Thin Client Virus Vulnerability Analysis

Introduction

Enterprise computing networks require effective protection against computer viruses and other security issues. These security breaches can result in costly service calls, user downtime and loss of business-critical data. When compared to the traditional unmanaged PC network model, the HP thin client computing model yields a less vulnerable segregated approach to computing with substantially better recovery time, while minimizing total cost of ownership (TCO).

According to an ICSA Labs virus analysis[1], the average downtime lost during an encounter was 23 person days. This down time accounted for data loss recovery and patching the connected network servers and PCs. With the HP thin client computing model, your exposure to virus attack on the thin client system is over 80% less than a standard Windows PC. This means that your user will experience significantly less downtime due to security vulnerabilities than a PC user. In addition, since no user data resides on the thin client, there is no risk of user data loss on the thin client. Finally, if a thin client's image is compromised or corrupted, the recovery time is typically measured in minutes instead of hours.

Furthermore, the HP thin client computing model utilizes PC blades and/or servers located in the data center. These centralized devices can be protected and monitored more easily with centrally managed virus and firewall tools. Compromised resources can be quickly taken offline, corrected, or recovered faster and cheaper than distributed PC resources.

This model also allows a user's data to be segregated and centralized for easy backup and recovery, ensuring a higher level of service and security for your users at a lower TCO than distributed PC resources.

At HP, we realize security and TCO are important factors in enterprise computing. A Fall 2003 EDC survey showed more than eight out of every 10 enterprises suffered a security breach as a result of malicious code. As a result, more than half the enterprises are increasing their IT security budgets. HP believes the thin client computing model is an effective solution for the security conscious enterprise.

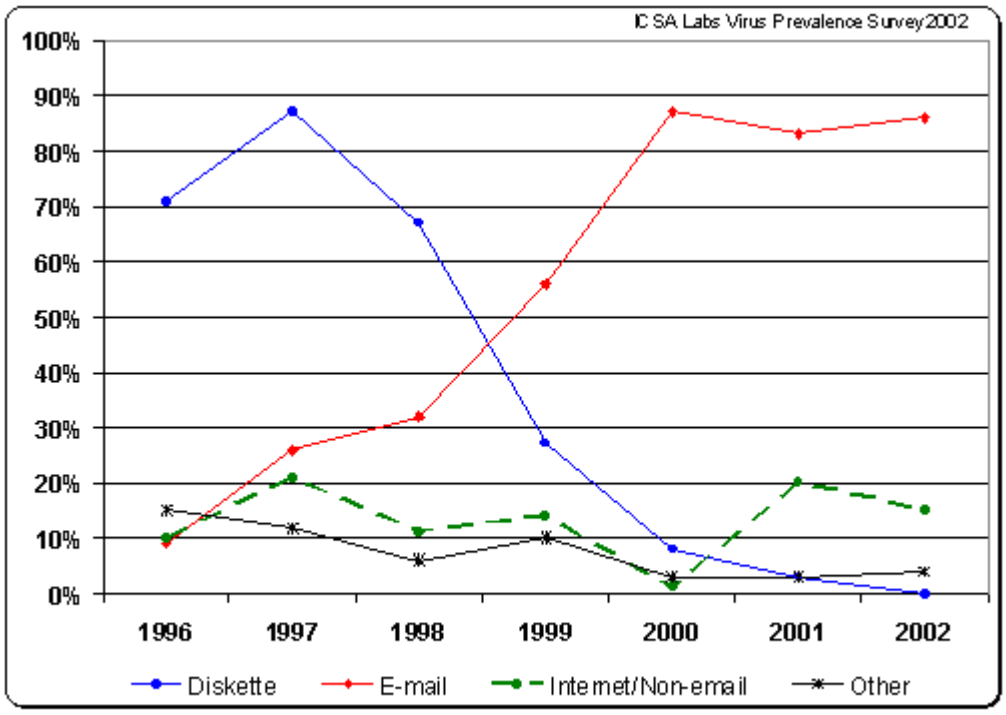
1.ICSA Labs 8th Annual Computer Virus Prevalence Survey

Virus Vulnerabilities, Encounters, and Impact

The following graph depicts security vulnerabilities experienced by actual enterprise customers as surveyed by ICSA Labs for the years 1996 through 2002. The second graph contains the most vulnerable technologies as perceived by the enterprises surveyed in 2003 by EDC. The graphs illustrate a strong correlation between the actual occurrence of each vulnerability and its associated technology in an enterprise. For example, 86% of the encounters experienced in 2002 were email related and according to EDC, 50% of the enterprises surveyed in 2003 perceive email as their most vulnerable technology.

