Global Information Assurance Certification Paper

Implementing Citrix MetaFrame XP Security Using Defense in Depth

by

Michael A. Kolba Jr.

April 5, 2004

Abstract

This research paper evaluates and recommends the implementation of security for a Citrix MetaFrame XP system. Ten areas of security are covered including:

- The testing and evaluation of system security
- System security configuration
- Application security configuration
- Client computer security implementation
- Firewall implementation
- Encryption usage
- Virus scanning
- Patch management and system vulnerabilities
- Physical system security
- Business remote access and employee policies

The implementation of security in these areas is then discussed using the concept of Defense in Depth and how it fits in with a security implementation based on it.

CONTENTS

INTRODUCTION

Identifying the Business Drivers

The increased need for business efficiencies has expanded the use and implementation of remote access solutions to provide workers with extended access to applications, data and network resources. Network bandwidth restrictions and the need to reduce telecommunications costs have also driven the implementation of thin-client solutions for data and application access throughout global organizations. Outsourcing of business functions and projects have further necessitated the requirement for third party contractors and business partners to be provided with this same level of access in order to fulfill contracted responsibilities and obligations on behalf of their clients. Few products are available to be implemented in such a wide range of situations.

Product Background

One such product, Citrix MetaFrame XP is the product of choice for companies worldwide and is used to meet these varied and diverse technical and business requirements. With Citrix MetaFrame XP, applications are installed on a Windows 2000 server with Terminal Services configured in application mode (Microsoft Corp., *"Deployment Planning Guide"*, Chapter 16). In this configuration, users are provided access to a virtual desktop, similar to the desktop that they would have on a pc or laptop. The primary difference is that this virtual desktop is server-based and allows multiple users to concurrently access their own separate, isolated desktops, along with any applications that may also be installed on the server.

Citrix MetaFrame XP provides enhanced functionality to this basic configuration by providing advanced features to the basic services provided by Microsoft Terminal Services. This functionality includes the publishing of an application or content, load-balancing of a published application or content across multiple servers, access to this published application or content via a web page and web browser, enhanced encryption of data and more efficient use of network bandwidth (Citrix Systems, *"Administrator's Guide, Citrix MetaFrame XP"*, Chapter 2).

Identifying the Problem

With the need to provide this access and functionality to a potentially broad user base, additional care must be taken by companies to not inadvertently expose their networks, resources and data; placing themselves, their customers and partners at risk. In today's age of increased business risk through theft, virus attack and exploitation of vulnerabilities, security of these resources and data has become a paramount concern for companies worldwide. Security has become a competitive business advantage when implemented well, and a disadvantage when disregarded.

Identifying the Solution & Methodology

The concept of Defense in Depth (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol. 1"*, 40) is the approach of using multiple layers of security to guard against the failure of a single component. By addressing security at multiple layers, and in multiple components, the overall strength of the security of the system is improved. More time, effort and resources is then required to compromise a system and by implementing security at multiple layers, and components, the chance of detecting an intrusion is also greatly increased. This paper

seeks to evaluate the security of various components and layers in a Citrix MetaFrame XP system, and recommend solutions for its implementation, using the principles of Defense in Depth.

TESTING AND EVALUATING SYSTEM SECURITY

Identifying the Need

The need for testing and evaluating the security of a system is necessary to determine how secure or insecure it is. By doing so, it helps to determine the level of risk when making decisions between application functionality and the implementation of security restrictions in order to achieve a balance between the two that furthers the goals of the business. When testing and evaluating the security of a system, an audit must be performed in order to inventory and assess the security and controls placed on a system. According to the General Accounting Office (United States, *"Federal Information Systems"*, 14), "as part of the planning phase of the audit, the auditor:

- gains an understanding of the entity's operations and identifies the computer-related operations that are significant to the audit,
- assesses inherent risk and control risk,
- makes a preliminary assessment on whether general controls are likely to be effective, and
- identifies the general controls that will be tested."

It is a fine line that must be walked to achieve this balance. Often, security restrictions and patches, when implemented, secure the system, but may break functionality required for an application (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol. 2"*, 1224) and may render the overall system useless and as a result, impair a business process or function. Testing and evaluation of these security restrictions and patches with applications and systems must be done to determine the consequences of their implementation and aid in making a risk-based assessment on whether to apply the proposed setting or patch.

Recommendations for Testing & Evaluation

When performing testing of a Citrix MetaFrame XP system and application, security settings applied to a server should be inventoried and the correct application or failure of these settings should be verified when testing is performed. Initial testing should be performed with an account that would replicate how a user or client would be configured. It should not be done with accounts that have administrative privileges, as these accounts are typically excluded from group policy security settings, and typically are granted full, file system and registry access on the server. This account should be used to test all the application and system functionality and should also be used to check against and verify the all of the security settings being applied. For example, if a policy is being applied to restrict the use of regedit.exe by a user, testing should be done to confirm that the user is unable to access that application.

These settings and restrictions should also be verified when being accessed from within the application as well. The main reason for this is that depending on how an application is programmed, security holes may be exposed or introduced by the application. An example of

this is the implementation of the group policy "Prevent Access to Drives from My Computer" (Microsoft Corp, "*OFF2000: Office Programs*"). While the implementation of this policy may restrict access to local system drives from the desktop, if you attempt to access these drives from within an application via File>Open or a similar mechanism, you may be able to bypass this security setting. Microsoft Office 2000 is one such application that would behave in such a manner. Any File>Open application function that would call that common dialog, would allow you to view and access these restricted drives. This bug has been fixed with a service pack, but it serves to illustrate the point that the application you are seeking to implement, may also introduce security holes in the system you are attempting to secure, and the system security should be verified in conjunction with the use of the application.

After this integration testing has occurred and the application has been determined to function properly with the defined security settings, additional testing and evaluation of the security of the system should be done from other systems and locations outside the system being tested. For example, if the local administrator account on the server is denied access to the server from the network through a group policy setting, you should attempt to connect to and administer the server from another pc or server with that restricted local administrator account to determine if the policy and restriction is in effect. The test scripts that you have previously defined and inventoried with the restrictions that you are seeking to implement should be verified in this manner to determine if there are additional vulnerabilities and exposures that need to be addressed and resolved. If they cannot be directly resolved through a change in a configuration setting, then try to mitigate the exposure through another layer of security being implemented.

System control also plays an important part in the testing and evaluation of the security of a Citrix MetaFrame XP system. The ability to make changes to a system and the ability to audit, monitor and log these changes is a critical part of the evaluation and testing of a systems security. The following audit settings in Table 1 are recommended settings from the National Security Agency.

Audit Policy Options	**Setting**
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No Auditing
Audit system events	Success, Failure

Table 1, Audit Policy Options (Haney, *"Guide to Securing" Chapter 4, 39*)

For the General Accounting Office, "when testing and evaluating system controls, there are six major categories of general controls that an auditor should consider when performing their evaluation. These are:

- **entitywide security program planning and management** that provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls;
- **access controls** that limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure;
- **application software development and change controls** that prevent unauthorized programs or modifications to an existing program from being implemented;
- **system software** controls that limit and monitor access to the powerful programs and sensitive files that (1) control the computer hardware and (2) secure applications supported by the system;
- **segregation of duties** that are policies, procedures, and an organizational structure established so that one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records; and
- **service continuity** controls to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected." (United States, *"Federal Information Systems*", 22-23)

On a Citrix MetaFrame XP system, as application upgrades are made or system changes implemented, these security settings, policies and controls should be re-visited and verified to ensure that the security and controls implemented are behaving as expected and that the application continues to function as it is required to. A periodic evaluation (National Institute of Standards & Technology, *"An Introduction"*, 13-14) against these defined controls should also be performed to determine if additional security settings or controls are warranted due to changes made to the application, the Citrix MetaFrame XP system, discovery of new vulnerabilities, changes in business policy or the risk tolerance of the corporation. The Security Self-Assessment Guide for Information Technology Systems (Swanson) can be used as an aid to assist in performing these security evaluations of systems and applications.

