeding your quota. Transfer messages you want to keep from your inbox to other folders, or to your computer's hard drive.
- Unsubscribe from any mailing lists that no longer interest you. Lists generate a huge amount of mail traffic.
- Don't attach very large files to e-mail messages. Generally, attachments should be less than one megabyte. Explore FTP alternatives to send files larger than this.
- Use BCC (blind copy) instead of CC to copy a message to a large number of people. This cuts down on the size of the mail header; it also makes messages easier for your correspondents to read.
- Update your address book regularly and remove addresses you don't need.
- Do not participate in chain letters. It's not only illegal but it's also not a good idea as it ties up network resources for all concerned.
- Learn to recognize virus hoaxes that circulate via e-mail, and don't pass them on.
- Make sure your computer is protected from e-mail viruses.
- Never click on an attachment unless the message has been scanned by your anti-virus program.
- If you were not expecting the attachment, it's best to just delete the message and the attachment.
- Some virus programs change the extension of the attachment so as to disguise its real purpose so you also need to be careful about attachments such as GIFs and JPEGs.
- If you receive advertising and other SPAM messages asking you to reply to the message to unsubscribe, be careful before replying to the messages. If the message is from a company that you are aware of, for example a software vendor or a department store, unsubscribing will usually work. Otherwise, simply delete or filter the Spam.
- Set up your e-mail program to filter SPAM directly to your trash can.

Section 8

Personal Computer Security

Many users do not think about securing their personal computer or Laptops and although this equipment may be relatively cheap to replace, replacing lost data and information and recreating your computing environments may not be so cheap.

Best Practices

- If you use a Laptop, use a security cable to secure the Laptop to a desk. Although this will not deter a determined thief, it will stop someone from attempting to steal the Lap Top quickly.
- If your PC is equipped with a lock, always lock it before leaving for the day.
- Save work-in-progress in case of power or equipment failure.
- Backup data regularly, at least once a week.
- Store all of the backup copies of your data in a secure place, such as a locking cabinet away from your workstation, or a Data Safe (this is a safe especially designed to protect diskettes against destruction from heat, smoke particles and humidity.) Backup copies of data should be stored off-site if practical.
- Backup your disk and then remove all sensitive or confidential data from the hard disk before sending hardware off-site for maintenance.
- Do not use illegal copies or pirated copies of software. Use only purchased or licensed software.
- Refer to Using Software - A Guideline to the Ethical and Legal use of Software for Members of the University Community for more information.
- Make sure that any diskettes you bring into the university environment are free of computer viruses. Use a virus scan program before using the diskettes on your PC, especially if you are connected to a Local Area Network. Please contact the UTCNS Microcomputer Maintenance group at 978-1299 for more information.
- Use a power bar or other similar equipment with surge protection to protect your equipment and data against losses caused by sudden power fluctuations.
- If you experience static electricity problems in your office, install an anti static device such as an anti static mat and touch the mat BEFORE you touch your keyboard or computer.
- If you use your PC to create and process sensitive or confidential data, consider installing access controls software to prevent unauthorized access to your PC.
- Remove all sensitive or confidential data from diskettes before discarding them or using them again for storing new information. Use a utility like Norton "Wipe" to securely erase the data from diskettes.
- Use a special utility like Norton "Wipe" to securely erase data from a hard disk or a diskette.
- If your PC is connected to a Local Area Network or the mainframe computer, always remember to logout before leaving your workstation.

Section 9

Information Confidentiality & Privacy

Information and data owned by the University must be protected whether stored on a Personal Computer, Laptop computer on and off campus, or stored on removable media, such as CDs, diskettes, etc. University owned information and data must also be protected while it is being transmitted over public networks.

Best Practices

- Do not leave confidential or other sensitive documents out in the open or unsecured.
- Do not share or talk about confidential information to which you have access with unauthorized staff or other individuals who have no right to know about it.
- Dispose of confidential or sensitive information properly. Shred paper documents and carbon paper; erase files on magnetic media using Norton "WIPE" or similar utilities or by degaussing; grind Microfilm and Microfiche.
- Do not volunteer unnecessary information to anyone.
- Do not discuss security procedures such as alarm systems, etc. with unauthorized staff or other individuals who have no right to know about it.
- Report suspicious activity or unusual happenings to management.
- Make sure that all reports and files are locked away in a cabinet at the end of each day.
- Never provide copies of written correspondence, directories or manuals to people outside the University unless otherwise authorized to do so by management.
- Remember that confidential information may be as critical to the University as physical property.
- If you use your Personal Computer or Lap Top to create, store or process sensitive or confidential data, consider installing access controls software to prevent unauthorized access to your machine.
- Remove all sensitive or confidential data from diskettes before discarding them, giving them to someone else, or using them again for storing new information. Use a utility like Norton "Wipe" to securely erase the data from diskettes.
- Use a special utility like Norton "Wipe" to securely erase data from a hard disk before you send it or your PC for servicing.
- If your PC is connected to a Local Area Network or the mainframe computer, always remember to logout before leaving your workstation.
- Keep in mind that data traveling over Local Area Networks can be compromised. "Sniffers" can be used to monitor/capture LAN traffic.