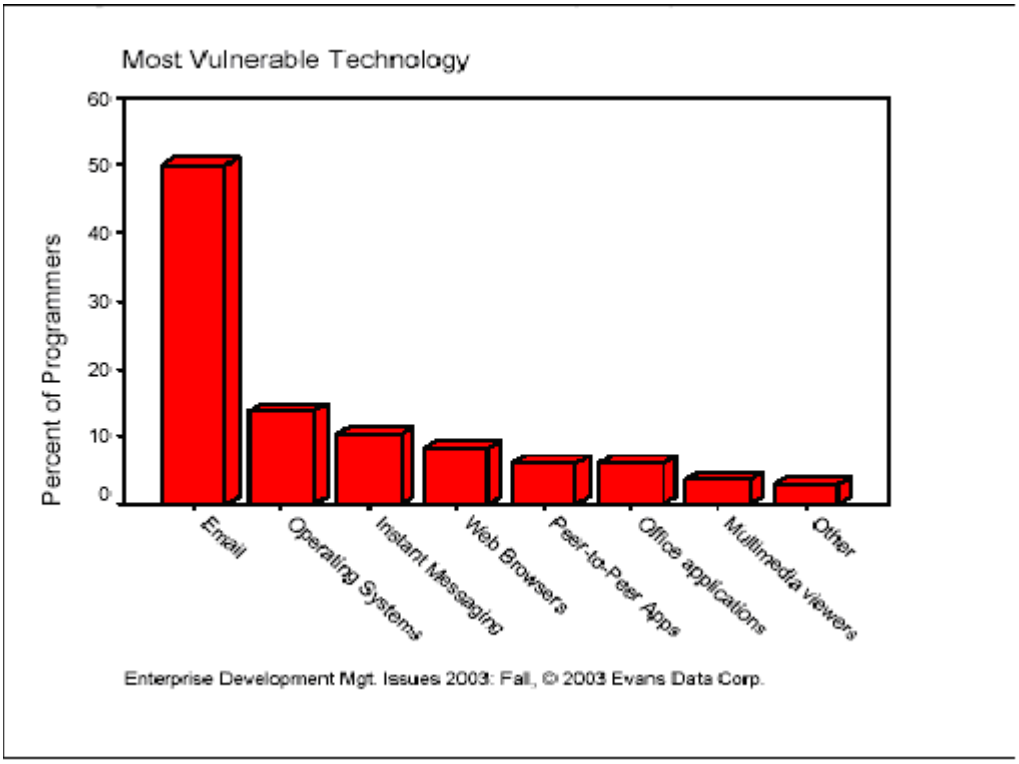
The third graph illustrates the impact of these vulnerabilities on the enterprises surveyed by ICSA in 2002.