SYSTEM SECURITY CONFIGURATION AND SETTINGS

Citrix MetaFrame XP Security

When implementing security on a Citrix MetaFrame XP system, there are some general configuration guidelines that should be followed if possible, as long as business reasons or application functionality does not dictate otherwise. The first recommendation is to publish an application (Citrix Systems, *"Administrator's Guide, Citrix MetaFrame XP"*, 244-263) in order to allow access to it. By doing this, you are not providing direct desktop access to the Citrix MetaFrame XP server in order to access the application. The application is launched without the Windows Explorer desktop shell. This is an important security consideration since in doing so; users are prevented access to other applications, tools and utilities normally available through a desktop. Publishing a desktop requires additional testing and configuration to secure the system.

As part of the installation of Citrix MetaFrame XP, there is an option to remap the server drives to different drive letters (Citrix Systems, *"Administrator's Guide, Citrix MetaFrame XP"*,

107-108, "*Advanced Concepts Guide*", 270-273). If drive remapping is configured, the typical C: drive where your operating system would be installed would be changed to a different drive letter of your choosing. This is important to do since it can make it more difficult for a malicious user to access if they do not know what drive it has been remapped to.

Microsoft Group Policy Security

Whenever possible, use Windows 2000 group policies. Windows 2000 group policies (Microsoft Corp., "*Step-by-Step*") are more flexible and allow for the setting and changing of more settings than are available in a Windows NT 4 system policy. This is an important consideration in a Citrix MetaFrame XP implementation because, since the server is a shared resource, typically accessed by numerous concurrent users, one adverse change to a system file could render the server unavailable to all users. Malicious users could also gain access to the local system drives and gain access to local server configuration information or data, thereby compromising its security and potentially the security of other servers on the network.

When implementing settings with Windows 2000 group policies, here are some guidelines (Entner, *"Policies and Profiles"*, 25) to follow when developing or testing new policies. Document all your group policy settings and the domain groups used to apply them.

1. **Stay away from the live AD**. Build a test domain that mimics the current client environment. This can be done with a minimum of resources and allows for greater flexibility without impacting the current AD structure.
2. **Test policies and profiles within a limited scope.** When applying policies and profiles use the smallest sampling of users that is practical. Create special test groups and be sure to import any current policies to determine overlay (inheritance and blocking) effects.

Group policy settings should not be applied to Administrators to prevent an incorrect policy from locking an administrator out of a server (Microsoft, "*Step-by-Step*").

Below is a listing of some recommended group policy settings compiled from SANS to use as a starting point when implementing a Citrix MetaFrame XP system (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol. 2"*, 1236-1254).

Password Policy Options	**Setting**
Enforce password history	24 Passwords
Maximum Password Age	90 days
Minimum Password Age	1 Day
Minimum Password Length	8 Characters
Passwords must meet complexity requirements	Enabled
Account Lockout Options	**Setting**
Account lockout duration	15 minutes
Account lockout threshold	5 attempts
Reset account lockout counter after	5 minutes

Table 2, Group Policy Settings (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol. 2"*, 1236-1254)

Security Options	**Setting**
LAN Manager authentication level	Send LM/NTLMv1 – Use NTLMv2 session security if negotiated
Rename administrator account	<enter renamed account>

Security Options	**Setting**
Secure Channel: Digitally encrypt secure channel data (when possible)	Enabled
Send unencrypted password to connect to third-party SMB servers	Disabled

Security Options	**Setting**
Message text for users	This system is for the use of authorized Users attempting to log on only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users also may be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Security Options	**Setting**
Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (when possible)	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Internet Explorer Security Options	**Setting**
Download signed ActiveX controls	Disabled
Download unsigned ActiveX controls	Disabled
Initialize and script ActiveX controls not marked as safe	Disabled
Run ActiveX controls and plug-ins	Disabled
Internet Explorer Security Options	**Setting**
Script ActiveX controls marked safe for scripting	Disabled
Java Permissions	High Safety
Launching programs and files in an IFRAME	Disabled
Active Scripting	Disabled
Logon	Automatic Logon Only in Intranet Zone
Define exceptions for sites you trust	Trusted Sites Zone
Define restrictions for sites you don't trust	Restricted Sites Zone
Administrative Templates Settings- Internet Explorer	
Disable changing proxy settings	
Disable changing Automatic Configuration settings	
Disable changing ratings settings	
Disable changing certificate settings	
Disable AutoComplete for forms	
Do not allow AutoComplete to save passwords	

Table 3, Group Policy Settings (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol. 2"*, 1236-1254)

Administrative Templates Settings- Internet Explorer Control Panel
Disable the General page
Disable the Security page
Disable the Content page
Disable the Connections page
Disable the Programs page
Disable the Advanced page
Administrative Templates Settings- Internet Explorer Browser Menus
File Menu: Disable closing the browser and explorer windows
Tools Menu: Disable Internet Options…..Menu option
Disable “Save this program to Disk” option
Administrative Templates Settings- Start Menu and Taskbar
Remove common program groups from Start Menu
Remove Run menu from Start Menu
Disable and remove the Shut Down command
Administrative Templates Settings- Microsoft Management Console
Restrict the user from entering author mode.
Restrict users to the explicitly permitted list of snap-ins
Administrative Templates Settings- Task Scheduler
Hide Property Pages (of tasks)
Prevent Task Run or End
Disable Drag-and-Drop (of .job files into the Tasks folder)
Disable New Task Creation
Disable Task Deletion
Disable Advanced Menu
Prohibit Browse (to schedule arbitrary programs or scripts)
Administrative Templates Settings- Control Panel
Disable Control Panel
Hide specified Control Panel applets
Show only specified Control Panel applets
Disable Add/Remove Programs
Hide the “Add a program from CD-ROM or floppy disk” option
Disable Display in Control Panel
Hide Background tab
Disable changing wallpaper
Hide Appearance tab
Hide Settings tab
Hide Screen Saver Tab
Activate screen saver
Screen saver executable name
Password protect the screen saver
Screen Saver timeout

Table 4, Group Policy Settings (Cole, Fossen, Northcutt, & Pomeranz, *“SANS Security Essentials Vol. 2”*, 1236-1254)

Administrative Templates Settings- Network and Dial-Up Connections
Prohibit deletion of RAS connections
Prohibit access to properties of a LAN connection
Prohibit access to current user's RAS connection properties
Prohibit access to properties of RAS connections available to all users
Prohibit access to the Dial-Up Preferences item on the Advanced menu
Prohibit access to the Advanced Settings item on the Advanced menu
Prohibit configuration of connection sharing
Prohibit TCP/IP advanced configuration
Administrative Templates Settings- Windows Explorer
Remove "Map Network Drive" and "Disconnect Network Drive"
No "Computers Near Me" in My Network Places
No "Entire Network" in My Network Places
Hide these specified drives in My Computer
Prevent access to drives from My Computer
Administrative Templates Settings- System
Disable the command prompt
Disable registry editing tools
Run only allowed Windows applications
Don't run specified Windows applications
Disable Autoplay on All Drives
Disable Task Manager
Exclude directories in roaming profile
Run these programs at user logon
Disable the run once list
Disable legacy run list

Table 5, Group Policy Settings (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol. 2"*, 1236-1254)

Personal Experiences with Group Policy Security

From my personal experience as a Citrix Certified Enterprise Administrator, in performing application engineering, integration and security implementation on a Citrix MetaFrame XP platform, I would also recommend looking at using the following settings as well. My reasoning for applying the settings is detailed below each set of recommendations. This may not apply to every situation, depending on business and application requirements.

