Guide to the Secure Configuration and Administration of Microsoft Exchange 5.x®

The Network Applications Team

of the

Systems and Network Attack Center (SNAC)

Author:
Trent Pitsenbarger

National Security Agency
ATTN: C43 (Pitsenbarger)
9800 Savage Rd.
Ft. Meade, MD 20755

W2KGuides@nsa.gov

Dated: 20 Jun, 2002
Version 3.1

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- Please keep track of the latest security patches and advisories at the Microsoft security bulletin page at http://www.microsoft.com/technet/security/current.asp.
- This document contains possible recommended settings for the system Registry. You can severely impair or disable a Windows NT System with incorrect changes or accidental deletions when using a Registry editor (Regedt32.exe or Regedit.exe) to change the system configuration. Currently, there is no “undo” command for deletions within the Registry. Registry editor prompts you to confirm the deletions if “Confirm on Delete” is selected from the options menu. When you delete a key, the message does not include the name of the key you are deleting. Therefore, check your selection carefully before proceeding.

Trademark Information

Windows NT, Microsoft Exchange, and Microsoft Outlook are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries.

All other names are registered trademarks or trademarks of their respective companies.

Written by:

Trent Pitsenbarger

National Security Agency
ATTN: C43 (Pitsenbarger)
9800 Savage Rd.
Ft. Meade, MD 20755
W2KGuides@nsa.gov

Table of Contents

About the Guide to the Secure Configuration and Administration of Microsoft Exchange

This document describes how to more securely install, configure, and administer the Microsoft Exchange Server and associated clients. The focus of these documents is Exchange Server 5.0 and 5.5, the Exchange Client, and the Outlook 97 and Outlook 98 clients. Please note that discussions regarding Exchange Server 5.5 assume service pack 1 (or later) has been installed. Exchange 2000 and Outlook 2000 guidance is under development.

This document is intended for the reader who is already very familiar with Microsoft Exchange but needs to understand how to install, configure, and administer the product in a more secure manner. The information presented here is written in a direct and concise manner in deference to this intended audience – very little introductory material in provided.

While this document is intended as a complement to the "*Guide to Secure Microsoft Windows NT Networks*," it presents the information a little differently. Some Exchange security issues, and corresponding configuration and administrative actions, are very specific to way the product is being used. For this reason, it is difficult in some areas to recommend specific, concrete actions. Instead, a summary is offered which describes the concerns and recommends a range of solutions that must be tailored to the specific environment. Most of the discussions relate to both versions of the Exchange Server (version 5.0 or version 5.5) or to all versions of the client. Where it is necessary to distinguish between versions, a header will be provided indicating which version of the product is applicable. For example, a recommended setting that applies to only Exchange Server 5.5 would be labeled as follows:

☐ Exchange 5.0 ☑ Exchange 5.5

PLEASE NOTE THAT ALL OF THESE DOCUMENTS ASSUME THAT THE READER IS A KNOWLEDGEABLE WINDOWS NT ADMINISTRATOR. A knowledgeable Windows NT administrator is defined as someone who can create and manage accounts and groups, understands how Windows NT performs access control, understands how to set account policies and user rights, is familiar with how to setup auditing and read audit logs, etc. These documents do not provide step-by-step instructions on how to perform these basic Windows NT administrative functions – it is assumed that the reader is capable of implementing basic instructions regarding Windows NT administration without the need for highly-detailed instructions.

This document consists of the following chapters:

Chapter 1, "Exchange Server Installation", provides an overview of the pertinent security issues related to the installation of the Exchange Server.

Chapter 2, "Client Installation" provides an overview of the pertinent security issues related to the installation of the Exchange Client and Outlook 97/98 Clients.

Chapter 3, “Administrative Permissions” describes how administrative permissions are assigned in the Exchange Server.

Chapter 4, “Core Components Administration” briefly describes the main functional components of an Exchange Server and details the pertinent security related settings.

Chapter 5, “Multi-Server Configurations” details the security considerations incumbent in Exchange environments which contain multiple servers.

Chapter 6, “Internet Mail Service” provides the security related configuration and administrative choices associated with Exchange’s Internet Mail Service.

Chapter 7, “Client Security and Advanced Security” looks at the security features available in the Exchange and Outlook clients and the installation and use of the Exchange Key Management Server.

Chapter 8, “ Web Access” describes the security related issues relating to user access of mailbox and public folders via the Hypertext Transfer Protocol (HTTP).

Chapter 9, “POP3/IMAP4/LDAP/NNTP” looks at the security settings associated with accessing the Exchange Server via the Post Office Protocol 3 (POP3), Internet Message Access Protocol (IMAP), Lightweight Directory Access Protocol (LDAP), and the Network News Transport Protocol (NNTP).

Chapter 10, “Custom Applications” covers how the use of custom applications can be structured to improve security.

Chapter 11, “Final Thoughts” takes a quick look at backup procedures, antiviral programs, and other topics.

An Important Note About Operating System Security

Exchange security is tightly coupled to the operating system. For example, Exchange log-on can be coupled to the operating system log-on so that a user does not have to log-on separately to Exchange.

File permissions, registry settings, password usage, user rights, and other issues associated with Windows NT security have a direct impact on Exchange security.

The recommended source of information for how to securely configure the Windows NT 4.0 server and workstation is the "*Guide to Secure Microsoft Windows NT Networks*" which is available from http://www.nsa.gov. It is preferable to implement this guide before installing Exchange; however, it one wishes to implement the Windows NT guide after installation of Exchange, follow the procedures outlined in appendix A to this document.

NOTE: It will be necessary to make minor modifications to these Windows NT guidelines in order for the Exchange Server and clients to function properly. These changes are detailed in this document.

Chapter
1

Exchange Server Installation

Pre-Installation

There are a number of security related actions that must be performed prior to the installation of Exchange.

Operating System Security

Before installing Microsoft Exchange Server or the Exchange or Outlook clients, invoke the Windows NT Operating System security guidelines contained within the "*Guide to Secure Microsoft Windows NT Networks*." Exchange security is tightly coupled to the operating system. File permissions, registry settings, password usage, user rights, and other issues associated with Windows NT security have a direct impact on Exchange security.

If invoking the "*Guide to Secure Microsoft Windows NT Networks*", after installing the Exchange Server or the clients, there are few additional steps that must be taken. Please reference Appendix A.

Create the Windows NT Exchange Services Account

Just as users identify themselves to the Windows NT environment via a user account, processes initiated by the Exchange server also identify themselves by an account. This account is commonly referred to as the "Exchange services account." The Exchange Server's access rights are as defined by that account using Windows NT access control mechanisms. For example, if the name of the account established for Exchange services is "Exchange_Primary," the Exchange server will only be able to access files and directories for which it has been granted the appropriate access permissions.

The following are recommended when creating this account:

- Create a unique account as the Exchange services account. The Exchange services account has carte blanche rights to access and manipulate the various components that comprise an Exchange environment. Creating a unique account will insure that these rights to are not shared with processes or individuals that do not need such access.
- Set the password per the "*Guide to Secure Microsoft Windows NT Networks*."
- Use a somewhat unpredictable name for the account.

- Do not enter a description for the account

It is important to create this account prior to installation, as the installation routine will ask the installer to enter the Exchange Services Account name and password.

Create Windows NT Exchange Administrator's Group

In order to simplify the assignment of administrative rights to the Exchange Server, it is recommended that a separate Windows NT Exchange Administrators Group be established. It is strongly recommended that you do not use the Windows NT administrator group, as it is not necessary to have Windows NT administrative rights for many Exchange administration functions.

Having a separate Exchange Administration Group, or Groups, offers several benefits. First, it will preclude the need for Exchange administrators to log in unnecessarily as a Windows NT administrator -- something that should be avoided for security reasons. Second, it will allow you to partition administrative rights. You may reserve the right to reconfigure the Exchange server to a select few, while allowing several individuals to manage mailboxes, for example. And finally, having an Exchange administrator group(s) will simplify the process of managing administrative rights -- adding a new administrator is as simple as making them part of the appropriate Exchange administrator group.

When creating Exchange Administrator Group(s):

- Do not use the Windows NT administrator's group.

- Consider partitioning Exchange Administrative rights through the use of multiple Exchange Administrative groups.

Installation

When installing the Exchange Server, the following guidelines are recommended in regards to where file location and the installation service packs and hot fixes.

- Do not install the Exchange Server on the same partition as the operating system. The default permissions applied to the %SystemDrive% directory by the "*Guide to Secure Microsoft Windows NT Networks*" will not allow installation of the Exchange Server to a directory under the %SystemDrive% directory (typically C:\). If necessary to install the Exchange Server on the same partition as the OS, simply create the destination directory before beginning and give the Exchange services account "Full Control".