Section 10

Browser Security

Did you know that your browser could be a security and privacy risk? You have probably heard of the various problems associated with web browsers. Browser security and privacy holes are many and range from cookies, java applets, JavaScript, ActiveX controls and just plain software bugs. These guidelines cover various Web browser security and privacy concerns in general and provide you with information that will enable you to choose how much protection you want to have when accessing the Internet with your browser.

About Cookies

A cookie is a small text file that is set by a web site and stored on your hard drive. The contents of the file is under the control of the web site and may contain information about you and/or your past and present surfing habits. You supply most of the information that a cookie gets about you. When you fill out a form that asks for your name and email address for example, that information may be stored in a cookie for future use. This is not necessarily a bad thing however. Cookies are most often used to customize your browser or for personalizing content delivery. In other words, if you go to www.yahoo.com and you choose to "Personalize" the page so that it shows your local weather and news, stock quotes, and entertainment, that information is stored in a cookie so that when you go back to the page all of your personalized settings are displayed for you. Cookies are sometimes used to track your browsing habits such as what sites you visited before and what sites you went to after the site that issued the cookie. This is often used for gathering statistics about the popularity of the site, market research and targeted advertising. A Web site can look at the cookie (only the site that issued the cookie can get access to this information) to see where you have been and where you are going so that the site can customize the banner ads that are displayed on your browser. You might notice when you go to a search engine like Yahoo or HotBot and type in a query, the banner ads that appear after you submit the search seem to be relevant to your search.

Controlling Cookkies

But what if you don't want any information about you to be collected by a web site? There are several ways to prevent cookies from being generated. The easiest way is to disable cookies in your browser options. By default, Internet Explorer and Netscape Navigator accept all cookies. However, you can set your browser to reject all cookies or accept only certain cookies.

To change Cookie settings in your favourite browser, follow the instructions below.

Internet Explorer

Click **Tools** from the menu. On the **Tools** click **Internet Options**. On the **Security** tab, choose **Custom Level**.

The **Security Setting** window is displayed.

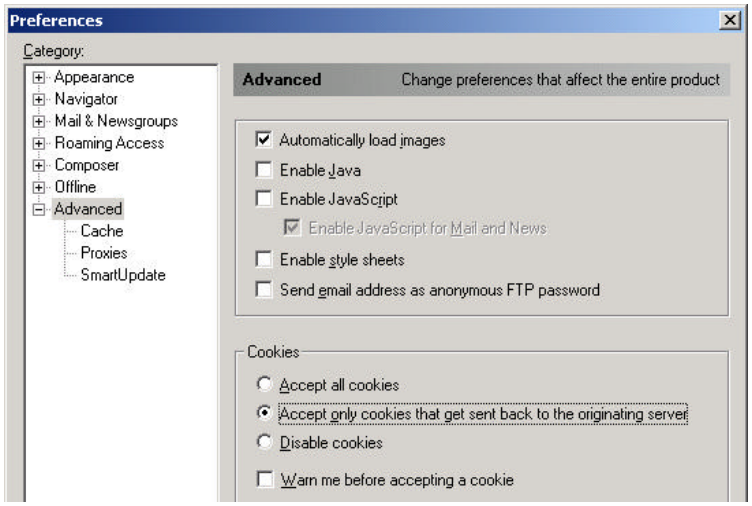
From here you can select "enable", which is the default, "disable", which will reject all cookies, or "prompt", which will prompt you whenever a cookie is about to be set.

You should use the “Prompt” option with caution however since you may end up spending a lot of time rejecting/ accepting cookies!

Netscape

Setting up cookies in Netscape is a bit different than in Internet Explorer.

Click on **Edit** from the Netscape menu and then choose **Preferences**. Once the Preferences window pops up, click on **Advance** to change the preferences that affect Netscape. There is a section dedicated to cookies and you can pick one of the four choices available to you.



Netscape offers one more option than Internet Explorer, **Accept only cookies that get sent back to the originating server.** This ensures that only the site that you are currently visiting will get the cookie data, and not some other third party, thus preserving some of your privacy.

Caution:

Keep in mind that if you disable cookies, you cannot save any custom settings on any Web site. Also, some Web sites won't work at all without cookies being enabled on your browser. For example, many sites that require you to login before accessing certain pages use cookies to enable the authentication process.

In terms of security, cookies are the least that you have to worry about. The more serious security problems are related to the use of Java, JavaScript, and ActiveX controls.