Security Options	**Setting**
Do not display last user name in logon screen	Enabled

Table 6, Group Policy Settings (Kolba, 2004)

The reason for this is that in a multi-user environment, you don't want usernames displayed in the login screen when multiple users will be using the system. By allowing this, you expose the ID's that are being used to access and log into the system.

Administrative Templates: Internet Explorer	Setting
Disable Internet Connection Wizard	Enabled
Disable the Reset Web Settings Feature	Enabled
Search: Disable Search Customization	Enabled
Search: Disable Find Files via F3 within the browser	Enabled

Table 7, Group Policy Settings (Kolba, 2004)

The above settings should be disabled because they could allow the users using the system to modify the Internet Explorer customizations and settings or restrictions that may be specified by your organization. In addition, by allowing the search function to be enabled, if you perform a search on the local system drives, file listings and directories will be reported in the search, even though access to the local server drives may be denied via the "Prevent access to drives from My Computer" or "Hide these specified drives in My Computer" group policy.

Administrative Templates: NetMeeting	Setting
Disable Remote Desktop Sharing	Enabled
Enable Automatic Configuration	Disabled
Disable Directory services	Enabled
Prevent adding Directory servers	Enabled
Prevent viewing the Web directory	Enabled
Prevent automatic acceptance of Calls	Enabled
Allow persisting automatic acceptance of Calls	Disabled
Prevent sending files	Enabled
Prevent receiving files	Enabled
Disable Chat	Enabled
Disable NetMeeting 2.x Whiteboard	Enabled
Disable Whiteboard	Enabled
Disable Application Sharing	Enabled
Prevent Sharing	Enabled
Prevent Desktop Sharing	Enabled
Prevent Sharing Command Prompts	Enabled
Prevent Sharing Explorer Windows	Enabled
Prevent Control	Enabled
Prevent Application Sharing in true color	Enabled
Disable Audio	Enabled
Disable Full Duplex Audio	Enabled
Prevent changing DirectSound Audio setting	Enabled
Prevent sending Video	Enabled
Prevent receiving Video	Enabled
Hide the General page	Enabled
Disable the Advanced Calling button	Enabled
Hide the Security page	Enabled
Hide the Audio page	Enabled
Hide the Video page	Enabled

Table 8, Group Policy Settings (Kolba, 2004)

NetMeeting in Table 8 is disabled due to the abilities it provides to auto-accept calls, share desktops and applications, allow the sending and receiving of files, audio and video. By

allowing these functions on a Citrix MetaFrame XP server, you are potentially allowing access to unauthorized users who should not access the applications, data and resources hosted on the server. Citrix MetaFrame XP has inherent functionality that can allow the shadowing of user sessions (Citrix Systems, *"Administrator's Guide, Citrix MetaFrame XP"*, 123, 209-210). This allows an authorized user to see and/or control the desktop session of another Citrix MetaFrame XP user, as well as send messages and otherwise communicate with the user. This can be a more secure method of collaboration between users because specific permissions are required to be granted to a user to allow this shadowing functionality.

Administrative Templates: Network	**Setting**
Offline Files	Disabled
Disable "Make Available Offline"	Enabled
Prevent use of Offline Files Folder	Enabled
Disable user configuration of "Offline Files"	Enabled

Table 9, Group Policy Settings (Kolba, 2004)

Offline Files should be disabled because it allows the caching of network data and resources onto the Citrix MetaFrame XP Server, which would bypass the security that may be applied on the file server hosting those files and directories, including firewall rules and NTFS permissions.

In addition to the security concerns there are performance and availability issues as well. Roaming profiles could increase in size and would increase login and logout speeds on the Citrix MetaFrame XP server. Concurrent usage of the MetaFrame XP server by users who use the system with Offline Files enabled, could lead to disk space problems due to the amount of data being cached locally to the server. In turn, this could prevent the login of users to the server or crash the system because of the inability to create or load a profile caused by lack of disk space.

Administrative Templates: Windows Explorer	**Setting**
Enable Classic Shell	Enabled
Hide Hardware Tab	Enabled
Hides the Manage Item on the Windows Explorer context menu	Enabled
Remove Search button from Windows Explorer	Enabled
Removes the Folder Options menu item from the Tools Menu	Enabled
Disable Windows Explorer default context menu	Enabled
Disable UI to change menu animation setting	Enabled
Hide the common dialog places bar	Enabled
Hide the common dialog back button	Enabled
Hide the dropdown list of recent files	Enabled

Table 10, Group Policy Settings (Kolba, 2004)

The previous items in Table 10 are settings used to configure the functionality of Windows Explorer. By enabling these settings, the user's ability to search, browse, navigate and access the local Citrix MetaFrame XP server through Windows Explorer is limited, even from

within applications. Enabling the Classic Shell defaults the Windows Shell to the previous NT 4 interface and behaviors. Performing a File>Open within an application will not list History, Favorites, My Network Places, My Documents and the Desktop items, which would ordinarily be displayed as part of the common dialog places bar. Disabling this functionality would prevent users from accessing these items through an application (which may otherwise be restricted).

Administrative Templates: Start Menu and Taskbar	**Setting**
Disable changes to the Taskbar and Start Menu Settings	Enabled
Add logoff to the Start Menu	Enabled
Remove Search from the Start Menu	Enabled
Remove Network & Dial-Up Connections from Start Menu	Enabled
Disable and remove links to Windows Update	Enabled
Disable context menus for the Taskbar	Enabled

Table 11, Group Policy Settings (Kolba, 2004)

Disabling the above list would prevent users from changing the Taskbar and Start Menu and prevent searching for files that may be located on the local system. It will also prevent access to Network and Dial-Up Connections, accessing Windows Update and using any taskbar context menus (like accessing Task Manager, which can give you access to the Run menu).

Administrative Templates: Desktop	**Setting**
Do not add shares of recently opened documents to My Network Places	Enabled
Remove Properties from the My Computer context menu	Enabled
Remove Properties from the My Documents context menu	Enabled
Prohibit user from changing My Documents path	Enabled
Disable adding, dragging, dropping and closing the Taskbar's toolbars	Enabled

Table 12, Group Policy Settings (Kolba, 2004)

The above settings would prevent the addition of shares of recently opened documents to My Network Places and prevent users from accessing properties for My Computer and My Documents. This will help to prevent browsing of the network, finding out information about the local server and prevent users from changing the My Documents path. If they can change this path, they may be able to try to specify a location on another server to try to gain access.

Administrative Templates: Windows Installer	**Setting**
Disable Windows Installer	For Non Managed Apps Only

Table 13, Group Policy Settings (Kolba, 2004)

Disabling Windows Installer is preferred to prevent the installation of unauthorized applications and software on the server. Establishing control over the installation of software onto a Citrix MetaFrame XP server is required to secure the system and prevent outages caused by the installation of untested software. Otherwise, this can cause a system incompatibility, instability or other problem which could render the system insecure or unavailable.