- The information store and directory service log files should be on a physical drive separate from the information stores and directory service themselves. These log files can serve as a record of all transactions made since the last backup. In the event of a loss of the drive holding the Information Store or directory service, having the logs on a separate physical drive will help ensure the ability to restore all lost data. In the event that the use of a separate physical drive is not feasible, using a

separate partition will provide a level of protection. The location of these files can be changed through use of the Exchange optimizer program, which can be run as an option during the installation routine or can be executed separately after installation is complete.

☑ Exchange 5.0 ☐ Exchange 5.5

- ❑ Install Service Pack 2. Some of the security related settings detailed in this document can not be set on the base installation of Exchange Server 5.0 but instead require the prior application of the service pack.

- ❑ At the time of this writing, Microsoft had released the several security relevant patches or hot fixes for Exchange Server 5.0. It is recommended to review the security bulletins at http://www.microsoft.com/technet/security/current.asp for the latest information. It is critical to install security related fixes as soon as possible.

☐ Exchange 5.0 ☑ Exchange 5.5

- ❑ Install Service Pack 4 (SP4) for Exchange Server 5.5. This service pack offers a variety of bug and security fixes. The service pack is cumulative (in other words, SP4 contains all the fixes and features of SP1 through SP3).

- ❑ At the time of this writing, Microsoft had released the several security relevant patches or hot fixes for Exchange Server 5.5. It is recommended to review the security bulletins at http://www.microsoft.com/technet/security/current.asp for the latest information. It is critical to install security related fixes as soon as possible.

Post Installation

There are very few items within the Exchange Server directory that require general user access; however, access rights are liberally granted by default. In order to revoke unnecessary access permissions, the following permissions are recommended for the directories where the Exchange Server is installed. It is also necessary to change the rights associated with the mapisvc.inf file.

- ❑ Give the following accounts Full Control access to all directories, subdirectories, and files within the directories where the Exchange Server was installed:
  - ❑ CREATOR OWNER
  - ❑ Domain Admins
  - ❑ Exchange_Primary
  - ❑ SYSTEM
  - ❑ <All Exchange Administrator Groups>
- ❑ Make certain that no other accounts are given access – it is particularly important to make certain that the group “Everyone” is not allowed access.

- ❑ Modify the permissions associated with the file %SystemRoot%\SYSTEM32\mapisvc.inf to allow the “Authenticated Users” group Modify access.

☑ Exchange 5.0 □ Exchange 5.5

- ❑ If you wish to share files from the sampapps\clients directory, add “Authenticated Users” with read access.

NOTE: Additional changes are necessary to Exchange Server directory and file permissions for those installations that access their Exchange Servers via Internet Explorer. Those changes are detailed in Chapter 8.

Chapter

2

Client Installation

The discussion in this chapter applies to the clients most commonly associated with Microsoft Exchange – the Exchange Client, Outlook 97, and Outlook 98.

Installation

It is important to use the most recent releases of the clients. Releases prior to those listed below do not include important features related and/or fixes for security vulnerabilities. It is also recommended to install the clients to a directory in a partition other than where the operating system is located.

When installing clients:

- If installing Outlook 97, use version 8.02 (or later).
- If installing the Exchange Client, use version 5.0.1458 (or later).
- If using Outlook 98, install the following patches:
  - Olcsp128.exe. The Olcsp128.exe hotfix updates the Outlook 98 S/MIME security feature to work with the new X.509 version 3 certificates available in the latest version of the Key Management Server that ships with Exchange Server 5.5 Service Pack 1 (or later). It also addresses an issue with renewing security keys after changing enrollment settings (a topic which will be discussed in Chapter 7). This fix can be found on the Exchange Server 5.5 Service Pack 1 (or 2) CD.
  - Ol98qfe.exe. The Ol98qfe.exe hotfix includes many protocol and client connectivity fixes required by the Outlook 98 client to work correctly with the latest Advanced Security features. One of these fixes includes an issue where messages sent to multiple recipients using S/MIME encryption cannot be decrypted by recipients using Outlook 98. This problem usually occurs when there are more than 15 recipients. This fix can be found on the Exchange Server 5.5 service pack CD. Reference: http://support.microsoft.com/support/kb/articles/q191/8/99.asp.
  - O98secu.exe. This patch improves the security of Outlook 98 by blocking file attachments that could contain malicious code. Attachments that obviously contain executable content – referred to as "Level 1" attachments in the Microsoft lexicon -- are stripped from incoming messages and from all previously saved messages. The patch and a complete listing of the file types that are considered Level 1 are provided at http://office.microsoft.com/Downloads/9798/Out98sec.aspx. This patch handles

what is defined as “Level 2” attachments in a different manner. Level 2 files are not blocked, but instead the user is required to save them to the hard disk before executing. This is intended to cause the user to pause before acting and not just absent-mindedly launch a potentially malicious attachment. By default, no file types are included in Level 2; however, the administrator can, in some cases, define the files types that should be included in Level 2 as well as modify the file types defined as Level 1. These modifications can only be made in instances where the user is connecting to an Exchange server and is not using .pst files for mail storage. The patch also controls access to the Outlook address book as a countermeasure against malicious code that replicates by auto-forwarding itself to a user’s contacts and provides protection against malicious embedded objects and scripts. A complete description and installation instructions are provided at the office update URL.

- Cdoup98.exe. In addition to using the Outlook object model to access the Outlook address book, a malicious program could also use Outlook Collaborative Data Objects (CDO). While O98secu.exe removes CDO from Outlook 98, this may be a feature that internal applications rely upon. If it is desired to reinstate CDO, use cdoup98.exe http://office.microsoft.com/downloads/9798/Cdoup98.aspx

- At the time of this writing, Microsoft had released the several security relevant patches or hot fixes for Outlook. It is recommended to review the security bulletins at http://www.microsoft.com/technet/security/current.asp for the latest information. It is critical to install security related fixes as soon as possible.

- It is also important to apply the latest patches to Internet Explorer. Some attacks, such as the BubbleBoy virus, use mail messages sent to an Outlook client to launch exploits against Internet Explorer vulnerabilities. It is recommended to review the security bulletins at http://www.microsoft.com/technet/security/current.asp for the latest information. It is critical to install security related fixes as soon as possible.

- Install the client to a partition other than where the operating system is located.

Post Installation

After installation is completed, the following permissions are recommended for the directories where the client is installed. Note that some of these recommendations reflect minor changes to the permissions invoked by the “*Guide to Secure Microsoft Windows NT Networks*” and are necessary for the Exchange environment to function properly.

The following permissions related to the clients are recommended:

- For the directory where the client was installed, apply the following permissions to all subdirectories and files:

  - Authenticated Users: Modify

  - CREATOR OWNER: Full Control

- Domain Admins: Full Control
- SYSTEM: Full Control

- Give "Authenticated Users" Modify access to the file %SystemRoot%\forms\frmcache.dat. This change is necessary for the clients to function properly.

Other Client Files

☑ Exchange Client ☑ Outlook 97 ☐ Outlook 98

In an environment where multiple people share the same workstation, it is probable that multiple user mail profiles will be created on a single machine. If this happens, file access errors can occur when using the Exchange Client or Outlook 97 client if multiple users select the same name for their profiles as a consequence of the tightened file permissions associated with the "*Guide to Secure Microsoft Windows NT Networks*." To avoid this problem, user profiles should be given unique names. A suggested method for insuring this is to use the account name in the profile as illustrated below:

- When creating user profiles, use unique names for the profiles based upon the account name, as in "%account name% outlook"

This is not an issue when using Outlook 98 due to differences in the manner in which the profiles are stored.

☑ Exchange Client ☑ Outlook 97 ☐ Outlook 98

The Personal Folders, Personal Address Books, and Offline Folders that can be created as part of a user's mail profile can be of concern from a security perspective. For example, if two users on the same Windows NT machine define a profile that includes the same Personal Folder (an easy thing to do if the defaults are accepted under the Exchange Client and Outlook 97), then they could end up with the ability to read each other's downloaded mail. To prevent this and other similar problems, the following guidelines are recommended.

- When creating user profiles, the following guidelines are recommended for storage location and file name:

File	Description	Default Location	Recommended Location
*.pst	Personal folder	%Systemroot%	%Systemroot%\Profiles\[username]\Personal Suggested name: <mailbox name>.pst
*.pab	Personal address book	%Systemroot%	%Systemroot%\Profiles\[username]\Personal Suggested name: <mailbox name>.pab
*.ost	Offline folders	%Systemroot%	%Systemroot%\Profiles\[username]\Personal Suggested name: <mailbox name>.ost

As a consequence of invoking the "*Guide to Secure Microsoft Windows NT Networks*", following these recommendations will ensure that the files inherit appropriate permissions to preclude inadvertent sharing between users.

☐ Exchange Client ☐ Outlook 97 ☑ Outlook 98

Outlook 98, by default, stores personal folders, address books, and offline folders files in the %Systemroot%\Profiles\<username>\ directory. It is recommended to accept the default location. Appropriate file permissions will be inherited as a consequence of invoking the "*Guide to Secure Microsoft Windows NT Networks*" to ensure that the files are not inadvertently shared between users.