Virus Encounter Vectors

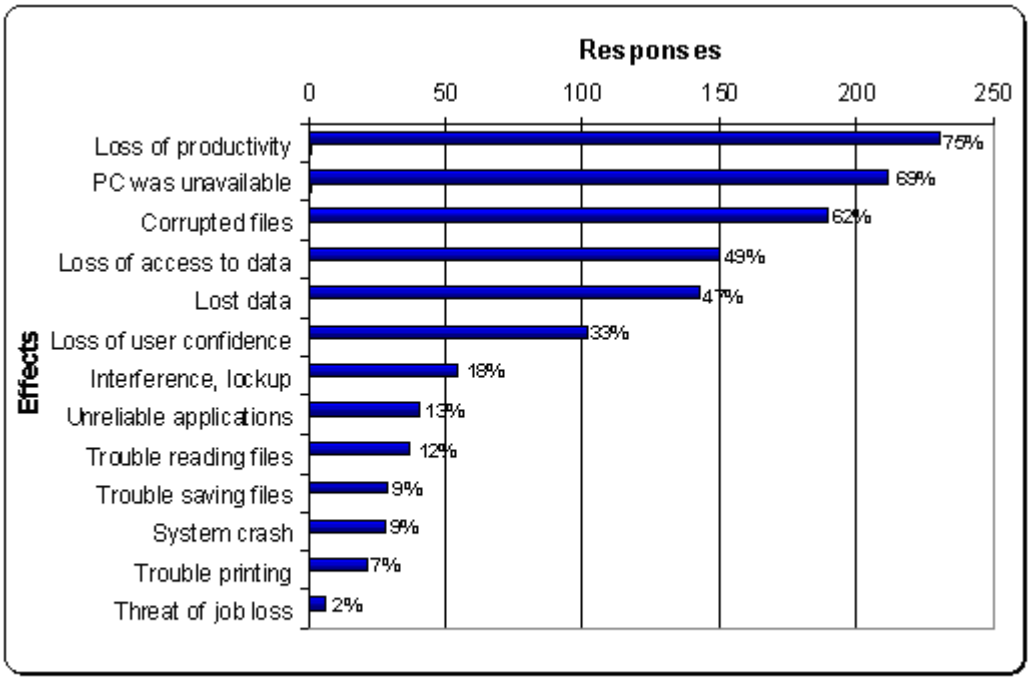


Note: "Other" in this graph represents unknown vectors and 3rd party/freeware software distribution.

Technology Vulnerabilities



Impact of Client Computing Vulnerabilities



HP Thin Client Response to Vulnerabilities

Given the data in the previous section, the thin client computing model substantially reduces the likelihood that the client device will encounter a vulnerability as compared to a standard PC. It also centralizes an enterprise's most vulnerable technologies in the data center where they can be most effectively controlled and protected from exposure at the user level.

The following table summarizes the previous data and shows that thin clients are substantially less susceptible to the virus vectors and are exposed to fewer of the perceived vulnerable technologies than a standard PC. The following sections detail these areas as related to the thin client computing model.

Technology	**Personal Computers (PC)**		**Thin Clients (TC)**	
	2002 Encounter Vector Experienced[a]	**2003 Perceived Vulnerability[b]**	**2002 Encounter Vector Experienced[a]**	**2003 Perceived Vulnerability[b]**
Email	86%	49.9%	0%	0%
Operating System	0%	13.5%	0%	13.5
Instant Messaging	0%	10.1%	0%[c]	0%[c]
Web Browser	4%	8.1%	0%[c]	0%[c]
Peer-to-peer Apps	11%	6%	0%	0%
Office Applications	0%	6%	0%	0%
Multimedia Viewers	0%	3.6%	0%[c]	0%[c]
Other[d]	4%	2.9%	0%	0%
Total	105%	100%	0%	13.5%

a.ICSA Labs Virus Prevalence Survey 2002
b.Enterprise Development Mgt. Issues 2003: Fall, © 2003 Evans Data Corp.
c.This vulnerability is zero only if this component is not installed on the thin client device
d.Other in this table represents unknown vectors and 3rd party/freeware software distribution

Diskette/Removable Media

The intrusion of viruses from diskettes has declined significantly over the years and does not appear to be a significant vulnerability point. Still, a small percentage of virus encounters do occur via CD-ROMs and

other removable media, typically when infected retail software is installed. Thin clients are predominantly deployed with no local removable drives such as CD-ROMs, diskettes, or hard drives.

Email/Office applications

With thin clients, users execute their email and office productivity applications on centralized servers and/or blade PCs. These applications and their associated data execute only on the server/blade. The user interface for these applications is rendered locally on the thin client through the Terminal Services Remote Desktop Protocol (RDP) or the Citrix® Independent Computing Architecture (ICA®) protocol. This means any virus or vulnerability introduced through your email/office or other remote applications typically affect the server/blade and not the thin client.

Additionally, the administrator has total control over the crucial applications and data on the servers or blade PCs, and can readily manage and deploy virus and firewall protection to these centralized systems. While these backend systems are at risk, applying patches or hot-fixes to centralized computing resources is more cost effective and takes less time than it does for standalone PC systems.

Web Browser/Internet/Non-email/Peer-to-Peer

These vectors and technologies are a growing concern. The majority of infection occurs through infected/malicious code that is downloaded or shared via these technologies. Security holes in internet browsers are reported frequently. Browser-related intrusions are centered on JavaScript, Java Applets and Active X.

The thin client model addresses these exposures in several ways. First, peer-to-peer applications and many of the internet and non-email web services are typically not deployed on thin clients. The best thin client strategy is to deploy only what you need to achieve your business goals. Second, user initiated file downloads and sharing typically occur at the server/blade PC level and not on the thin client itself. The thin client typically does not provide the user with the space and access rights to support this. For example, on HP XPe thin clients, the Enhanced Write Filter (EWF) prevents permanent modifications (writes) to the contents of the system's flash. Finally, the internet browser is an optional feature on the HP thin clients. It can be removed to ensure a more secure environment.