Administrative Templates Settings- Network and Dial-Up Connections	**Setting**
Prohibit Access to the Network Connection Wizard	Enabled
Prohibit enabling/disabling a LAN connection	Enabled
Prohibit renaming LAN connections or RAS connections available to all users	Enabled
Prohibit renaming of RAS connections belonging to the current user.	Enabled
Prohibit adding and removing components for a LAN or RAS connection.	Enabled
Prohibit enabling/disabling components of a LAN connection	Enabled
Prohibit access to properties of components of a LAN connection	Enabled
Prohibit access to properties of components of a RAS connection	Enabled

Table 14, Group Policy Settings (Kolba, 2004)

The above settings would prevent users from accessing and modifying LAN connections on the server. This is desired to prevent users from changing the LAN connection configuration or obtain server-specific information that should otherwise not be accessed (like the IP address of a server).

Administrative Templates Settings- System	**Setting**
Group Policy Slow Link Detection	Enabled, 0

Table 15, Group Policy Settings (Kolba, 2004)

The above setting would disable slow link detection of Group Policy (and force the policies to be enforced), irregardless of network bandwidth or speed. If slow network connections are detected, then the policies that you seek to apply will not be enforced. The trade-off here is that it may lengthen login times for users, so the policies can be applied.

Implementing these recommended settings will help to secure a Ctrix MetaFrame XP system. Pre-configured group policy templates are available from organizations such as the National Institute of Standards and Technology, the National Security Agency, SANS, and Microsoft (Cole, Fossen, Northcutt, & Pomeranz, 2003, *"SANS Security Essentials Vol. 2"*, 1236-1254).

APPLICATION SECURITY CONFIGURATION AND SETTINGS

Microsoft Group Policy

After evaluating system security and implementing the configuration settings necessary to impose system restrictions, the security of the application running on Citrix MetaFrame XP should be addressed. For the implementation of application security with some popular Microsoft applications, you can use the group policy templates available for Windows Media Player and the Microsoft Office XP suite of applications (Microsoft Corp, *"Understanding System"*). These group policies should be applied in the same manner as system group policies were applied in the previous section. Some examples of security settings I have used with these templates are shown on the following pages. As with system group policies, depending on your needs and requirements, you may need to use different settings than those listed.

Administrative Templates: Microsoft Office XP	Setting
Disable command bar buttons and menu items	Enabled File>Open>Tools>Search Tools>Add-Ins Tools>Tools on the Web Tools>Speech Tools>Online Collaboration Help>Office on the Web Help>Registration Help>Detect & Repair
Word: Macro Security Level	Enabled/Medium
Word: Trust all installed add-ins and templates	Enabled
Excel: Macro Security Level	Enabled/Medium
Excel: Trust all installed add-ins and templates	Enabled
Access: Trust all installed add-ins and templates	Enabled
PowerPoint: Macro Security Level	Enabled/Medium
PowerPoint: Trust all installed add-ins and templates	Enabled
Publisher: Macro Security Level	Enabled/Medium
Publisher: Trust all installed add-ins and templates	Enabled
Outlook: Macro Security Level	Enabled/Medium
Unsafe ActiveX Initialization	Disabled
Prevent users from changing Office encryption settings	Enabled
Tooltip for disabled toolbar buttons and menu items	<enter message>
Provide feedback with sound	Disabled

Table 16, Group Policy Settings (Kolba, 2004)

The Office XP settings listed above can be set as a computer based policy on the server. They are set with these settings to enhance performance by disabling sound and speech. The security settings are set to prevent users from repairing or modifying the Office XP installation and enable users to run macros if required. It sets trust levels for add-ins that are already installed and prevents Unsafe ActiveX components from being run. Users are prevented from accessing Add-Ins to configure and install additional ones, not initially installed or configured. Finally, the search function is disabled to prevent the listing of and potential access to local system files.

Administrative Templates: Office XP Clip Organizer	Setting
Disable clips online access from Clip Organizer	Enabled
Disable menu item: File>Add Clips to Organizer >From Scanner or Camera	Enabled
Prevent automatically importing clips	Enabled
Prevent users from importing new clips	Enabled
Prevent changes to primary collection	Enabled
Enable preview of sound and motion on Terminal Server	Disabled

Table 17, Group Policy Settings (Kolba, 2004)

The above settings prevent the installation of additional Clip-Art on the server by users and optimizes performance by disabling sound and motion previews.

Administrative Templates: Windows Media Player	**Setting**
Prevent Automatic Updates	Enabled
Prevent CD and DVD Media Information Retrieval	Enabled
Prevent Music File Media Information Retrieval	Enabled
Hide Privacy Tab	Enabled
Hide Security Tab	Enabled
Set and Lock Skin	Enabled
Prevent Codec Download	Enabled
Allow Screen Saver	Disabled
Hide Network Tab	Enabled
Streaming Media Protocols	Disabled
Configure HTTP Proxy	Disabled
Configure MMS Proxy	Disabled
Configure RTSP Proxy	Disabled
Configure Network Buffering	Disabled

Table 18, Group Policy Settings (Kolba, 2004)

The above settings for Windows Media Player are set to prevent the modification and configuration of the settings by users. They also prevent the automatic update of Windows Media Player and disable streaming media protocols to optimize server performance and not introduce additional potential vulnerabilities.

Administrative Templates: Excel 2002	**Setting**
Disable command bar buttons and menu items	Enabled File>Open>Tools>Search Tools>Add-Ins Tools>Tools on the Web Tools>Speech Tools>Online Collaboration Help>Office on the Web Help>Registration Help>Detect & Repair
Excel: Macro Security Level	Enabled/Medium
Excel: Trust all installed add-ins and templates	Enabled
Administrative Templates: FrontPage 2002	**Setting**
Disable command bar buttons and menu items	Enabled File>Open>Tools>Search Tools>Add-Ins Tools>Tools on the Web Tools>Speech Tools>Online Collaboration Help>Office on the Web Help>Registration Help>Detect & Repair

Table 19, Group Policy Settings (Kolba, 2004)

Administrative Templates: PowerPoint 2002	**Setting**
Disable command bar buttons and menu items	Enabled File>Open>Tools>Search Tools>Add-Ins Tools>Tools on the Web Tools>Speech Tools>Online Collaboration Help>Office on the Web Help>Registration Help>Detect & Repair
New Animation Effects	Disabled
Check Spelling as you type	Disabled
Administrative Templates: Word 2002	**Setting**
Disable command bar buttons and menu items	Enabled File>Open>Tools>Search Tools>Add-Ins Tools>Tools on the Web Tools>Speech Tools>Online Collaboration Help>Office on the Web Help>Registration Help>Detect & Repair
Provide Feedback with Animation	Disabled
Check Spelling as you type	Disabled
Administrative Templates: Publisher 2002	**Setting**
Disable Tools>Tools on the Web	Enabled
Check Spelling as you type	Disabled

Table 20, Group Policy Settings (Kolba, 2004)

The settings in Table 19 and 20 are similar to the ones described in the Office XP computer policy, but instead can be configured as part of a user-based policy. To enhance system performance, the spell-check as you type feature and feedback with animation functions are also disabled.