Chapter

3

Administrative Permissions

Introduction

In addition to the file and directory permissions established at the operating system level, Exchange introduces application level permissions which are the topic of this chapter. The rights associated with a given user are a combination of rights established at the application level and the operating system level. For example, a Windows NT user account with Administrative rights to NT does not necessarily have the appropriate permission within Exchange to administer the Exchange server. These rights must be expressly granted through the Exchange Administrator tool.

It is impossible for these guidelines, which are intended for general usage, to expressly detail the exact permissions that should be applied to the plethora of containers and objects contained within the Exchange Administrator tool. Instead, this chapter will focus on some key concepts that should be kept in mind when assigning administrative privileges.

Use of Exchange Administrators Account(s)

In order to simplify the assignment of administrative rights to the Exchange Server, it is recommended that a separate Windows NT Exchange Administrators Group – or Groups - be established. It is strongly recommended that you do not use the Windows NT administrator group, as it is not necessary to have Windows NT administrative rights for many Exchange administration functions.

Having a separate Exchange Administration Group, or Groups, offers several benefits. First, it will preclude the need for Exchange administrators to log in unnecessarily as a Windows NT administrator -- something that should be avoided for security reasons. Second, it will allow you to partition administrative rights. You may reserve the right to reconfigure the Exchange server to a select few, while allowing several individuals to manage mailboxes, for example. And finally, having an Exchange administrator group(s) will simplify the process of managing administrative rights -- adding a new administrator is as simple as making them part of the Exchange Administrator Group.

Roles

The Exchange Administrator tool allows various degrees of administrative rights to be applied in fine detail to the various levels of the Exchange hierarchy. Microsoft Exchange has a number of predefined roles to assist in assigning administrative privileges. These predefined roles are identical *in concept* to the roles defined under Windows NT (such as giving "Read" access to a file which is a package of rights that gives the user Read and Execute permission on the file).

These predefined roles are well defined in the Exchange Server help facility. A few of these roles are somewhat confusing and their misapplication could result in security concerns, most notably the "permissions admin" role and "admin" role.

An individual with admin rights has the capability to perform day-to-day administration on an Exchange server. They can add mailboxes and manipulate numerous Exchange settings. The permission admin right includes all these rights plus the ability, as the name implies, to change the permission rights on the various objects within the Administrator tool. Permission admin rights can be dangerous as a rogue administrator with those rights could give themselves "send as" rights to a mailbox and effectively be able to masquerade as another user.

Understanding Inheritance

Permissions can be set on every object with the Exchange Administrator tool – in large organizations with many users, the total number of objects could be astronomical. Fortunately, permissions are, for the most part, inherited from the parent container which greatly simplifies the task of assigning permissions. It is important to understand how permissions are inherited with the Exchange Administrator tool to ensure that the permissions are set up properly.

Generally speaking, the effective permissions granted a user on a directory object are the sum of two types of permissions:

- The permissions the user account has on that object; and

- The permissions the user account inherits from above. The account inherits only the permissions assigned to the same user account on object(s) above it in the hierarchy. The inheritance does not end at the immediate parent. It continues up the directory tree to the top level of the hierarchy.

The only exception to this general description of inheritance is the configuration container. Due to its critical role, the configuration container does not inherit permissions.

Summary

In summary, when assigning administrative permissions in the Exchange environment it is recommended that:

- The Windows NT administrator's group not be used.
- Partitioning Exchange Administrative rights through the use of multiple Exchange Administrative groups should be considered.
- Judicious use of the role "permission admin" should be made.
- The role inheritance plays in the assignment of permissions must be fully understood.

Chapter

4

Core Component Administration

Introduction

Figure 1 illustrates the basic components of Microsoft Exchange Server 5.0/5.5. These components work in concert to process information from client software packages, to synchronize servers in multi-server environments, and to perform general Exchange housekeeping.

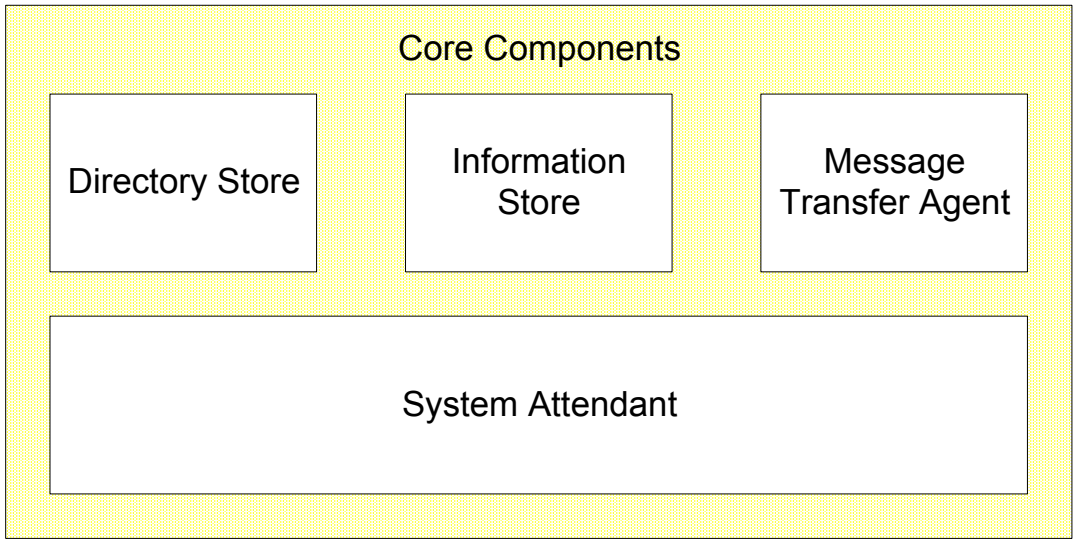

Figure 1 Exchange Server Core Components

Directory Store

The Microsoft Exchange Server's Directory Store contains all the information about a site that is required to process data delivery. This includes addresses, distribution lists, details about public folders and mailboxes (but not the public folders and mailboxes themselves), and configuration information about the Exchange environment. The Directory Store provides a single, central location where administrators, users, and applications can look up and configure information about a variety of objects, such as user mailboxes. The directory also generates address books that contain information about users, such as e-mail addresses and other related information.

The Directory Store is also responsible for enforcing security on all the directory objects, such as user mailboxes.

The Directory Store is managed at both the site and server level where, from a security perspective, two items are of interest – Lightweight Directory Access Protocol (LDAP) access and diagnostic logging.

Site Level

LDAP is a protocol that allows a client to query the Exchange directory for a variety of information related to the Exchange users. Directory store settings at the site level allows control over the information that is exported to LDAP clients under three scenarios --- anonymous requests, authenticated requests, and inter-site replication. It may be desirable, for example, to allow fully authenticated users (those who log on using a Windows NT account) full access to all user attributes as they browse the Exchange Directory Store. However, it may not be desirable to allow anonymous users, who by definition are not authenticated, to be able to access a complete listing of the users on your Exchange network. It is recommended that careful consideration is given to the information enabled for export via LDAP, particularly in relation to anonymous requests.

LDAP export settings are administered at the site level in the Exchange Administrator tool:

- Select the **DS Site Configuration** object under the Configuration object. Then select **File/Properties** and the "Attributes" tab. Consider carefully the attributes available for export via LDAP, particularly in relation to anonymous users.

Server Level

Diagnostic logging is a feature that is primarily intended to allow the administrator to log any of a plethora of events to aid in diagnosing system problems – it is recommended that a few of the events be logged as standard practice.

Directory Store diagnostic logging levels are administered from the server level in the Exchange Administrator tool:

- Select the appropriate **server** under the Servers object. Then select **File/Properties**. Then select the "Diagnostic Logging" tab and highlight the MSExchangeDS entry. It is recommended to log the following at the "maximum" level:
  - LDAP Interface
  - Security

Use the Windows NT event viewer to view logged events.

Information Store

The Information Store is responsible for maintaining and accessing messages in response to client requests. The Information Store consists of two components, a Private Information Store and a Public Information Store.

The private store is primarily for user mailboxes and consists of messages sent from user to user. They are accessible by the mailbox owner and others for whom access has been allowed. The public store is used for newsgroups and other objects for which wide access is typically defined. Each store can hold just about any kind of object -- mail, files, voice mail, and links to other files.

The Information Store is managed in the Exchange Administrator at both the site and server levels where, from a security perspective, two items are of interest at both levels.

Site Level

At the site level, message tracking and top-level folder creation are of interest.

Enabling message tracking instructs the Exchange server to create a daily log file of all messages that are handled by the Information Store. That log can be used to track messages through the Exchange Server environment. This could be useful in various security contexts. For example, if a user inadvertently introduces one of the infamous Word macro viruses, message tracking could be used to determine just how far the infected document has spread.