Operating System

Compared to a standard PC operating system, embedded operating systems are substantially smaller, providing less surface area to attack. Also, it is usually easier to configure an embedded OS to have fewer services that can be exploited than it is for a standard operating system. Advantages of the operating system will differ based upon the embedded OS chosen. Different operating systems are targeted at different rates and inherently have unique vulnerabilities. For example, CE .NET is substantially smaller and lighter than XPe or XP and is not targeted aggressively.

The following is a comparison of operating systems and their exposure on HP systems to the most exploited vulnerabilities of 2003 as listed by TruSecure®[1]. As compared to a standard Windows PC,

1.Wildtrends 2003: A Look at Virus Trends in 2003 and a Few Prediction for 2004; A TruSecure® Whitepaper

only two (MS03-026 and MS03-007) or around 22% these nine most exploited vulnerabilities were relevant to the HP XPe thin client. Patches for both are included in the image.

Number of Viruses	Exploited Vulnerability Number	Exploited Vulnerability Name
28	MS01-020	Incorrect MIME Header Can Cause IE to Execute Email Attachment
16	MS00-072	Share Level Password
6	MS03-026	Buffer Overrun In RPC Interface Could Allow Code Execution
3	MS99-032	Scriptlet.typelib/eyedog
2	MS00-075	Microsoft VM ActiveX Component
1	MS99-042	IRFRAME ExecCommand
1	MS00-043	Malformed Email Header
1	MS00-046	Cache Bypass
1	MS03-007	Unchecked Buffer in Windows Component

In addition to being a smaller target, HP's thin client XP embedded OS contains an Enhanced Write Filter (EWF) preventing damage to the local file system and its OS files. The EWF protects the contents of the media by redirecting all the writes to a temporary virtual memory location. These writes are lost when the system is shutdown or restarted. Finally, none of these vulnerabilities were relevant to the HP CE .NET thin client. CE .NET is significantly smaller than XPe and is not a targeted operating system.

Instant Messaging

2003 saw a rise in viruses that infected devices via instant messenger (IM) clients. The proliferation of IM clients and greater acceptance of their use in corporate settings will continue to increase the attractiveness of this vulnerability for virus infections[1]. Instant messenger is an optional component for the HP thin client and can be removed to ensure the most secure environment.

Multimedia Viewers

This technology is a growing concern for security conscious network administrators. The majority of infection occurs through infected/malicious code that is downloaded or shared via the internet. Security holes in internet Media Player have also been reported. Media Player-related intrusions are centered on requests and downloads of media files and skins. Media Player is an optional component for the HP thin client and can be removed to ensure the most secure environment.

1.Wildtrends 2003: A Look at Virus Trends in 2003 and a Few Prediction for 2004; A TruSecure® Whitepaper

Thin Client Firewall

A key component to ensure the most secure computing environment is a firewall. HP offers the Microsoft Internet Connection Firewall as an add-on. If one of your systems on the network is compromised by malicious code, the firewall will help prevent your thin client from infection. Additionally, a firewall will help prevent external attacks from reaching your system, protecting against intruders infecting the thin client with malicious code.

The following sections show how to enable the Internet Connection Firewall feature to provide Internet security for your HP Compaq t5700 thin client. This paper also discussed how to disable the Internet Connection Firewall feature, which may help in troubleshooting some applications that do not function as expected behind a firewall.

The Internet Connection Firewall can be downloaded from:

http://h18007.www1.hp.com/support/files/ThinClients/us/download/20070.html

What is Internet Connection Firewall and How Does it Work?

Internet Connection Firewall is software that can set restrictions on the information that is communicated between a computer network and the Internet. Internet Connection Firewall is recommended for any Microsoft Windows XP-based computer that is connected directly to the Internet.

Internet Connection Firewall is a "stateful" firewall. A stateful firewall is one that monitors all aspects of the communications that cross its path and examines the source and the destination address of each message that the firewall handles. To prevent unsolicited traffic from the public side of the connection from entering the private side, Internet Connection Firewall keeps a table of all the communications that have originated from the computer that is running Internet Connection Firewall.