Finally, the settings on the next page in Table 21 for Outlook are configured in the following manner. The modification of attachment security is prevented. The caching of a password for Internet e-mail is disabled. The Add-in manager, Instant Messaging and NetMeeting are all disabled. Virus Security for e-mail is enabled. HTTP e-mail is restricted from being configured by users. Junk e-mail is set to be filtered. OST files are prevented from being created on the server for user e-mail. Menu items and command bars are disabled as in the Office XP policy settings and finally, the preview pane is disabled to prevent the automatic viewing of an e-mail that may have a malicious attachment. All of these settings help to contribute to a stronger security configuration of Outlook, its collaborative functions and tools, and lessens the possibility of a virus being introduced through e-mail and attachments.

Administrative Templates: Outlook 2002	**Setting**
Prevent users from customizing attachment security settings	Enabled
Allow access to e-mail attachments	<specify file extensions allowed>
Outlook virus security settings	Enabled
Disable "Remember Password" checkbox for Internet e-mail setting dialog	Enabled
Security>Cryptography Settings	<set appropriate settings for your e-mail implementation
Preview Pane	Disabled
Disable "Add-in manager…" button	Enabled
Disable Instant Messaging in Outlook	Enabled
Instant Messaging Installation URL	Disabled
NetMeeting	Disabled
Prevent users from adding HTTP e-mail accounts	Enabled
Junk e-mail filtering	Enabled
OST Creation	Enabled Prevent OST Creation
Disable command bar buttons and menu item	Enabled File>Open>Tools>Search Tools>Add-Ins Tools>Tools on the Web Tools>Speech Tools>Online Collaboration Help>Office on the Web Help>Registration Help>Detect & Repair

Table 21, Group Policy Settings (Kolba, 2004)

Always keep in mind that a Citrix MetaFrame XP server is a shared resource and should have controls in place to restrict or prevent unauthorized changes to the applications or system to ensure the security and integrity of the system and applications. By setting the above group policy settings, the usability of the applications, the performance and the control of the system can be better maintained (National Institute of Standards & Technology, *"An Introduction"*, 159-160).

Application Security & Authentication

For client-server applications running on Citrix MetaFrame XP, an identification and authentication mechanism is the first line of defense. This concept is the basis for most types of access control and establishing user accountability. Identification is the means by which a user provides a claimed identity to a system. Authentication is the means of establishing the validity of this claim (National Institute of Standards & Technology, *"An Introduction"*, 181). This is typically done with a username for the identification and a password for the authentication to determine the validity of the user's identification. If a password is used for authentication to the application, it should be a different password than the one that was used to access the MetaFrame XP Server. In this situation, if someone happened to illicitly gain access to the MetaFrame XP server, they would still need to obtain the users ID and password that is used to access the application in order to access any data.

Another item to evaluate in the implementation of application security is the prevention or restriction of the use of cached passwords. By allowing the application to save or cache a password, this potentially creates an additional security risk. In caching or saving a password, the user isn't forced to re-enter the required password each time the application is accessed. If cached or saved passwords are to be used in an application, make sure to have some other security in place that can serve as an extra layer of defense, in case the primary authentication method of accessing the Citrix MetaFrame XP server is compromised. Implementing a logical access control in the application will serve to not only specify who has access to an application, but also what type of access is permitted (National Institute of Standards & Technology, *"An Introduction"*, 195). In this way, confidential data can still be protected if the malicious individual doesn't access the application with an account having that level of privilege.

Citrix MetaFrame XP Application Security

Finally, within a Citrix MetaFrame XP system, security can be implemented with the application that is published. Access to this published application can be granted to specific users or groups of users by adding the user or domain group to the published applications access list. Users who do not have access to the published application will not be able to see, access or launch the application. In publishing the specific application, an additional access control is implemented to help secure it.

CLIENT COMPUTER SECURITY

Citrix ICA Client and Web Access

The client computer is the computer system that an individual uses to access the Citrix MetaFrame XP system and the applications published on it. This client can be a laptop, desktop or even a handheld device. In order to access a published application on Citrix MetaFrame XP, the client device will need to have the Citrix ICA client software installed. The Citrix ICA client can be used stand-alone, or can be used in conjunction with a web browser to access the published application (Citrix Systems, *"Administrator's Guide, Citrix ICA"*, 13-28).

When accessing a published application, the Citrix client connects to a farm, which is a logical grouping of Citrix MetaFrame XP servers and all of the applications that are installed and published on them. The Citrix client is configured to access the specified farm and when the user logs into the farm, all of the published applications that the user has access to are displayed within the client. The login to the farm is performed with the user's domain account, and based on the group memberships that the users account has, specified published applications will then be presented to the user. By using group memberships to grant or restrict access to these published applications, an additional layer of security is implemented. The Citrix Client has the ability to cache a users ID and password and the use of this functionality is not recommended (Citrix, *"Administrator's Guide, Citrix ICA"*, 80-81) because if the security of the users client pc is compromised, a malicious individual can then gain access to the published applications and resources located on the Citrix MetaFrame XP server through the use of the cached credentials within the client.

A web browser can also be used to gain access to Citrix published applications within a farm. By using a web browser to connect to a web site running Citrix NFuse, a user is presented

a web login page that is used to log into a Citrix farm. The user logs in with their domain account and is then presented with the same application listing that they would receive when using the native Citrix ICA client. The user then clicks on an icon representing the application and an ICA configuration file is passed from the browser to the Citrix Client installed on the PC. This configuration file contains all the settings required to launch the specified published application on a specific server. The web browser should be enabled for 128-bit encryption.

The advantage of using Citrix NFuse and a web browser to access published applications within a farm is that the configuration of the settings used to connect to the farm or applications can be centralized to simplify administration. The implementation of security can also be centralized by placing controls or restrictions on the access allowed to this website.

Physical Security

When considering Client security, additional measures should be taken to secure the system that will be used to access MetaFrame XP and the applications published on it. The use of BIOS system passwords should be implemented to help secure access to the system in addition to the use of an operating system logon used to gain access to the desktop interface and any applications on the system. Password protected screen savers should be implemented on the client PC's to prevent malicious users from gaining access to applications and data that may be running on a pc, while a user is away from their system.

Account Privileges & Security

Users with administrative rights on the network should use restricted, user level privileged accounts for their daily activities and pc use, and have separate administrative accounts that could be used as required for accessing systems and applications. By doing this, the spread of viruses and worms can be limited if an administrator's pc becomes infected. The logging, auditing and monitoring of administrative activity can then be focused on these specific administrator accounts, which enhances security and detection of malicious activity. It also makes it more difficult for a hacker to gain administrative access to servers and resources through an administrator's workstation, by limiting what their user accounts can do (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol. 2"*, 1247).

Network Connectivity

Additional security can be imposed on a client workstation by implementing the use of personal firewalls and VPN clients when accessing the company's network and network resources, including Citrix MetaFrame XP servers and the applications published on them. Personal firewalls will allow only specified inbound and outbound network traffic to be able to reach the client pc or network resources. The use of VPN client software would form a secure tunnel over which network traffic to and from the client workstation can be securely transmitted and received and help protect the workstation and network resources from malicious attack. It would also typically require an extra authentication to be performed in order to access the corporate network and network resources such as a MetaFrame XP server.

Microsoft Group Policy

As group policies were implemented on a Citrix MetaFrame XP server, group policies can also be applied to client computers and workstations. The same testing methodology used

for evaluating security on a server can be used on a client pc, and group policies for systems and applications that were detailed and applied to a Citrix MetaFrame XP server in the previous sections, should be evaluated and applied in the same manner to the client workstation to secure it from unauthorized changes and malicious attack or intrusion.