To enable message tracking on the Information Store, from the Exchange administrator:

- Select the **Information Store Site Configuration** object under the configuration object and then select **File/Properties**. Enabled message tracking from the "General" tab.

Public folders are created via clients, not the Exchange Administrator Tool. The top-level folder creation settings allow the administrator to control who has that right. Note that the default condition is that everyone can create public folders. Depending on the sensitivity of the data and the manner in which public folders are used, it may be desirable to curtail the rights of individuals to create public folders. (For example, public folders may be used to hold newsgroups which are available for access remotely via newsreaders.) This setting also has implications in relation to the security of custom applications within the Exchange environment, as will be discussed in Chapter 10.

To control who can create public folders, from the Exchange Administrator tool:

- Select the **Information Store Site Configuration** object under the configuration object and then select **File/Properties** and the "Top Level Folder Creation" tab. Depending upon the specific usage of public folders, it may be desirable to restrict this right.

Server Level

At the server level, the logons feature and diagnostic logging are of interest.

There are no specific security settings in relation to the logons feature. The intent of the feature is to provide an easy way to determine who is logged onto the Information Store at any given time.

To determine whom is logged onto the Private Information Store via the Exchange Administrator tool:

- Select the **Private Information Store** object under the server object. Then select **File/Properties** and the "Logons" tab.

To determine whom is logged onto the Public Information Store:

- Select the **Public Information Store** object under the server object. Then select **File/Properties** and the "Logons" tab.

The diagnostic logging feature of the Information Store is identical in function to that of the Directory Store, as described above. It is recommended that diagnostic logging be enabled for a number of events related to both the private and Public Information Stores.

To enable diagnostic logging for the Private Information Store, via the Exchange Administrator tool:

- Select the **Private Information Store** object under the server object. Then select **File/Properties** and the "Diagnostics Logging" tab. Highlight the MSExchangeIS/Private object. It is recommended to log the following at the "maximum" level:
  - Logons
  - Access Control
  - Send On Behalf Of
  - Send As
  - Download

To enable diagnostic logging for the Public Information Store, from the Exchange Administrator tool:

- Select the **Public Information Store** object under the server object. Then select **File/Properties** and the "Diagnostics Logging" tab. Highlight the

MSExchangeIS/Public object. It is recommended to log the following at the "maximum" level:

- Logons
- Access Control
- Send On Behalf Of
- Send As
- Download

Use the Windows NT event viewer to view logged events.

Message Transfer Agent

The Message Transfer Agent routes messages between Exchange servers. The Message Transfer Agent is used anytime a message has to go off a server.

The Message Transfer Agent is managed at both the site and server levels in the Exchange Administrator where, from a security perspective, two items are of interest – message tracking and diagnostic logging. Message tracking and diagnostic logging for the Message Transfer Agent are identical in concept to that of the Directory Store and Information Store.

Site Level

Message tracking is enabled at the site level in the Exchange Administrator:

- Select the **MTA Site Configuration** object from within the configuration object, and then select **File/Properties**. Message tracking is enabled from the "General Tab."

Server Level

Message transfer agent diagnostic logging levels are administered from the server level in the Exchange Administrator:

- Select the **Message Transfer Agent** object from the appropriate server object, and then select **File/Properties** and the "Diagnostic Logging" tab. It is recommended to log the following at the "maximum" level:
  - Security

- Configuration

Use the Windows NT event viewer to view logged events.

Chapter

5

Multi-Server Configurations

Server-to-Server Communications

Server-to-server communication in the Exchange environment is necessary to facilitate message transfers between users on different servers and for replication of directory information and public folders between servers.

Communication between servers is facilitated by use of a "connector" to connect the server's message transfer agents. The security posture of the Exchange environment is very dependent on which connector is used and how it is configured. There are several types of connectors available:

- Site Connector. The site connector uses remote procedure calls (RPCs) for server-to-server communication.
- X.400 Connector. The X.400 connector can be used for connectivity between servers in different sites as well as connecting to other X.400 compliant mail systems. The connector complies with both the 1984 and 1988 CCITT X.400 standards.
- Dynamic Remote Access Service Connector – The dynamic remote access service (RAS) utilizes the Windows Remote Access Service for part-time network connection between Microsoft Exchange Server sites.
- Internet Mail Service (IMS). The IMS connector supports message transmission using the Simple Mail Transport Protocol (SMTP) – the mail protocol used on the Internet. The IMS connector can be used for connectivity between servers in different sites as well as connecting to other SMTP compliant mail systems.

For connecting two servers within the same Exchange site, only the Microsoft Exchange Site Connector can be used. Data sent via the site connector is automatically encrypted using RC4 128-bit encryption (in the North American version of Exchange). Server-to-server communications are authenticated using the standard Windows NT challenge/response.

For communications between sites, there are more numerous options. The site connector can be used here, as well. When using the site connector in this manner, once again encryption is automatically invoked. No encryption is available when using the X.400 connector and authentication is via simple, plaintext passwords. When using the dynamic remote access connector, security is dependent on the setup of the Windows

NT Remote Access Service (RAS). With RAS, 128-bit RC4 encryption is an administrator option. Authentication under RAS is available via three mechanisms – the Challenge Handshake Authentication Protocol (CHAP), Shiva Password Authentication Protocol (SPAP), and Password Authentication Protocol (PAP). The use of PAP should be avoided as it does not provide for encryption of the authentication process. RAS is covered in detail in the "*Guide to Implementing Windows NT in Secure Networking Environments."* Finally, the Internet mail service can be used to connect servers. Here, RC4 encryption and authentication are administrator selectable options.

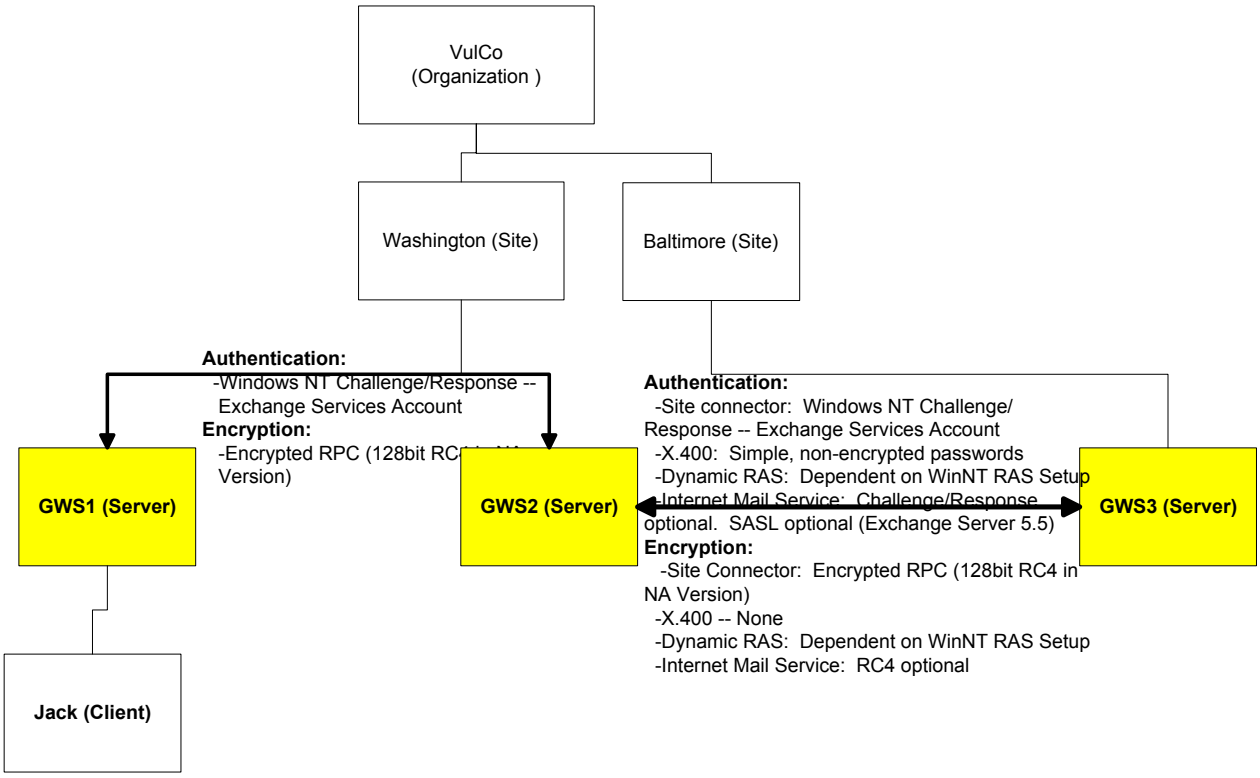

Figure 2 Server-to-Server Security Options

Exchange to "Foreign" E-mail System

Exchange can also connect to what Microsoft terms "foreign" e-mail systems. Foreign e-mail systems are simply e-mail networks outside of the Exchange environment, such as X.400 and Simple Mail Transport Protocol (SMTP) mail systems. Exchange Server 5.0 and Exchange Server 5.5 provide connectors for both of these. Exchange Server 5.5 and third party vendors offer additional connectors that are not covered in this document.