Communications that originate from a source outside the computer that is running Internet Connection Firewall, such as from the Internet, are dropped by the firewall unless an entry is created on the Services tab to permit passage. Instead of sending notifications about activity, Internet Connection Firewall silently discards unsolicited communications. This stops common hacking attempts such as port scanning. Such notifications might be sent frequently enough to become a distraction. Instead, Internet Connection Firewall can create a security log to view the activity that is tracked by the firewall.

Downloading Internet Connection Firewall

The current HP image ships without the Internet Connection Firewall enabled. This is because most computer users are unaccustomed to using operating systems in which a firewall is enabled by default. To meet the challenge of increasing security vulnerabilities, such as viruses and worms, and to reduce maintenance and total cost of ownership, HP provides the Internet Connection Firewall for download at hp.com.

The Internet Connection Firewall can be downloaded from:

http://h18007.www1.hp.com/support/files/ThinClients/us/download/20070.html

Enabling Internet Connection Firewall

The Internet Connection Firewall is useful when you want to protect a dial-up connection when dialing directly into an Internet service provider (ISP), or to protect a LAN connection that is connected to an asymmetric digital subscriber line (ADSL) or cable modem. You can also enable the Internet Connection

Firewall feature on the Internet connection of an ICS host computer to provide protection to the ICS host computer.

Configuring Internet Connection Firewall Using Network Setup Wizard

To enable Internet Connection Firewall feature using the Network Setup Wizard, perform the following steps:

1. Run the Network Setup Wizard. Select **Start > Settings > Control Panel** and double-click **Network and Internet Connections**, and then click **Setup**.
2. The Internet Connection Firewall is enabled when you choose a configuration in the wizard that indicates that your computer is connected directly to the Internet.

Configuring Internet Connection Firewall Manually

To configure Internet Connection Firewall manually for a connection, perform the following steps:

1. In Control Panel, double-click **Networking and Internet Connections**, and then click **Network Connections**.
2. Right-click the connection on which you would like to enable ICF, and then click **Properties**.
3. On the Advanced tab, select the option, “Protect my computer or network”.
4. If you want to enable the use of some applications and services through the firewall, you need to enable them by clicking the **Settings** button, and then selecting the programs, protocols, and services to be enabled for the ICF configuration.

Disabling Internet Connection Firewall

To disable the Internet Connection Firewall, perform the following steps:

1. In Control Panel, double-click **Networking and Internet Connections**, and then click **Network Connections**.
2. Right-click the connection on which you would like to disable ICF, and then click **Properties**.
3. On the Advanced tab, click the box to clear the option, “Protect my computer or network”.

Using Altiris to Deploy Internet Connection Firewall

The install package, Add_Internet_Connection_Firewall_1.00_B1.exe, contains only files for the Internet Connection Firewall. It does not execute any commands that are needed to complete the installation of the component. To successfully deploy this component to the client, the following steps must be done in addition to executing the install package:

1. The Add_Internet_Connection_Firewall_1.00_B1.exe install program must be executed using the "-s" switch. If this program is not executed using the "-s" switch, the program may not install correctly.
2. After executing the install program, the write filter must commit the changes to the flash memory. This can be done by executing the command line.

```
C:\windows\system32\ewfmgr.exe c: -commit
```

3. A reboot must be executed after the changes are committed to the flash memory. This can be done from an Altiris deployment server job.

NOTE: For space reasons on a thin client running Windows XPe, HP recommends that the setup program be executed from a network share, and the %TEMP% and %TMP% Windows XPe system variables be temporarily re-defined. Unless the client has free uncompressed space equal to three to four times the size of the install package, the install will probably fail.

After modifying the enclosed example batch file, create a new job in the Altiris deployment server.

1. Leave the security context as "Default"
2. Add a reboot to the job.
3. Select the "Run the Script from file" option and select the `Add_Internet_Connection_Firewall_1.00_B1.bat` file.
4. Under the "In which OS would you like to run this script?" option, select "Windows".

NOTE: The "Window state" option can be any of the options.