FIREWALL IMPLEMENTATION

Citrix MetaFrame XP Firewall Design & Background

Firewall implementation is one of the most important parts of implementing security for Citrix MetaFrame XP. Due to third party and contractor access to applications and resources with MetaFrame XP, a DMZ implementation is often required to implement security for network resources and data. By implementing a firewall as another layer of security to protect your Citrix MetaFrame XP servers, you limit the protocols and port accessible to the servers as well as hide the servers IP address, through the use of network address translation. There are two basic recommended designs given by Citrix (Citrix Systems, *"Administrator's Guide, Secure Gateway"*, 87-90) for implementing MetaFrame XP with NFuse and Citrix Secure Gateway. The first design is a Single-Hop DMZ deployment with two variations, and the second design is a Double-Hop DMZ deployment.

With each of these implementations, the security of the MetaFrame XP Servers, applications and network resources located in the secured portion of the network is maintained through multiple layers of security. Firewalls separate the unsecured portion of the network and the secured portion of the network, limiting the access an external malicious attacker may obtain to it. Ticketing is used to secure the ICA Sessions from the client, to prevent someone from hijacking the connection by limiting the timeframe that the session request is valid for. Finally, NT domain account authentication through NFuse and Citrix XML service is used to gain access to the published applications on the MetaFrame XP Servers.

Single-Hop Design with a Single Server

In a Single-Hop deployment the design is as shown on the next page:

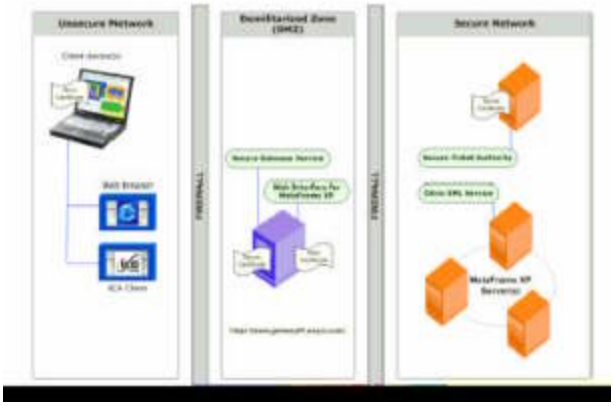

Figure 1- Single Hop Deployment (Citrix, *"Administrator's Guide, Secure Gateway"*, 92)

This Citrix design (Citrix Systems, *"Administrator's Guide, Secure Gateway"*, 93) has a server located in the DMZ that hosts both the Citrix Secure Gateway and the NFuse Web Interface. A web server that resides in the secured portion of the network serves as the Secure

Ticket authority. The MetaFrame XP servers and applications are located in the secured network. Between the unsecured network and the DMZ, the firewall has port 443 open. Between the DMZ and the secured network, the firewall has port 80, 443 and 1494 open.

Single-Hop Design with Two Servers

In the second variation of the Single-Hop Deployment, the NFuse Web interface is on a separate server, also located in the DMZ. This implementation works in the same manner as the first variation, except that users who may be establishing connections to Citrix MetaFrame XP Servers from the secured network, can access applications directly from the NFuse web server in the DMZ. External users from the unsecured network will still access Citrix MetaFrame XP servers through the Citrix Secure Gateway which redirects the traffic to the NFuse Web Interface located on the separate server in the DMZ according to Citrix (Citrix Systems, *"Administrator's Guide, Secure Gateway"*, 90).

Double-Hop Design

A Double-Hop DMZ deployment is used where the DMZ is divided into two separate segments as shown below.

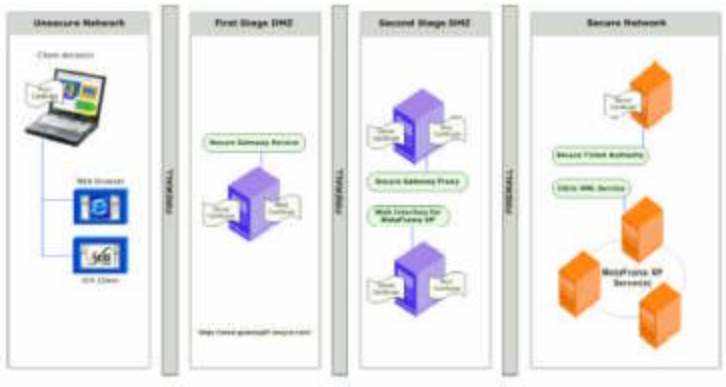

Figure 2- Single Hop Deployment (Citrix Systems, 2003, 100)

According to Citrix, (Citrix Systems, *"Administrator's Guide, Secure Gateway"*, 100) this deployment functions similarly to a Single-Hop DMZ with separate Secure Gateway Servers and NFuse web servers. It differs in that the Secure Gateway is split into two components- a Secure Gateway Service server located in the first DMZ, and a Secure Gateway Proxy server which is located in the second DMZ with the NFuse web server. The firewall separating the secure network and the second DMZ has ports 443, 1494 and 80 open. The firewall separating the first DMZ and second DMZ has port 443 open and the external firewall out to the unsecured network has port 443 open.

ENCRYPTION

Encryption with Citrix MetaFrame XP

The use of encryption can extend down to the client pc where access to Citrix published applications and MetaFrame XP Servers can be performed natively through the use of the Citrix ICA Client. When using the Citrix ICA Client natively, encryption of ICA traffic to and from

the Citrix MetaFrame XP server can be specified and set at levels from basic, up to 128-bit according to Citrix (Citrix Systems, *"Administrator's Guide, Citrix ICA"*, 76-77).

The ICA protocol configuration on a Citrix MetaFrame XP server can be configured to use a specified level of encryption where all data transmitted will be encrypted at that level This is similar to the settings on the client, but is performed on the server-side. Encryption can also be implemented on a published application (Citrix Systems, *"Administrator's Guide, Citrix ICA"*, 209), where the encryption level required to access a published application can be specified. When setting encryption levels, the level specified on the client, must match or exceed the level specified on the ICA protocol on a Citrix MetaFrame XP server on the published application being accessed. If the encryption level of the Citrix ICA Client doesn't meet the specified requirements of the published application or ICA protocol, the user will be unable to launch that application or connect to the Citrix MetaFrame XP Server.

Encryption can also be used with the combination of Citrix NFuse, Citrix Secure Gateway a web browser and the Citrix Client when accessing a Citrix MetaFrame XP farm, server and published application. Citrix NFuse, Citrix Secure Gateway and the web browser components can be secured through the configuration and use of certificates and SSL/TLS encryption (Citrix Systems, *"Citrix MetaFrame XP Security Standards"*, 9). In this scenario, the web browser traffic to the NFuse web page is encrypted through the use of SSL/TLS. The traffic between the ICA client and Citrix Secure Gateway components is also encrypted with SSL/TLS. When the traffic from the ICA Client reaches the secure gateway, it is then decrypted and forwarded to its destination MetaFrame XP server. By setting encryption with the ICA protocol, the session traffic between the Citrix Secure Gateway and the destination MetaFrame XP servers can also be secured, (Citrix Systems, *"Citrix MetaFrame XP Security Standards"*, 14).

Encryption with a VPN Client

Use of a VPN client when accessing network resources remotely can also add an additional layer of security by encrypting all of the network traffic between the client pc and the VPN gateway connected to the network. This is recommended since the traffic is passing over public internet connections may be insecure.