Security Issues Related to Java, JavaScript, and ActiveX

Java, JavaScript, and ActiveX controls are used by many sites to provide visitors with a more interactive experience. However, these controls pose one of the biggest risks to browser security. The reason is that Java and ActiveX are actually executable code that you download and run on your local computer. JavaScript is a scripting language that gets downloaded with an html page from a Web site.

ActiveX can be more dangerous than Java or JavaScript. The reason is that ActiveX can actually make system calls that can affect the files on your hard drive. With ActiveX controls, files can be created or overwritten and replaced with other files. Imagine the damage that could be done if your autoexec.bat were replaced with a different version. Many of the hostile ActiveX controls have been effectively blocked in Internet Explorer 5.01 and later versions.

Although JavaScript can be less destructive than Java or ActiveX, it can still pose some problems. It is relatively easy to create a local denial of service attack using JavaScript. Known security exploits of these controls have been fixed by Netscape and Microsoft. The important thing is to make sure that you have applied all security patches released by the vendors of the browser you are using. This holds true for any software you run on your computer whether it is a browser, or Microsoft Excel or Power Point.

You should check for security patches on vendor sites to make sure that your software is up to date.

For Netscape, visit the "Current" Security Notes page at http://home.netscape.com/security/notes/index.html and the "Previous" Security Notes page at http://home.netscape.com/security/notes/previous/index.html.

For, Internet Explorer, go to the security updates page at http://www.microsoft.com/windows/ie/download/default.htm.

Making Your Browser More Secure

You can protect yourself from ActiveX, Java, and JavaScript problems though. It is easily done with either Internet Explorer or Netscape Navigator.

Internet Explorer

Internet Explorer makes it easy for you to set the security level that you wish to use. You do this by going to the **Tools** menu and choosing **Options**. From the **Options** window select the **Security** tab. A window will pop up and will list the four content zones for which you can specify security settings. Each zone can be set to one of four security settings.

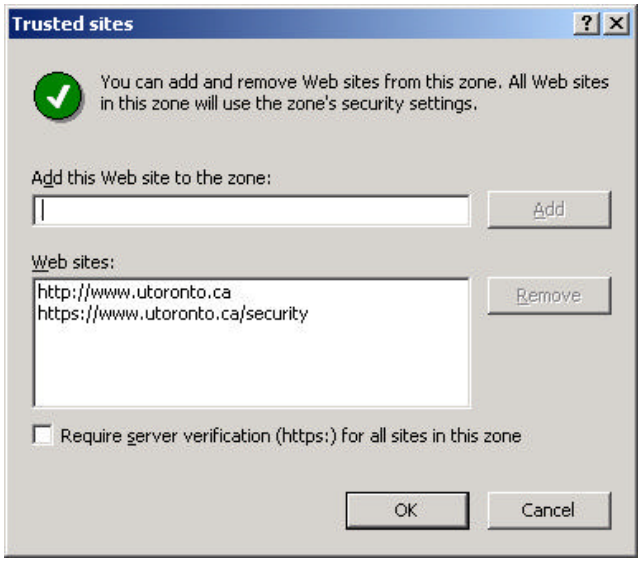
To set the security settings for a particular zone, highlight the zone. Then choose the **Default Level** for that zone or customize the security settings.

The default setting for the Internet Zone is **Medium**. This setting gives you the most browser functionality while still prompting you about possible unsafe content. The **Medium** setting disallows all unsigned ActiveX

controls. **Medium Low** will give you the same functionality but you will not be prompted before content is downloaded. The **Low** setting allows all content to come through and gives you no security at all. **High** blocks everything - cookies, ActiveX, and Java - but your browser functionality will suffer as a result.

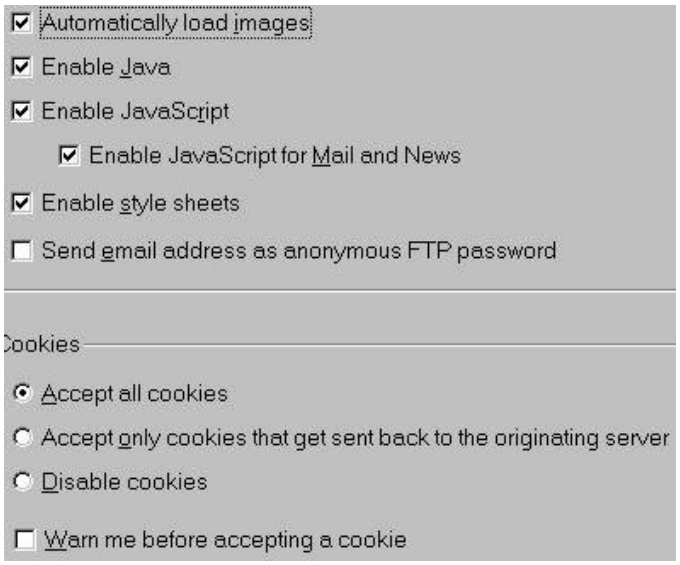
Keep in mind that some sites will not work without Java or JavaScript being enabled. It's all a matter of balance and need.