5. Add a reboot to the job.
6. Select the "Run the Script from file" option and in the "run this script" box type:

```
C:\windows\system32\sleep.exe 60

C:\windows\system32\ewfmgr.exe c: -commit
```

7. Add a reboot to the job.
8. The job is now ready to be deployed.

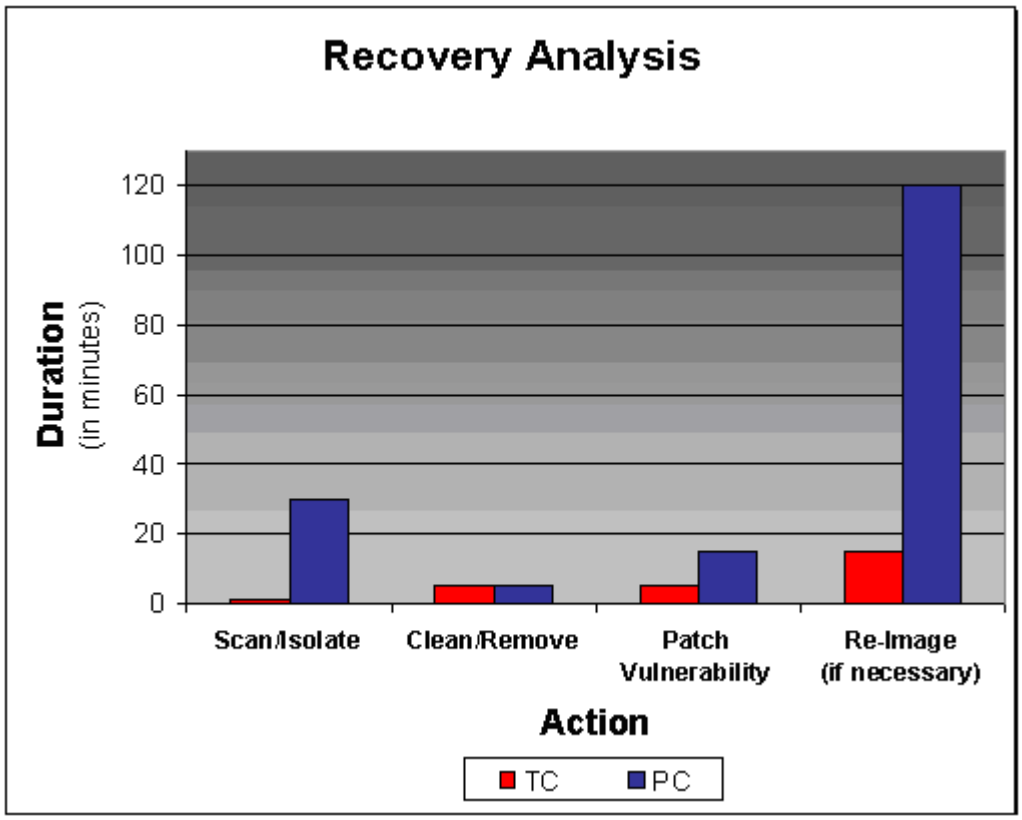
Pros and Cons of Internet Connection Firewall

Pros	Cons
ICF is free.	Like all firewalls, ICF will block certain applications.
ICF performed robustly under attack as well as under high utilization.	ICF does not perform any outbound filtering.
By default, the firewall rule set is very restrictive, preventing most attacks.	ICF does not have real-time notification of attacks.
ICF is a stateful firewall. Stateful firewalls are generally more secure than packet filters.	ICF does not create granular access rules.

Recovery Time

In the event of a virus attack or other security issue, the HP thin client computing model offers significantly shorter recovery time when compared to the traditional desktop model. If a thin client's image is compromised or corrupted, the recovery time is typically measured in minutes instead of hours. Recovery usually involves a power cycle (1 minute), patch (5 minutes), or re-image (15 minutes) of the system. This is substantially less time than the typical two hours it takes to re-image a PC or the multiple hours that can be spent rebuilding and recovering a user's data and environment.

The following graph compares the average recovery time of thin clients and desktop computers. In all categories, the HP thin client computing model meets or greatly exceeds the recovery speed performance of the traditional desktop computing model.



Locking Down A Thin Client

Additional security is available for the HP Compaq t57x0 thin client series. Although the default "User" account on the t57x0 thin client is already somewhat locked down, the account does have administrative rights and can still perform activities such as downloading programs to the desktop and executing them. A t57x0 can be further locked down by creating an account with normal user rights (rather than administrative rights) and additionally applying more restrictive policies, such as preventing the user from downloading any files to the thin client. The following sections provide information and instructions for applying these restrictions.

Standard User Rights

By default, a user account without administrative rights cannot modify the C: drive on a thin client. Furthermore, a user without administrative rights cannot commit changes using the Enhanced Write Filter (EWF).