Encryption of File System & Data

Lastly, data on a network resource being accessed through Citrix MetaFrame XP, such as a file server, can also be encrypted through the use of Encrypting File System (EFS) present in Windows 2000. This encrypted data would only be able to be accessed by the person who encrypted the data, so if an intruder gained access to the data, they would not be able to access it unless they had stolen the id and password of the individual originally encrypting it, in accordance with SANS guidelines (Cole, et al., *"SANS Security Essentials Vol. 2"*, 1196-1202).

VIRUS SCANNING

Overview

Virus Scanning is a critical component of a security implementation on Citrix MetaFrame XP. Due to the need of users to access data and files remotely and upload or download files from their local systems, it is imperative that virus scanning is implemented to prevent the

introduction of a virus into the network. Citrix MetaFrame XP provides the ability to map client drives within their session so users of the system have the ability to access local files on their pc or laptop. In this manner they can copy files and data to and from the MetaFrame XP server and any mapped network drives within their session on the server. Virus scanning should be implemented on the client pc, the Citrix MetaFrame XP server that the user connects to, and on any servers that the user has access to while in their Citrix MetaFrame XP session. In this fashion, it can be ensured that if an infected file is introduced into the system and network, its detection and cleaning or removal can be performed to eliminate any further infection.

Restrictions and Exceptions

Some special things need to be addressed with virus scanning configuration on a Citrix MetaFrame XP system. On-access virus scanning should be enabled by default, and all files should be scanned whenever possible. Users on the MetaFrame XP server should also be prevented from changing any of the virus scan settings on the server. By doing this, users of the system will be less likely to introduce a virus into the system and network.

In some cases, applications do not work well with virus scanning configurations on Citrix MetaFrame XP and these settings and configurations may need to be adjusted to allow for the proper functioning of the application. In these cases, certain files or directories may need to be excluded from virus scanning. In other cases, virus scanning may need to be disabled entirely on the server. In these cases, provisions should be made to implement tighter security on the server or arrange outage periods where application access on the Citrix MetaFrame XP server is disabled and scheduled virus scans of the server can be done to check for infection without affecting the application or users (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol. 2"*, 1054-1091).

Due to the remote access functionality performed by Citrix MetaFrame XP, these servers should be considered higher risk for infection by virus due to their ability to be accessed by remote users or third party contractors where the virus scanning protection of their client pc cannot be guaranteed. By treating these servers as being higher risk, steps can be taken to further secure the systems, applications and data residing on them and prevent virus infection and potential loss of access to server resources or destruction of data.

Virus Definition Updates

In addition to the above virus scanning concerns, virus definitions must always be kept up-to-date on any Citrix MetaFrame XP server to ensure the optimal virus protection for the server and resources accessed through it. A number of virus scanning products have mechanisms to automatically update virus definitions and engines to ensure that any server or pc has the most current versions available and they should be implemented whenever possible (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol. 2"*, 1078-1081).

PATCH MANAGEMENT AND SYSTEM VULNERABILITIES

Testing Procedures

Patches need to be thoroughly tested and evaluated before being implemented on a Citrix MetaFrame XP system. A baseline set of patches and security settings that meet the security

requirements of the organization should be applied to a system prior to the installation of applications in order to determine if the application will function appropriately with the baseline. Depending on these results of testing, patches may need to be removed or not applied in order to restore application functionality or prevent functionality from being disabled. In these situations, if possible, the application vendor should be contacted to determine if there is a fix or update that would allow the application to function with the desired system patches or security settings. Sometimes the application of patches may introduce additional security vulnerabilities, so this should also be checked when testing (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol. 2"*, 1259-1264).

System Control

On a Citrix MetaFrame XP server, Windows Update should be disabled through the use of a group policy to prevent unauthorized and uncontrolled installation of software and patches on a system. Patches and updates should be performed in a controlled and documented manner so the security and control of the system can be maintained. Backups should be performed before applying patches in case something goes wrong and data needs to be restored.

If vulnerability is discovered, and a patch can't be applied, the vulnerability should attempt to be mitigated or lessened. An example of this is the vulnerability discovered in the Windows Messenger service. If the application of the patch breaks an application, or can't be implemented for a period of time, the messenger service could be stopped and disabled on the server to eliminate the exposure that the vulnerability presents (Microsoft Corp, *"Microsoft Security Bulletin MS03-043"*). Risk based assessments need to be performed when a new vulnerability is discovered, to determine the impact to a MetaFrame XP system and applications installed on it.

Management & Reporting

One recommendation when looking at patch management and system vulnerabilities is to implement some kind of patch management product or solution (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol. 2"*, 1269-1278). By doing this, reports can be run against servers to determine the patches installed on a server and the patches that may be available to be installed on it, based on its configuration. Multiple servers can be maintained simultaneously, and baselines can be recorded and reported against when using a patch management system. Patches can also be removed, and typically, the maintenance of these items is recorded in a log within the patch management application which provides additional control and auditing functionality. The ability to deploy and install these patches can be restricted to users who have access and authorization to perform that task. Patch management is a critical part of the security of a MetaFrame XP system and should not be overlooked. Vulnerabilities are discovered daily and the ability to report against and address these vulnerabilities is vital to the security of a Citrix MetaFrame XP system and the resources accessed by it.

PHYSICAL SYSTEM SECURITY

Server Security

Physical security of a MetaFrame XP server is fairly straightforward. The server should be located in a data center, where the physical security of the system can be protected. They

should have the following characteristics, according to SANS (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol. 1"*, 275-288). Some sort of authorization and approval process to gain entry to them. They have access controls such as keycards and keypads with pin numbers. Cameras and additional surveillance equipment are typically installed to ensure the protection of the servers and the data that may reside on them. There also may be time restrictions on access to the data center as well. Data centers also may have staff that looks after the servers and equipment located there. They may also be responsible for tracking and logging access.

If a server can't be located in a controlled data center, it should be located in place where physical access can be restricted and the environmental characteristics can be controlled so the server stays within its environmental operating requirements (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol. 1"*, 275-288).

Server Access

Only administrators of the system should be provided with access to the server (Citrix Systems, *"Advanced Concepts Guide"*, 169). The server should also never be left in a logged in state. By doing this, the server may be able to be accessed by unauthorized individuals (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol.1"*, 257). By considering these requirements, the physical security of a server can be ensured.

BUSINESS REMOTE ACCESS AND EMPLOYEE POLICIES

Policy Characteristics

Remote access policies for a business and employee policies can be an important measure to be implemented for increasing the security of a MetaFrame XP server and system. Defining a remote access policy can provide a framework used to help define the technical requirements and security restrictions necessary for a MetaFrame XP server, the applications installed on it and the resources accessed through it.

A remote access policy can define who is allowed to have remote access to the corporate network, and what type of computer system and software is to be used in gaining this access. It can detail how a user's account is to be used and the authentication methods required for gaining access. Authorization requirements for gaining the requested access and the process in which the access is granted can also be specified. It can restrict the access a user is allowed to have and set times access is permitted. It can also define the type of access and the requirements for allowing business partners and contractors remote access to a company's network, systems, resources and data. They can also specify the use of monitoring and collection of information regarding user activities, and how this information will be used by the company. These are all very important concerns to be considered when designing security for a Citrix MetaFrame XP system.