If you wish, instead of using the slider to set your browser security, you can customize the settings for a particular zone yourself. By clicking on the **Custom level…** button, you can set up your own custom level of security. For example, you can set the zone level to **High** but enable cookies manually so that you don't lose whatever custom settings you may have for certain sites.



You can also specify the actual sites that fall into the **Local intranet**, **Trusted sites** and **Restricted sites** zones. The example to the left shows the University of Toronto home page and the Computer Security Administration page as Trusted sites.

For sites in the **Trusted Sites** zone, you may also choose to require server certificate verification for all sites included in the zone. However, this is an all or none option. If you are going to include sites that do not require server certificate verification, then do not check off the **Require server certification (https:) for all sites in this zone** option.



Netscape Navigator

Netscape Navigator's security settings are a little easier to set up, but you have far fewer options to choose from. To set up Netscape's security go to the **Edit** menu and choose **Preferences**. Click on **Advanced** in the left frame and you will be presented with a list of security options in the right frame. The only available options for ActiveX, Java, and JavaScript are **enable** or **disable**. There is no option for prompting. The **prompt** option is only available for cookies.

The default in Netscape is to accept all Java, JavaScript, and cookies. You have no option to accept or reject ActiveX, but since Netscape does not support ActiveX, you don't have to worry about it.

The default security setting for Netscape Navigator is **Low**. Changing the setting is easy. With Netscape you don't have the level of customization that Internet Explorer allows.

When you enter a secure site, in other words, a site that sends your information in encrypted form, both Internet Explorer and Netscape navigator give you a visual indicator that the site is in fact secure. With IE you will see a little closed padlock in the lower right hand corner of the browser window. In Netscape a similar padlock can be seen in the lower left hand corner of the browser. It is important that you verify that a site is secure before you send any information of a confidential nature over the Internet. Never send credit card information or any other confidential information unless the site offers encryption to protect the information.

Browser security has come a long way in the last few years. They have gone from being extremely insecure applications to applications that offer customizable security. But as long as there are "hackers" out there, new security holes will be found and exploited. Remember, always practice save surfing!

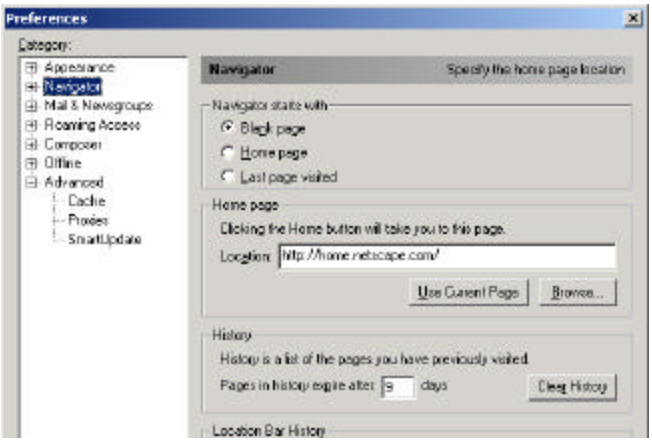
Terminating Sessions

When you access a web site, your browser saves page images in cache. Cache is used by the browser to store images of pages you have visited. Web browsers do this in order to speed up access. Web browser also maintains a history of sites you have visited. If you do not clear the cache and history files, anyone can view the information you have accessed simply by using the back button on the browser.

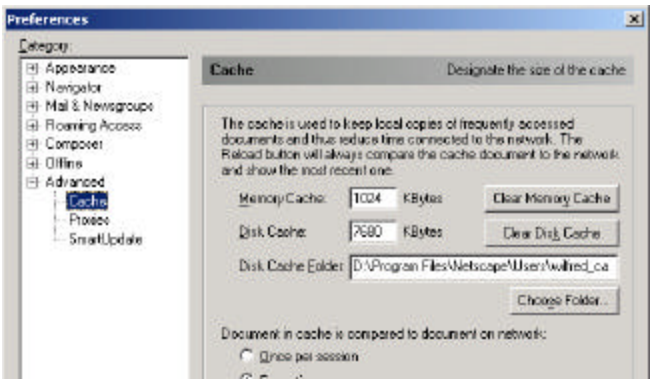
Browsers have facilities that let you clean the cache and history lists.

Netscape History and Cache Cleanup

In Netscape, click on **Edit** and choose **Preferences**. Choose **Navigator** from the left frame. You can specify when pages in the history list expire be entering the number of days. You can also clear the history list by clicking on **Clear History**.