The X.400 connector provides connectivity to X.400 hosts. Server-to-server communication between Exchange and X.400 hosts is not encrypted, nor is any kind of robust authentication provided. Only plain text authentication is available as an option.

The Internet Mail Service (IMS) provides connectivity to SMTP hosts. In Exchange Server 5.0 there are no encryption or authentication options when connecting to non-Exchange SMTP hosts. In Exchange Server 5.5, Secure Socket Layer (SSL) encryption and Simple Authentication and Security Layer (SASL) authentication can be used provided these features are supported by the other hosts with which the Exchange Server will connect. Please note that this feature is not well documented and attempts by the author and others to enable SMTP over SSL have failed.

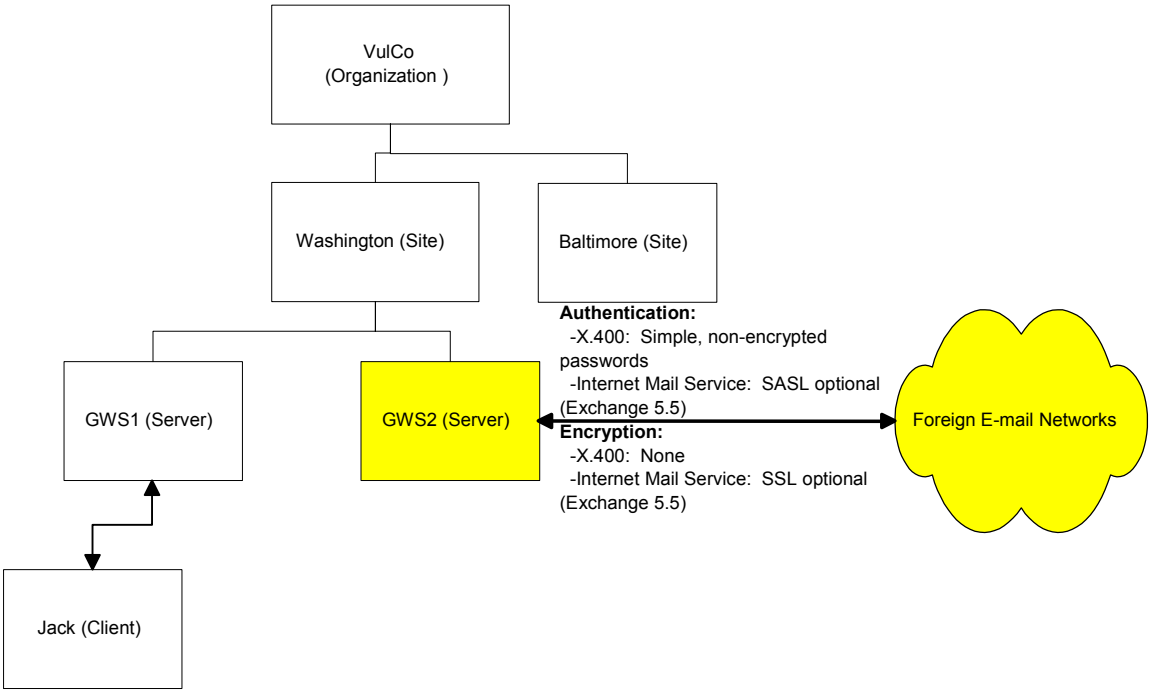

Figure 3 Exchange to "Foreign" E-mail Systems -- Security Options

Summary

When connecting servers in an Exchange environment:

- Consider the encryption and authentication features provided when selecting a connector.

- If using the Internet Mail Service as a server-to-server connector, it is recommended that encryption and authentication be enabled. To do so, select the **Internet Mail Service** object under the site/configuration/connections object and select **File/Properties** and the "Security" tab. If using "Windows NT challenge/response and encryption", enter an account name and password chosen unique for this function.

- If using the Dynamic Remote Access Service connector, configure RAS per the "*Guide to Implementing Windows NT in Secure Networking Environments."*

Chapter

6

Internet Mail Service

Chapter 5 dealt with the use of the Internet Mail Service (IMS) in providing connectivity between Microsoft Exchange servers and touched on its use as a gateway for Simple Mail Transport Protocol (SMTP) traffic. This chapter rounds out the discussion on use of the IMS as a SMTP gateway.

There are, from a security perspective, six areas of interest in relation to using the Internet Mail Service as a SMTP gateway:

- Limiting message size -- controlling the maximum size of incoming/outgoing messages. From a security perspective, this is of interest given the restrictions that can be placed on the size of incoming messages. If an incoming message from another SMTP host exceeds the set limit, the Internet Mail Service does not write any data beyond the set limit. This prevents large messages from filling up the disk space on your Exchange server, reducing the threat of denial of service attacks.
- Message tracking -- enabling message tracking instructs Exchange to create a daily log file of all messages that are handled by the IMS. This can be useful in a variety of security contexts when it is desirable to understand the flow of a message through the Exchange environment.
- Disabling auto-replies -- disabling auto-replies for messages received via the IMS. Users can set up out-of-office messages that are sent automatically on receipt of a message. In some cases, it is possible that the information a user might include in this message should not be shared outside the organization. This could create a problem if the out-of-office messages were sent in response to e-mails from the Internet. Also, by default, the Internet Mail Service includes the sender's display name, in addition to the sender's address, in outbound messages. This can be disabled as well.
- Restricting user access -- controlling which Exchange users can/cannot send outgoing messages through IMS. The Internet Mail Service can be set up to accept or reject messages from any sender listed in the Microsoft Exchange Server address book. WARNING: This feature is of limited value. It is of utility only for restricting individuals who are logging into the Exchange Server natively. These settings do not apply to individuals who access the Exchange Server through SMTP.
- Accepting/rejecting SMTP connections – controlling from which IP addresses incoming SMTP messages are accepted. If an Exchange server is not intended for universal access, the IMS can be set to accept or reject messages based upon IP address. Exchange Server 5.5 offers some additional capabilities for controlling SMTP connections. With version 5.5 it is possible to:
    - Limit SMTP connections to those that are authenticated, encrypted, or both. This restriction applies to both connections with other hosts and client connections. The authentication mechanisms available when connecting to

other hosts were detailed in Chapter 5. The method a client uses for logging into the SMTP service is controlled by the user at the client end. There are two options -- logging in via an account name and password entered by the user and transmitted as a base64 encoded message and logging in using Secure Password Authentication (SPA). The latter is defined, in Microsoft documentation, as "any authentication in which the actual password is not sent over the network". However, for SMTP login SPA simply does not work. If the client is setup to use SPA it simply will not accept it -- it reverts to the account name and password option without any error indication. The result is that the password is sent as a base64 encoded value -- anyone with a simple, and easily available, utility could decode a captured password. The bottom line is that there is no truly robust method available to authenticate client access to SMTP connections.

- ♦ Restrict access to clients that are homed on the server. This option requires the user to have a mailbox on the Exchange Server before a connection will be allowed. This can be used to restrict SMTP connectivity to users served by the Exchange Server.
- ♦ Accept clients only if authentication account matches submission address. This option precludes a user from masquerading as another when dropping off a message via SMTP. Of course, given the issue with the lack of a robust mechanism to protect user passwords in transit, this feature is of limit value in countering a determined adversary.

- ■ Exchange Server 5.5 supports the Secure Multi-Purpose Internet Mail Extension (S/MIME) for message confidentiality, confidentiality and integrity. As part of the S/MIME standard, clients can add a signature to a message that is used by the recipient to verify the identity of the user. In order to preserve these signatures as messages pass through the Internet Mail Service it is necessary to enable this option. S/MIME will be discussed further in Chapter 7.

To configure the Internet Mail Service, first select the **Internet Mail Service** object under the connections object in the Exchange Administrator tool, select **File/Properties** and then:

- ❑ Select the "General" tab to set a message size limit. It is recommended that a message size limit that is reasonable for the environment the IMS is connected be set. Note that whatever limit is set applies to both incoming and outgoing messages.
- ❑ Select the "Internet Mail" tab to set message tracking. It is recommended that message tracking be enabled.
- ❑ From the "Internet Mail" tab, click on "Interoperability" (Exchange Server 5.0) or "Advanced Options (Exchange Server 5.5). It is recommended that the following be disabled:
  - ❑ Out of office responses
  - ❑ Automatic replies
  - ❑ Display names

- Select the “Delivery Restrictions” tab. These settings are advertised to restrict which Exchange users can/cannot send outgoing messages through IMS; however, they have no effect upon users accessing the Exchange Server through SMTP.

  ☑ Exchange 5.0 ☐ Exchange 5.5

- Select the “Connections” tab, check “Accept or reject by host” and select “Specify Hosts.” Unless an Exchange server is intended for universal access, it is recommended to restrict access.