DisableCMD

This command provides additional restrictions to a user account. The command prevents users from running the interactive command prompt, Cmd.exe. This setting also determines whether batch files (`.cmd` and `.bat`) can run on the computer. If you enable this setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

NOTE: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Terminal Services.

Permission Changes on Desktop Folder

An administrator can change the security permission on the Desktop folder so that it is Read-only.

Prevent File Downloads from Internet Explorer

An administrator can set permissions so that a user cannot download files from Internet Explorer. To restrict a user from downloading files from the Internet, perform the following steps:

1. Open Internet Explorer.
2. Select `Tools > Internet Options`.
3. From Internet Options, select the Security tab and click Custom Level.
4. Scroll down to `Downloads > File Downloads`.
5. Select Disable to prevent Internet downloads.

Prevent Disk-on-Key Access

An administrator can disable Disk-On-Keys by performing the following steps:

1. Select `Start > Settings > Control Panel > System`.
2. Select the Hardware tab.
3. From the Hardware tab, click the Device Manager button.
4. From Device Manager, click on Disk Drives to view all available drives.

5. Right-click on the device you wish to disable and select Disable.
6. To disable a USB device, click on Universal Serial Bus controllers and repeat steps 4 and 5.

NOTE: Future types of Disk-on-Keys may be developed that cannot be blocked by the above method.

7. To prevent users with administrative rights from enabling Disk-on-Keys, you can delete Device Manager after using it to disable the USB devices.

Hiding Desktop Items on the HP Compaq t57x0 Thin Client

Administrators can remove all or some items from a user's desktop using the hide-stuff.reg file. The hide-stuff.reg file will remove all icons from the start menu for the default user. It also removes the tray icon. This will only allow the user to double-click on the IE and/or remote desktop icons that are on the desktop. The hide-stuff.reg file is:

```
REGEDIT4

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVer-
sion\Explorer\Advanced]

"Start_ShowControlPanel"=dword:00000000

"Start_ShowMyComputer"=dword:00000000

"Start_ShowPrinters"=dword:00000000

"Start_MinMFU"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Poli-
cies\Explorer]

"NoTrayItemsDisplay"=dword:00000001

"NoStartMenuMorePrograms"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVer-
sion\Explorer\StartPage]

"Favorites"=hex:ff
```

The hide-stuff-reg file can be modified to include whatever icons you wish. The following table is a list of definitions for each line of the file. To include a particular icon or item, simply delete the appropriate line.

Code	Definition
"Start_ShowControlPanel"=dword:00000000	Hide the control panel
"Start_ShowMyComputer"=dword:00000000	Hide My Computer
"Start_ShowPrinters"=dword:00000000	Hide Printers

Code	Definition
"Start_MinMFU"=dword:00000000Programs	Hide Recently used
"NoTrayItemsDisplay"=dword:00000001	Hide the Tray icons
"NoStartMenuMorePrograms"=dword:00000001	Hide the More Programs Menus
"Favorites"=hex:ff	Hide Favorites from Internet Explorer

After modifying the hide-stuff.reg file, perform the following steps:

1. Log on as Administrator on the t5700.
2. Copy the attached file into `c:\Documents and Settings\User\Desktop\`.
3. Log off and log on as User.
4. Double-click on the hide-stuff.reg file on the desktop.
5. Click Yes to the warning dialog box.
6. Click OK and log off.
7. Log on as Administrator again.
8. Delete c:\Documents and Settings\User\Desktop\hide-stuff.reg.
9. Log on again as User.
10. Click the Start button, and you'll see that all icons are gone.
11. Make sure that the hide-stuff.reg is removed from the desktop and log off.
12. Log on as Administrator.
13. Go in Control Panel and start the EWF Manager.
14. Click the "Commit data to volume" button and reboot.

Summary

The HP thin client computing model provides significantly better virus protection than its PC counterpart. This protection is achieved by:

- Centralizing an enterprise's computer resources in the data center.
- Using centralized virus protection and firewall tools to protect these resources.
- Segregating the user's data for enhanced security, backup, and quick recovery.
- Deploying HP thin clients for simple, secure, reliable, and efficient access to these centralized resources.
- Using HP centralized management tools to manage and patch at all levels of the enterprise.

For more information

For additional HP Compaq t5000 thin clients information, please refer to the following:

http://h18004.www1.hp.com/products/thinclients/index_t5000.html

367974-002, 10/2004