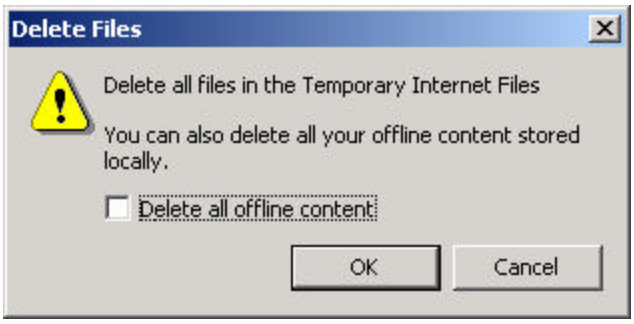
Browsers use two types of cache: Memory Cache and Disk Cache. You can clear Memory and Disk cache in order to ensure that no one else who has access to your computer can view information that you have accessed using the browser. To clear cache, click on **Edit** and choose **Preferences**. Choose **Advance** from the left frame and expand the list by clicking on the plus sign. Then click on **Cache**. To clear cache, click on **Clear Memory Cache** and **Clear Disk Cache**.



Internet Explorer History and Cache Cleanup

On the **Tools** menu in Internet Explorer, click **Internet Options**. On the **General** tab, click **Settings**. To delete temporary Internet files (cache) click **Delete Files…** To clear history, click **Clear History.**

To clear **Temporary Internet Files**, click **Delete Files…** and when the **Delete Files** window is displayed, click **OK**.



Malicious Code

With the number of computer viruses and worms increasing on a daily basis, it is important that you have a virus-scanning program running on your computer. It is also important to make sure that the program is updated regularly so that it is able to detect new viruses and other malicious code.

A few things to keep in mind:

- Be careful of e-mail attachments since many viruses and worms are spread as e-mail attachments. If you are not certain of the contents and source of any attached files, you're better off to just delete the message.
- Make sure that you update your virus-scanning program regularly. If you don't, you risk getting your computer infected and spreading viruses to colleagues. An out-of-date virus program can give you a false sense of security.
- If your virus-scanning program has an active monitoring feature, make sure that it is turned on.
- If your computer does become infected, contact your network administrator.

Confidential Information

When using the Internet to view and transmit confidential information, make sure that you have a “secure” connection to the site you’re visiting. When you are finished, clear the Cache and History files right away.

Section 11

Reporting Security Incidents

(Placeholder)

Section 12

Institutional Users

Network Security Considerations

(Placeholder)

Open Source Firewall

Overview

A firewall is one of the tools used to secure a computer network. A firewall can prevent unwanted access to departmental systems while preventing local systems from attacking systems on other networks (on the other side of the firewall). Unfortunately, firewalls (like other security systems) require on-going monitoring of their performance to ensure that they do not unnecessarily restrict access to important computer resources while preventing unwanted access.

The open source firewall developed by CNS is based on a widely accepted technique called packet filtering. Each packet going through the firewall is evaluated against rules set by the administrator and is either passed along or rejected. The firewall logs its activities to help the administrator understand whether there has been an attempted attack. To reduce administrative costs this firewall can be administered locally (from the console) or remotely (using a secure connection). It can also be configured to watch a particular computer for new rules.

No firewall can prevent malicious people from exploiting known vulnerabilities in software (as buffer overflow exploits and worms do). This firewall is no different. What it does is to ensure that the traffic entering and leaving the secured LAN is talking to the correct applications on the correct computers.

A crucial point about this firewall is that it uses a low-level approach to configuration; the administrator must analyze his or her needs at the level of ports and packet types in order to choose the required permissions. This is a two-edged sword: it results in a relatively inexpensive product but it requires a certain amount of expertise to administer. Commercially available products can simplify some configuration task by allowing the administrator to simply choose from a set of applications to be allowed/disallowed but these products typically cost many thousands of dollars. Adding this functionality to the CNS developed firewall would be hugely expensive.

The open source firewall available to all departments on campus. CNS also provides a service to assist departments in performing security evaluations of their networks.

Security Perspective

Current Practice:

- Departments routinely maintain sensitive and confidential information on Internet connected computers.
- Departments routinely deploy business systems that are critical for the day-to-day operations of the unit on Internet connected computers.
- The built-in security features of typical departmental computers are inadequate to protect them from mischief and malice when connected to the Internet.

The Threats:

- Theft or corruption of important data. The consequences of compromised data can range from a loss of staff and student productivity, to public embarrassment (and liability).
- Denial of service. All computer systems have vulnerabilities that can be exploited to cause the computer to work poorly or not at all. Software is widely available on the Internet that exploits these vulnerabilities, and these programs are routinely directed at University computers.