Very often, these policies can be the first and last line of defense for a corporation and can be used to form the basis of legal restrictions and protections regarding a contractor or employee's use and access of a company's network and resources (Cole, Fossen, Northcutt, & Pomeranz, *"SANS Security Essentials Vol.1"*, 362-363). They serve as a first line of defense because they serve as a deterrent to performing these unauthorized and malicious activities, and

can notify employees and business partners about the consequences of violating these rules and restrictions. When a policy is enacted, and legal restrictions are implemented for doing business with a contractor, if the contractor violates the policies and restrictions the company has some legal protections in place to enact a lawsuit to recoup damages suffered, or pursue criminal charges. If an employee violates these policies and restrictions, and accesses data or applications without authorization, steals or destroys data, the company then may have grounds for terminating the employee or pursuing legal action. In this respect, it can be a last line of defense for a corporation. Enacting these types of written policies and restrictions is an important part of securing a system, and provides protections beyond the technical ones that may be implemented.

CONCLUSION

The implementation of Citrix MetaFrame XP security covers many different topics and areas. System and application security testing and evaluation, system security configuration, application security configuration, client security, firewall implementation, encryption, virus scanning, patch management, physical system security, business remote access policies and employee policies all play important roles in security implementation on a Citrix MetaFrame XP system. On their own, each item and component provides a measure of security for the system, application and data that you are protecting. On their own, this protection can be incomplete.

By considering all the items detailed in these sections and implementing the security recommendations within, a layered approach of security implementation is taken. The client PC used to access the Citrix MetaFrame XP server is protected with group policy restrictions to disable certain functionality and features that could be used to obtain information about the systems or access the network and unsecured resources. Password protected screen savers prevent unauthorized users from accessing and using the client PC and the Citrix software used to access the Citrix MetaFrame XP server. Network traffic from a client to a server is protected with various forms of encryption. The servers that are being accessed in the system are protected by firewalls which limit the access to them. The servers are protected from physical access by being located in a secure location or data center where physical access is monitored and controlled. Group memberships for domain accounts allow access to published applications and other required resources. Once the server is accessed, group policy restrictions are placed on the systems and applications to prevent the use of certain functions that may render the system, application or network resources insecure. Application restrictions that require appropriate ID's and passwords to access them are also implemented. Once accessed, the ability to use parts of a system, application or other resources is restricted by logical controls. Virus scanning and patch management provide protection from viruses and limit vulnerabilities that may be present. Written policies notify users of access restrictions and potential penalties for violating them. They also serve to protect the company once a violation occurs. Auditing is used to track authorized and unauthorized access.

By implementing multiple layers of security, the failure of a single security component prevents the compromise of the security of the Citrix MetaFrame XP system, the applications running on it, or the resources accessed through it. Putting Defense in Depth into practice increases security, limits a company's exposure to attack, theft or loss and becomes a competitive business advantage by limiting or eliminating these risks and their associated costs.

REFERENCES

Citrix Systems, Inc. *"Administrator's Guide, Citrix ICA Win32 Clients Version 7.0."* (2003) Retrieved February 24, 2004, from Citrix Support Knowledgebase Web site: http://support.citrix.com/servlet/KbServlet/download/169-102-8767/ICA_Win32_Guide.pdf

Citrix Systems, Inc. *"Administrator's Guide, Citrix MetaFrame XP Server for Windows with Feature Release 3."* (2003) Retrieved January 24, 2004, from Citrix Support Website Web site: http://support.citrix.com/servlet/KbServlet/download/246-102-8751/MetaFrame_XP_Guide.pdf

Citrix Systems, Inc. *"Administrator's Guide, Secure Gateway for MetaFrame Version 2.0."* (2003) Retrieved February 24, 2004, from Citrix Support Knowledgebase Web site: http://support.citrix.com/servlet/KbServlet/download/2373-102-8730/Windows_Secure_Gateway_Guide.pdf

Citrix Systems, Inc. *"Advanced Concepts Guide, Citrix MetaFrame XP for Windows with Feature Release 3."* (2003) Retrieved February 24, 2004, from Citrix Support Website Web site: http://support.citrix.com/servlet/KbServlet/download/2951-102-9534/Feature_Release_3_Advanced_Concepts.pdf

Citrix Systems, Inc. *"Citrix MetaFrame XP Security Standards and Deployment Scenarios, MetaFrame XP Server for Windows with Feature Release 3."* (2003) Retrieved February 24, 2003, from Citrix Support Knowledgebase Web site: http://support.citrix.com/servlet/KbServlet/download/2607-102-8992/MetaFrame_XP_FR3_Security_Standards.pdf

Cole, Eric., Fossen, Jason., Northcutt, Stephen., & Pomeranz, Hal. *"SANS Security Essentials with CISSP CBK Version 2.1"* (Vol. 1). (2003).

Cole, Eric., Fossen, Jason., Northcutt, Stephen., & Pomeranz, Hal. *"SANS Security Essentials with CISSP CBK Version 2.1"* (Vol. 2). (2003).

Entner, Michael. *"Policies and Profiles Standards"* (Version 1.1). (2002). (Original work published 2001) Retrieved February 22, 2004, from Citrix Support Knowledgebase Web site: http://support.citrix.com/servlet/KbServlet/download/13-102-7615/Policies_and_Profiles_Standards.pdf

Haney, Julie. *"Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set"* (Version 1.2.1). (2003). Retrieved March 1, 2003, from National Security Agency Security Configuration Guides Web site: http://www.nsa.gov/snac/os/win2k/w2k_group_policy_toolset.pdf

Microsoft Corp. "*Deployment Planning Guide*." Chapter 16. (2000). Retrieved January 24, 2004, from Microsoft Windows 2000 Web site: http://www.microsoft.com/windows2000/techinfo/reskit/dpg/default.asp

Microsoft Corp. "*Understanding System Policies*." (2002). Retrieved February 24, 2004, from Microsoft Office XP Resource Kit, Using System Policies Web site: http://www.microsoft.com/office/ork/xp/two/admb01.htm

Microsoft Corp. "*Microsoft Security Bulletin MS03-043, Buffer Overrun in Messenger Service Could Allow Code Execution (828035)*." (2003). Retrieved February 24, 2004, from http://www.microsoft.com/technet/security/bulletin/MS03-043.mspx

Microsoft Corp. "*OFF2000: Office Programs Can Browse Restricted Drives*." (2003). Retrieved March 1, 2003, from Microsoft Support Knowledge Base Web site: http://support.microsoft.com/default.aspx?scid=kb;en-us;302753

Microsoft Corp. "*Step-by-Step Guide to Understanding the Group Policy Feature Set*." (2004). Retrieved February 24, 2004, from Microsoft TechNet Web site: http://www.microsoft.com/technet/prodtechnol/windows2000serv/howto/grpolwt.mspx

National Institute of Standards, & Technology, Technology Administration. *"An Introduction to Computer Security: The NIST Handbook"* (Special Publication 800-12th ed.). (n.d.). Retrieved February 24, 2004, from National Institute of Standards and Technology, Computer Security Resource Center Web site: http://cs-www.ncsl.nist.gov/publications/nistpubs/800-12/handbook.pdf

Swanson, Marianne. *"Security Self-Assessment Guide for Information Technology Systems"* (Special Publication 800-26th ed.). (2001). Retrieved February 24, 2004, from National Institute of Standards and Technology Web site: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf

United States General Accounting Office, Accounting, & Information Management Division. *"Federal Information Systems Controls Audit Manual, Volume I: Financial Statement Audits"* (GAO/AIMD-12.19.6). (2001). Retrieved February 24, 2004, from United States General Accounting Office, Special Publications: Computer and Information Technology Web site: http://www.gao.gov/special.pubs/cit.html