  ☐ Exchange 5.0 ☑ Exchange 5.5

- Select the “Connections” tab. Unless an Exchange server is intended for universal access, it is recommended to restrict access by use of one or more of the following:

  - Use the “Accept Connections” option to require authentication, encryption, or both on all SMTP connections (applies to both client connections and connections to other hosts).

  - Use the “Clients can only submit if homed on this server” option to require the user to have a mailbox on the Exchange Server before a connection will be allowed.

  - Use the “Clients can only submit if authentication accounts matches submission address” option to help preclude a user from masquerading as another when dropping off a message via SMTP.

- Select the “Internet Mail” tab. Enable (check) “Clients support S/MIME signatures” if S/MIME will be used.

Note: An additional IMS security related setting, “securing outbound connections” (security tab), is discussed in Chapter 5.

Chapter

7

Client Security and "Advanced Security"

Introduction

Chapter 2 described issues related to the installation of the Exchange client and Outlook clients. This chapter will address other issues related to the clients, specifically protection against malicious file attachments, the use of encryption to protect messages, and methods that users can apply at the client to manage access to their mailboxes or public folders.

File Attachment Security

Executable content is a term that refers to files or other objects that contain an executable component. This executable component could serve a useful application or it could be malicious – an example being a Word macro virus.

Both the Exchange client and the Outlook 97/98 client can be set to monitor mail messages for some forms of executable content. Upon launching of these kinds of executable content, the client will provide notification that an executable is about to launched and offer the opportunity to cancel the action. Outlook 98 also offers, via patch O98secu.exe, the ability to strip attachments from incoming mail messages as described in Chapter 2.

Note that the option to monitor for executables only exists in recent versions of the clients -- Outlook 97 version 8.02 or higher, Exchange client version 5.0.1458 or higher, and Outlook 98. Attachment blocking is only available in Outlook 98 with the O98secu.exe patch installed.

To enable file attachment security:

☑ Exchange Client ☑ Outlook 97 □ Outlook 98

- Verify the proper versions of Outlook 97 and/or the Exchange client are being used -- Outlook version 8.02 or higher and Exchange client version 5.0.1458 or higher.

- Verify the option to check for executable file attachment is enabled (which is the default). From the client, select **Tools/Options** and the "Attachments" tab. Under "Security Method," select the option "High."

Please note that file attachment security, while useful, is limited.

The Outlook and Exchange clients are very good at detecting obvious forms of executable content, such as *.exe, *.bat, and *.com files. They provide no mechanisms against embedded hyperlinks, which could point to a potentially dangerous executable, nor do they detect other forms of executable content, such as Microsoft Word macros or potentially dangerous OLE embedded objects. Microsoft provides for protection against some of these threats through the associated application. For example, both Internet Explorer and Microsoft Word have security mechanisms that can be enabled to help counter the executable content threat.

Likewise, file attachment security offers no protection against attacks contained within the body of an e-mail. Microsoft's "security zones", described in the next section, offer protection against this threat.

☐ Exchange Client ☐ Outlook 97 ☑ Outlook 98

- ❑ As mentioned in Chapter 2, install the patch O98secu.exe to improve the performance of attachment security.

- ❑ If electing not to install this patch, then verify the option to check for executable file attachments is enabled (which is the default). From the client, select **Tools/Options** and the "Security" tab. Click on "Attachment Security," select the option "High." This will provide the minimal level of protection as described above.

Security Zones

☐ Exchange Client ☐ Outlook 97 ☑ Outlook 98

Outlook 98 can take advantage of Internet Explorer security zones to protect against malicious code, (ActiveX controls, Java, or scripts) embedded into the body of messages. Internet Explorer includes a capability to restrict the execution of such code based upon four zones. Before jumping into how Outlook 98 uses these settings, a quick review of their use in Internet Explorer is in order.

- Local Intranet zone: This zone contains addresses that are typically behind the organization's firewall or proxy server. The default security level for the Local Intranet zone is "medium".
- Trusted Sites zone: This zone contains sites that are trusted -- sites that are believed not to contain files that could corrupt the computer or its data. The default security level for the Trusted Sites zone is "low".
- Restricted Sites zone: This zone contains sites that are not trusted -- that is, sites that may contain content that, if downloaded or ran, could damage the computer or its data. The default security level for the Restricted Sites zone is "high".
- Internet zone: By default, this zone contains anything that is not on the computer or an intranet, or assigned to any other zone. The default security level for the Internet zone is "medium".

For each zone, one of four levels of restrictions can be enabled:

- High: Do not execute
- Medium: Warn before executing
- Low: Run without warning
- Custom: Establish custom settings

Outlook 98 utilizes these zones in that you can select which of two zones -- the Internet zone or the Restricted zone -- Outlook messages fall into. The settings for the selected zone are then applied by Outlook to all messages. While the Outlook 98 patch O98secu.exe sets the zone to "Restricted sites", it is not quite as conservative as it should be in regards to some of the settings which underlie the Restricted site. It is therefore recommended to:

- Use the Restricted zone. To set the zone, select **Tools/Options** and the "Security" tab. Select "Restricted sites" from the zone drop-down box.
- Set the settings for the Restricted zone as recommended below by selecting "Zone Settings" and clicking on "Custom Level". Note that changes made here will also apply to the Restricted zone when web surfing with Internet Explorer. These recommendations apply specifically to Internet Explorer 5.0; the options available under Internet Explorer 4.0 are similar but do not include all of the settings.
  - Download signed ActiveX controls - DISABLE
  - Download unsigned ActiveX controls - DISABLE
  - Initialize and script ActiveX controls not marked as safe - DISABLE
  - Run ActiveX controls and plug-ins - DISABLE
  - Script ActiveX controls marked safe for scripting - DISABLE
  - Allow cookies that are stored on your computer – DISABLE
  - Allow per-session cookies (not stored) - DISABLE
  - File download - DISABLE
  - Font download - DISABLE
  - Java permissions – DISABLE JAVA
  - Access data sources across domains – DISABLE
  - Don't prompt for client certificate selection when no certificates or only one certificate exists -- DISABLE
  - Drag and drop or copy and paste files - DISABLE
  - Installation of desktop items - DISABLE

- Launching programs within an IFRAME – DISABLE
- Navigate sub-frames across different domains - DISABLE
- Software channel permissions - HIGH SAFETY
- Submit nonencrypted form data - DISABLE
- Userdata persistence - DISABLE
- Active scripting - DISABLE
- Allow paste operations via script - DISABLE
- Scripting of Java Applets - DISABLE
- Logon - Anonymous logon

Note that following these recommendations will disable many advanced features; however, for the vast majority of e-mail users there will be no operational impact. This is because most e-mail messages are simple text messages with attachments. The features that are disabled deal primarily with script and controls embedded within the body of the message which is not typically done.

Note once again that these settings are shared with the Internet Explorer browser and web pages typically DO incorporate the kinds of features which are disabled via these settings. While this could represent an operational impact, keep in mind that the Restricted zone is intended to include those sites that are not trusted - one should restrict what those sites can do and in fact these recommended settings are only slightly more restrictive than the default settings for this zone. Also note that descriptions of these settings simply are not provided by Microsoft or documented in any known public documentation. As a consequence, we are investigating the settings further and may make some modifications to our recommendations as our efforts mature.

Using these settings will counter known attacks that use active content contained within the body of e-mail messages such as the BubbleBoy virus. Note that these settings do not guard against attacks contained within an e-mail attachment, such as Word macro viruses. File attachment security, which was discussed in the prior section, is applicable to this kind of threat.

Respecting the Concept of Least Privilege

Least privilege is a basic tenet of computer security that basically means “giving a user only those rights that s/he needs to do their job”. Executable content runs in the security context on which it was launched – practically speaking, this means in the context of the user launching the code. Good practices include making certain that administrative accounts are kept to a minimum, that administrators use a regular account as much as possible instead of logging in as administrator to do routine things such as reading their mail, and setting resource permissions properly. This will limit the access of any malicious executables that may be inadvertently launched.

- Respect the concept of least privilege – give users only those rights and access that they need to do their job

Client-to-Server Encryption

RPC Encryption

By default, client-to-server communication is NOT encrypted. There are two methods that can be used to provide encryption when using the Exchange client or Outlook clients. The first is by setting options in the client to use encrypted Remote Procedure Calls (RPC). When the encrypted RPC option is enabled, 128-bit RC4 encryption is used on the link between the client and server. Using encrypted RPC provides a level of security with very little overhead, although it can be noticeable on slow, dial-up accesses. Note that using encrypted RPC only protects the messages in transit to the server where they are decrypted for storage.

To enable RPC encryption, from the client:

- Select **Tools/Services** and the select "Microsoft Exchange Server." Choose "Properties" and the "Advanced" tab. Under "Encrypted Information," select both options.