How a firewall helps:

- Any requests from non-trusted hosts can be rejected; this technique can be used to provide a simple level of confidentiality, and it can be used to prevent Denial of Service attacks, and other known intrusion techniques.
- Often it is necessary to allow traffic (e.g. SMTP, IMAP) from non-trusted hosts. In these cases, the firewall will not prevent certain types of attacks; for instance, it won't protect against viruses in e-mail, nor will it stop atacks that use buffer overruns.

Service Perspective

- Successful firewall deployment and operation requires a very precise set of technical networking skills and a concerted effort to remain current on the "state of the art". This is necessary because of the technical complexity of the problem, the sophistication of the attacks being crafted, and the evolving nature of attacks.
- Departments' capacities to deploy and operate firewalls vary through the university.

Departments with firewalls

Departments with firewalls have engaged in a self-assessment, which determined the need to protect their systems. As the complexity of the problem and the sophistication of the threats increases, many of these departments are experiencing unacceptable costs in terms of providing the level of technical support within their own organization or via a commercial service provider. Organizations experiencing this are interested in avenues that consolidate security support (thereby reducing individual costs).

Departments without firewalls

In many areas of the university, some departments with the competence to deploy firewalls have not done so, perhaps based on a perception that:

- Their systems and data are not a risk.
- Firewalls unacceptably compromise academic freedom.
- Installing/maintaining a firewall would be too great an additional workload.

These perceptions may be quite accurate, in that they are based on a thorough understanding of the values and risks to the department, and because most system administrators review their environment periodically, with a view to responding to the increasingly hostile attacks that come from the Internet.

In departments without the competence to deploy firewalls there is often:

- A lack of awareness of the risk their systems are exposed to
- A lack of expertise to carry a project forward
- The perception that the cost of commercial firewall products is too much

Deployment

Hardware Requirements

At a minimum, the firewall machine should be equivalent to a Pentium II, with 64 Mb of RAM, a 5Gb hard drive, and 2 PCI NICs; in addition, the hardware must be supported by FreeBSD (see http://www.freebsd.org/relnotes/4-STABLE/hardware/i386/). Required processor speed will be dependent on IP traffic. Required hard drive capacity will be dependent on the desired degree of log retention.

Host Setup

A step-by-step Installation Guide is provided with the distribution package; this covers the installation of both FreeBSD and the firewall software itself. The firewall software installation has an option that allows the creation of a second firewall machine as a hot spare.

The installation can usually be accomplished in less than two hours. The installation should pose few problems, because of the straightforwardness of the process itself, and because of the completeness of the Installation Guide.

The default filtering rules allow all traffic to pass between the "inside" and the "outside". All access to the firewall itself is blocked, except for SSH access through a port, and via hosts, chosen during the install; this SSH connection is used for remote administration.

Operations

Administrative Functions

There are several classes of function available:

- System configuration and control, rebooting, etc.)
  - System summary, IP settings, date and time
  - Reboot, shutdown, exit
- Group management (i.e. Groups of IP nos.)
  - Show, edit, add, delete groups
- Permissions and rules (see Creating new filter rules)
  - Show, add, delete permissions
  - Update rules (after changing permissions)
  - Show rules
- Importing rules (see Creating new filter rules)
  - Add, delete, view URLs for normal rules
  - Add, delete, view URLs for emergency rules
- Logs and mail management
  - Review or watch current or archived log (complete)
  - Review or watch current or archived (denials only)
  - Manage email addresses (for recipients of notifications)
  - Send log or archive to recipients (entire or summary)
  - View log summary
- Maintenance
  - Save configuration to remote site, floppy, or locally
  - Restore configuration from remote site, floppy, or locally
  - Configure ports for sshd, snmpd
  - Manage maintenance list (tracking)

Administrative Interface

The interface consists of a set of text menus; these have built-in help, activated by entering either an empty response or question mark.

Remote Administration

The firewall can be configured to accept SSH connections from specific hosts, so that an administrator can log in and make changes.

Logs, Alerts, Reporting

All traffic is logged; log entries for outbound traffic can be marked selectively, using the RECORD permission. Logs are rolled and compressed daily, and logs and/or summaries can be e-mailed to specified addresses.

Creating new filter rules

The Administrative interface is used to define permissions which control traffic flow, based on IP address (or group of IPs) and port number; there are four types of permission, each of which is a macro which expands to a set of IP firewall rules.

The defined rules may be modified (presumably to handle temporary situations) by downloading (importing) another set of rules from a specified URL. These can be normal rules, which augment those already defined, or emergency rules, which replace them.

The syntax and semantics of the permissions is beyond the scope of this report; in fact, there was a consensus that it would be difficult for an inexperienced administrator to fashion a set of permissions that would achieve a particular desired effect without assistance. It should also be pointed out that the approach used in configuring this firewall is a low-level one. For instance, one cannot just pick from a set of applications to be allowed; one must know which ports and packet types an application uses, and establish permissions based on them.

Effectiveness

Failure recovery

If a second machine has been configured as a hot spare, it will automatically take over if the primary fails, and become the primary; when the old primary is re-started, it becomes the hot spare. Rule changes made on the primary are automatically mirrored on the hot spare. This facility was felt to be a valuable and convenient feature.

If there is no hot spare and the primary fails, connectivity between inside and outside can only be restored by bypassing the firewall.

Performance

Throughput

The effective performance can be measured by testing with the firewall in and out of the network path. No quantitative measures of this sort have been made to date; however, a comparison of the throughput of several workstations, only one of which was behind a firewall, showed no apparent differences. The pilot projects showed that the firewall is transparent to users.

Security

Firewalls using this technology have been in use, here and around the world, for years. They have stopped known attacks and prevented unauthorized probing of the secured network. No strenuous deliberate attacks have been carried out against this firewall; however, the regular sweeps have disclosed no vulnerabilities.

By way of example:

- The installation of the firewall on the Simcoe Hall network eliminated attacks (LPR and others) which had previously been experienced.
- While some 60 servers on campus were infected by the Code Red Worm, both the Simcoe Hall network and the CANS network (also behind one of these firewalls) were unaffected, even though the servers there did not have the protective patch applied.

Security Assessments

Upon request, the Computer Security Administration Group of CNS will assist departments with a security assessment of their computing environment. This process includes the following steps:

- **Information Gathering** - The department should gather all pertinent information to help with he assessment. This should include:
  - Network Topology
  - Hardware & Software Inventory
  - List of Services provided
  - Information on any security incidents
- **Preliminary Review** - Computer Security Administration will meet with a representative of the department to conduct a preliminary review of the department's computing environment
- **Conduct Assessment** - Computer Security Administration will enlist expertise from within CNS to assist the department in conducting the assessment of their computing environment
- **Draft Recommendations** - Computer Security Administration will assist the department representative with recommendations for enhancing the security of the department's computing environment
- **Draft Assessment Report** - An assessment report is drafted and distributed to affected parties

Local Area Network security guidelines are available at http://www.utoronto.ca/security/LAN.htm
Please contact us at security.admin@utoronto.ca for more information on this service.

Getting The Open Source Firewall

The Open Source Firewall is available via anonymous FTP from:

ftp://cns.utoronto.ca/pub/filbert/

If you run into any problems, please contact: filbert@cns.utoronto.ca

The directory at the FTP site includes the following files:

- README
- Install - firewall installation guide
- feb.tar - the firewall software itself
- FreeBSD_install_CD-ROM.iso - image of the FreeBSD install CD

Consulting Services

(Placeholder)

Section 13

Reporting Security Incidents

All computer security incidents should be reported to Computer Security Administration. This enables Computer Security Administration to monitor and investigate computer security incidents involving University computers and users. Computer Security Administration is able to draw upon other resources within Computing & Networking Services to protect University networks and systems in order to minimize disruption of services caused by such incidents.

Computer Security Administration also keeps tracks of the number and type of security incidents in order to provide regular reports to senior management on the state of University networks.

What sort of incidents should be reported?

- Hacking attacks
- Unauthorized access and use of computing resources
- Harassment and threats using e-mail
- Denial of Service attacks
- Malicious code (Viruses, worms, etc.)

To whom should incidents be reported?

Generally speaking, incidents should be reported through your Local Area Network (LAN). If you do not have a LAN Administrator or know who your LAN Administrator is, you may contact Computer Security Administration directly by sending e-mail to **security.admin@utoronto.ca**.

How should incidents be reported?

In order to ensure that Computer Security Administration is able to investigate incidents, it is critical that any system logs (in case of hacking attacks or unauthorized access) and e-mail headers (in case of incidents involving the use of e-mail) are saved.

Detailed logs should include information such as date and time of attack, IP numbers, protocols used, etc.

Since the forging of e-mail addressed is quite easy to do, it is important that e-mail headers are made available in order to determine the origin of an e-mail message. If you are using MS Outlook or Outlook Express, you can view and copy the e-mail headers of a message as follows:

- Open the message and click on **View**
- Choose **Options** from the drop-down menu
- The system will open a window which include the Internet headers
- Highlight the headers using your mouse and then right click and **Copy** the headers

Section 14

References

Computer Security Administration
www.utoronto.ca/security

- Security Guidelines
- University of Toronto Codes
- Patches & Alerts

Section 15

Glossary

Cookies

A cookie is information that a Web site puts on your hard disk so that it can remember something about you at a later time. Typically, a cookie records your preferences when using a particular site. Using the Web's Hypertext Transfer Protocol (HTTP), each request for a Web page is independent of all other requests. For this reason, the Web page server has no memory of what pages it has sent to a user previously or anything about your previous visits. A cookie is a mechanism that allows the server to store its own information about a user on the user's own computer. You can view the cookies that have been stored on your hard disk (although the content stored in each cookie may not make much sense to you). The location of the cookies depends on the browser. Internet Explorer stores each cookie as a separate file under a Windows subdirectory. Netscape stores all cookies in a single cookies.txt file.