"Advanced Security" – Exchange Server 5.0

The second method of securing client-server communication is through the use of what Microsoft terms "Advanced Security." While the concepts are the same, the implementation details are quite different between Exchange Server 5.0 and Exchange Server 5.5 with Service Pack 1 (or later). For that reason, the two versions will be discussed separately.

Advanced security consists of a public key based technology that provides for message encryption and decryption, authentication, and message integrity. A Key Management Server (KMS), which is an optional installation available on the Exchange Server CD, is used to create and distribute keys, allocate and revoke security certificates as required, place public credentials in the Directory Store, replace user keys that have been corrupted, and perform other management functions in relation to the public key features. While the KMS is a critical component of the advanced security features in Exchange, the security workload is actually split between the client and server. The client performs the actual encryption and decryption of messages as well as the application and verification of digital signatures. The client also stores the user's private key in an encrypted manner. The Exchange client and Outlook 97 store the information in a file (*.epf) while Outlook 98 uses the registry.

When advanced security is invoked, several administrator-selected options are available for the encryption/decryption algorithm:

- DES. The Digital Encryption Standard is an algorithm validated by the National Institute of Standards and Technology (NIST). This is available only in the North American version of Exchange and it uses a 56-bit key.
- CAST. CAST is named after Carlisle Adams and Stafford Tavares of Northern Telecom Research. A 64-bit version is available in the North American release of Exchange; a 40-bit version is used in the international release.

Certain algorithms are not available for international use due to restrictions the US has imposed on exporting encryption algorithms. In the event that a North American user who is enabled with DES or 64-bit CAST sends a message to someone who is only enabled with the 40-bit version, Exchange automatically downgrades to the 40-bit version for that message.

Message Digest 5 (MD5) is used for the digital signatures that provide the authentication and data integrity features. MD5 results in a 128-bit hash value. Since the US has no export restrictions on algorithms used for these security features, the same version is used in the North American and international releases.

The use of advanced security has several advantages over the use of RPC encryption. When using advanced security, an encrypted message remains encrypted until decrypted by the recipient; messages encrypted using RPC encryption are only encrypted in transit from the client to server and stored in unencrypted form once they reach the server. Also, advanced security supports authentication and message integrity -- features not available when using RPC encryption. For these reasons, the use of the advance security features is recommended.

In addition to algorithm selection, the installation and use of the Key Management Server requires the Exchange administrator to make several decisions and perform several actions that are security critical:

- Installation. It is recommended that the Key Management Server be installed in the same directory as the Exchange Server (typically “exchsrvr”) so that the KMS directory will inherit the appropriate permissions. If you choose to install the KMS to another location, the recommended directory and file permissions are those outlined for the Exchange server directory in Chapter 1.
- Access. During the installation of the Key Management Server, the administrator decides whether or not to use a manual password versus a disk password. Each has its advantages and problems. For the manual password, memorizing the long password may be difficult and writing it down is potentially non-secure. When saving the password to disk, the password is not encrypted on the disk and is readable to anyone who obtains the disk -- the disk must be kept in a secure place. The use of a floppy disk to store the Key Manager password requires that the Key Manager service have access to the floppy. Per the “*Guide to Secure Microsoft Windows NT Networks*”, the floppy disk is allocated at logon and is no longer available to the Key Manager service. In order for the Key Manager service to access the floppy, it is necessary to change this setting. The C2 Configuration Manager tool provides a very efficient way to change this setting.
- KMS Administrators (KMSA). To be able to perform most administrative tasks associated with the KMS, one must be designated a Key Management Server Administrator. Note that this application will not accept global or local groups – the KMSAs must be added individually. Given the critical nature of the KMS, this right should be granted judiciously.

- KMS password. It is very critical to change the password used to control access to KMS administration functions, as the default is simply "password." Once again, it is recommended that you follow the guidelines published in the "*Guide to Implementing Windows NT in a Secure Environment*" when selecting the password.
- Each mailbox must be enabled for advanced security. This can be done mailbox by mailbox, or it can be done for all mailboxes at once. To enable many mailboxes at once, run the DOS program SIMPORT.EXE which is installed in the "bin" subdirectory of your KMS directory. It will ask a series of questions and then enable advanced security on all the accounts. The path:

  \EXCHSRVR\BIN

  must be included so the program can have access to a file called

  SECADMIN.DLL

  You can add this directory to your path definition via the control panel, system icon, environment tab.

Finally, it is important to remember that the KM server database contains the private encryption keys for every user in your entire organization. It is recommended that you back up all KM server data files in the Kmsdata subdirectory (for example, Exchsrvr\kmsdata*.*) separately from other data and that you make sure these backup tapes are stored in a more secure manner than your everyday backups. All keys in these files are 128-bit RC2 encrypted, so this database is protected.

The problem with tape cartridges is that they are maintained offline. If someone were to steal one, that person could restore the files to his or her own server, and then try to crack the key used for the database, with no fear of being detected. (Source: Exchange Server 5.5 Resource Guide)

Advanced Security Summary – Exchange Server 5.0

In summary, to enable advanced security:

- It is recommended that the Key Management Server be installed in the same directory as the Exchange Server (typically exchsrvr) so that the KMS directory will inherit the appropriate permissions. If the KMS is installed to another directory, use of the permissions defined in Chapter 1 is recommended.

- If during the installation the choice is selected to use of a floppy disk to store the Key Manager, it is necessary that the Key Manager service have access to the floppy. KMS access to the floppy can be enabled via the C2 Configuration Manager. From the C2 Configuration Manager, select the "Removable Media Drives" security feature and disable "Allocate Floppy Drives at logon."

- It is recommended that either DES or 64-bit CAST for the encryption algorithm be selected. To do so, select the **Encryption** object under the site container and select **File/Properties** and the "Security" tab.

- Define KMS administrators, being careful to restrict this right to a select few. To define KMS administrators, select the **Encryption** object under the site container and then select **File/Properties** and the "Security" tab. Click "Key Management Server Administrators…."

- Change the default KMS password to one that meets the password recommendations contained in the "*Guide to Secure Microsoft Windows NT Networks*." To do so, select the **Encryption** object under the site container and then select **File/Properties** and the "Security" tab. Click "Key Management Server Administrators…."

- Enable mailboxes for advanced security. To do so for multiple mailboxes, SIMPORT.EXE can be used as described above. To enable mailboxes individually, select the **mailbox** under the recipients container and then select **File/Properties** and the "Security" tab. Click on "Enable Advanced Security" and follow the on-screen directions. When using Outlook 97 or the Exchange client, the recommended location of the file containing the user credentials on the client machine is "%Systemroot%\Profiles\<username>\Personal". The suggested name is "<mailbox name>.epf".

- It is recommended that you back up all KM server data files in the Kmsdata subdirectory (for example, Exchsrvr\kmsdata*.*) separately from other data and that you make sure these backup tapes are stored in a more secure manner than your everyday backups.

"Advanced Security" – Exchange Server 5.5 with Service Pack 1 (SP1) or Later

As was the case with Exchange Server 5.0, advanced security under Exchange Server 5.5 SP1 (or later) consists of a public key based technology that provides for message encryption and decryption, authentication, and message integrity. A Key Management Server (KMS), which is an optional installation available on the Exchange Server CD, works in conjunction with the Microsoft Certificate Server to create and distribute keys, allocate and revoke security certificates as required, place public credentials in the Directory Store, replace user keys that have been corrupted, and perform other management functions in relation to the public key features. While the KMS is a critical component of the advanced security features in Exchange, the security workload is actually split between the client and server. The client performs the actual encryption and decryption of messages as well as the application and verification of digital signatures. The client also stores the user's private key in an encrypted manner. The Exchange client and Outlook 97 store the information in a file (*.epf) while Outlook 98 uses the registry. Outlook 98 offers a choice of three levels of security protection for private keys stored on the client computer:

- High: When this option is chosen, the user will be prompted for a password each time his or her security keys are accessed.
- Medium: The user will be prompted each time an application requests access to the key. An option is presented to abort or continue, but no password is required.
- Low: No notification is given and no password is required.

When advanced security is invoked, several administrator-selected options are available for the encryption/decryption algorithm:

- DES. The Digital Encryption Standard is an algorithm validated by the National Institute of Standards and Technology (NIST). This is available only in the North American version of Exchange and it uses a 56-bit key.
- 3DES. This version of DES utilizes three 56-bit keys in the encryption process, which effectively increases its key length by a factor of three.
- CAST. CAST is named after Carlisle Adams and Stafford Tavares of Northern Telecom Research. A 64-bit version is available in the North American release of Exchange; a 40-bit version is used in the international release.
- RC2-128 bit. This is a block cipher developed by RSA Inc. As suggested by the name, it uses a 128-bit key. It is available in the North American version of Exchange.
- RC2-64 bit. RC2 with a 64 bit key. It is available in the North American version of Exchange.
- RC2-40 bit. RC2 with a 40 bit key. It is available in both the North American and international version of Exchange.