Denial Of Service

On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

Domain

On the Internet, a domain consists of a set of network addresses. This domain is organized in levels. The top level identifies geographic or purpose commonality (for example, the nation that the domain covers or a category such as "commercial"). The second level identifies a unique place within the top level domain and is, in fact, equivalent to a unique address on the Internet (an IP address). Lower levels of domain may also be used.

DSL

DSL (Digital Subscriber Line) is a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. xDSL refers to different variations of DSL, such as ADSL, HDSL, and RADSL. Assuming your home or small business is close enough to a telephone company central office that offers DSL service, you may be able to receive data at rates up to 6.1 megabits (millions of bits) per second (of a theoretical 8.448 megabits per second), enabling continuous transmission of motion video, audio, and even 3-D effects.

Driver

A driver is a program that interacts with a particular device or special (frequently optional) kind of software. The driver contains the special knowledge of the device or special software interface that programs using the driver do not.

Encryption

	Encryption is the conversion of data into a form, called a ciphertext that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.
Ethernet	Ethernet is the most widely-installed local area network (LAN) technology.
Firewall	A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.
Gateway	A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.
Hacker/Hacking	Hacker is a term used by some to mean "a clever programmer" and by others, especially journalists or their editors, to mean "someone who tries to break into computer systems." Hacking is the act of breaking into a computer system for the purpose of using the resources of that system for unauthorized purposes including attacking other systems on the network, gaining access to information on that system, or making unauthorized changes to files and data on that system.
IP	The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.
IPsec	IPsec (Internet Protocol Security) is a developing standard for security at the network or packet processing layer of network communication.
NDIS	NDIS (Network Driver Interface Specification) is a Windows specification for how communication protocol programs (such as TCP/IP) and network device driver should communicate with each other.
NIC	A network interface card (NIC) is a computer circuit board or card that is installed in a computer so that it can be connected to a network.
Packet	A packet is the unit of data that is routed between an origin and a destination on

	the Internet or any other packet-switched network
Personal Firewall	A personal firewall (sometimes called a desktop firewall) is a software application used to protect a single Internet-connected computer from intruders. Personal firewall protection is especially useful for users with "always-on" connections such as DSL or cable modem. Such connections use a static IP address that makes them especially vulnerable to potential hackers. Often compared to anti-virus applications, personal firewalls work in the background at the device (link layer) level to protect the integrity of the system from malicious computer code by controlling Internet connections to and from a user's computer, filtering inbound and outbound traffic, and alerting the user to attempted intrusions.
Port	On computer and telecommunication devices, a *port* (noun) is generally a specific place for being physically connected to some other device, usually with a socket and plug of some kind. Typically, a personal computer is provided with one or more serial ports and usually one parallel port. The serial port supports sequential, one bit-at-a-time transmission to peripheral devices such as scanners and the parallel port supports multiple-bit-at-a-time transmission to devices such as printers.
Protocol	In information technology, a protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection. There are hardware telephone protocols. There are protocols between each of several functional layers and the corresponding layers at the other end of a communication. Both end points must recognize and observe a protocol. Protocols are often described in an industry or international standard.
Spam	Spam is unsolicited e-mail on the Internet. From the sender's point-of-view, it's a form of bulk mail, often to a list culled from subscribers to discussion group or obtained by companies that specialize in creating e-mail distribution lists. To the receiver, it usually seems like junk e-mail. It's generally equivalent to unsolicited phone marketing calls.
Spoof	To deceive for the purpose of gaining access to someone else's resources (for example, to fake an Internet address so that one looks like a certain kind of Internet user)
Spyware	On the Internet, spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program. Data collecting programs that are installed with the user's knowledge are not, properly speaking, spyware, if the user fully understands what data is being collected and with whom it is being shared.
TCP/IP	TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network. When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.
Trap Door	A hole in the security of a system deliberately left in place by designers or

	maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers. Syn. trap door; may also be called a `wormhole'.
Trojan	In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.
Virus	A virus is a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event. A virus is often designed so that it is automatically spread to other computer users. Viruses can be transmitted as attachments to an e-mail note, as downloads, or be present on a diskette or CD. The source of the e-mail note, downloaded file, or diskette you've received is often unaware of the virus. Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances cause their code to be executed by the computer. Some viruses are playful in intent and effect ("Happy Birthday, Ludwig!") and some can be quite harmful, erasing data or causing your hard disk to require reformatting.
VPN	A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. Tunneling is using the Internet as part of a private secure network. The "tunnel" is the particular path that a given company message or file might travel through the Internet.
Worm	A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.