Certain algorithms are not available for international use due to restrictions the US has imposed on exporting encryption algorithms. These rules are somewhat complex, but in general exports are restricted to algorithms using shorter key lengths. In the event that a North American user who is enabled with an algorithm that uses a North American key length sends a message to someone who is only enabled with the international version, Exchange automatically downgrades to the shorter key length for that message.

Message Digest 5 (MD5) or Secure Hashing Algorithm 1 (SHA-1) are used for the digital signatures that provide the authentication and data integrity features. MD5 results in a 128-bit hash, and SHA-1 results in a 160-bit. Since the US has no export restrictions on algorithms used for these security features, the same version is used in the North American and international releases.

Exchange Server 5.5 SP1 (or later) uses these algorithms is support of the Secure Multi-Purpose Internet Mail Extension (S/MIME). S/MIME is an extension to the Simple Mail Transport Protocol (SMTP) that is used for e-mail on the Internet. It provides data confidentiality, data integrity, and authentication services for Internet e-mail. The S/MIME standard specifies the used of X.509 v3 certificates issued by Certification Authorities (CA) for certification of the validity of user's public values. Exchange Server 5.5 SP1 (or later) also offers an option to issue X.509 version 1 certificate for backward compatibility with Outlook 97 and the Exchange client.

The use of advanced security has several advantages over the use of RPC encryption. When using advanced security, an encrypted message remains encrypted until decrypted by the recipient; messages encrypted using RPC encryption are only encrypted in transit from the client to server and stored in unencrypted form once they reach the server. Also, advanced security supports authentication and message integrity -- features not available when using RPC encryption. For these reasons, the use of the advance security features is recommended.

In addition to algorithm selection, the installation and use of the Key Management Server requires the Exchange administrator to make several decisions and perform several actions that are security critical:

- Installation. It is recommended that the Key Management Server be installed in the same directory as the Exchange Server (typically "exchsrvr") so that the KMS directory will inherit the appropriate permissions. If you choose to install the KMS to another location, the recommended directory and file permissions are those outlined for the Exchange server directory in Chapter 1.
- Access. During the installation of the Key Management Server, the administrator decides whether or not to use a manual password versus a disk password. Each has its advantages and problems. For the manual password, memorizing the long password may be difficult and writing it down is potentially non-secure. When saving the password to disk, the password is not encrypted on the disk and is readable to anyone who obtains the disk -- the disk must be kept in a secure place. The use of a floppy disk to store the Key Manager password requires that the Key Manager service have access to the floppy. Per the "*Guide to Secure Microsoft Windows NT Networks*", the floppy disk is allocated at logon and is no longer available to the Key Manager service. In order for the Key Manager service to access the floppy, it is necessary to change this setting. The C2 Configuration Manager tool provides a very efficient way to change this setting.
- KMS Administrators (KMSA). To be able to perform most administrative tasks associated with the KMS, one must be designated a Key Management Server Administrator. Note that this application will not accept global or local groups - the KMSAs must be added individually. Given the critical nature of the KMS, this right should be granted judiciously. Unlike Exchange Server 5.0, Exchange Server 5.5 SP1 (or later) offers the ability to require multiple KMSAs to concur prior to conducting certain key management related tasks. Specifically:
    - Add administrators, delete administrators, or edit these multiple password policies. The number of passwords required for this task must be equal to or greater than the number selected for the remaining tasks in order for the use of multiple passwords to be effective.
    - Recover a user's security key.
    - Revoke a user's security key.
    - Import or untrust another Certification Authority's certificate. This allows management of cross certifications between certificate authorities (readers who require a refreshed on key management fundamentals, include cross certification, are referred to Module 10 "*Advanced Security*" of the Course of Instruction that accompanies this document.)
    - Change enrollment settings (between V1 and V3 certificates). X.509 version 1 certificates are available when backward compatibility is required with Outlook 97 or the Exchange client. If only Outlook 98 is used, version 3 certificates can be issued. One can also choose to issue both in homogenous networks.
- KMS password. It is very critical to change the password used to control access to KMS administration functions, as the default is simply "password." Once again, it is

recommended that you follow the guidelines published in the "*Guide to Implementing Windows NT in a Secure Environment*" when selecting the password.

- Each mailbox must be enabled for advanced security. This can be done mailbox by mailbox, or it can be done for all mailboxes at once. Unlike Exchange Server 5.0, multiple users can be enrolled in advanced security via the Exchange Administrator tool. Exchange Server 5.5 SP1 (or later) also offers the ability to email the temporary key (also called a token) that is used to transfer critical user key values. It is recommended not to mail a user's temporary key as, by default, client/server communications are not encrypted. Furthermore, even if RPC encryption has been enabled as discussed in the module entitled "Client Security", this is an option the user could have disabled.

Finally, it is important to remember that the KM server database contains the private encryption keys for every user in your entire organization. It is recommended that you back up all KM server data files in the Kmsdata subdirectory (for example, Exchsrvr\kmsdata*.*) separately from other data and that you make sure these backup tapes are stored in a more secure manner than your everyday backups. All keys in these files are 128-bit RC2 encrypted, so this database is protected.

The problem with tape cartridges is that they are maintained offline. If someone were to steal one, that person could restore the files to his or her own server, and then try to crack the key used for the database, with no fear of being detected. (Source: Exchange Server 5.5 Resource Guide)

Advanced Security Summary – Exchange Server 5.5

In summary, to enable advanced security:

- It is recommended that the Key Management Server be installed in the same directory as the Exchange Server (typically exchsrvr) so that the KMS directory will inherit the appropriate permissions. If the KMS is installed to another directory, use of the permissions defined in Chapter 1 is recommended.

- If during the installation the choice is selected to use of a floppy disk to store the Key Manager, it is necessary that the Key Manager service have access to the floppy. KMS access to the floppy can be enabled via the C2 Configuration Manager. From the C2 Configuration Manager, select the "Removable Media Drives" security feature and disable "Allocate Floppy Drives at logon."

- It is recommended to select an encryption algorithm with the longest available key length. To do so, select the **Site Encryption Configuration** object under the site container and select **File/Properties** and the "Algorithms" tab.

- Define KMS administrators, being careful to restrict this right to a select few. To define KMS administrators, select the **CA** object under the site container and then select **File/Properties** and the "Administrators" tab. Click "Add Administrators"

- Change the default KMS password for each KMSA to one that meets the password recommendations contained in the "*Guide to Secure Microsoft Windows NT*

Networks." Each KMSA needs to perform this task. To do so, select the **CA** object under the site container and then select **File/Properties** and the "Administrators" tab. Click "Change my KM Server Password".

- Consider requiring multiple KMSAs concurrence for certain KM related activities. No specific recommendations are offered, as they would vary depending the sensitive of the data being protected. To manage this feature, select the **CA** object under the site container and then select **File/Properties** and the "Passwords" tab.

- Enable mailboxes for advanced security. To do so for multiple mailboxes, go to the "Enrollment" tab of the **CA** properties dialog box. To enable mailboxes individually, select the **mailbox** under the recipients container and then select **File/Properties** and the "Security" tab. Click on "Enable Advanced Security" and follow the on-screen directions. It is not recommended to mail the user's token.

- It is recommended that you back up all KM server data files in the Kmsdata subdirectory (for example, Exchsrvr\kmsdata*.*) separately from other data and that you make sure these backup tapes are stored in a more secure manner than your everyday backups.

☑ Exchange Client ☑ Outlook 97 □ Outlook 98

- The recommended location of the file containing the user credentials on the client machine is "%Systemroot%\Profiles\<username>\Personal". The suggested name is "<mailbox name>.epf".

□ Exchange Client □ Outlook 97 ☑ Outlook 98

- Select medium or high level of password protection for user keys stored in the registry.

Defining Access Rights from the Client

While there are no specific recommended security settings, it is important to understand the power that users have to delegate access to their mailbox and to public folders which they create. These access rights are implemented by users at the client – neither access to the Exchange Administrator tool or membership in an Exchange Administrator Group is required.

Via the client software package, users can grant others a wide range of access rights to their mailbox that range from simple "reviewer" rights (read only) to "owner" rights, which includes all the rights that can be associated with a mailbox. Obviously, this could cause security concerns.

Also via the client, the user can set permission on folders he/she created. The access rights that are associated with public folders also range from the relatively benign

“contributor” right (allowing one only to post) to “owner” which allows the full range of rights, including the ability to post custom forms to the folder. Issues associated with posting forms to folders are detailed in Chapter 10.

Chapter

8

WEB Access

Exchange provides the capability for users to access their mailboxes and public folders via a web browser using the web-standard Hypertext Transfer Protocol (HTTP). Web access to Exchange is provided through an Information Internet Server (IIS) Active Server Page. Exchange Server 5.0 is only supported with IIS 3.0, Exchange Server 5.5 is supported with IIS 3.0 or IIS 4.0. "Outlook Web Access" is the term Microsoft uses for the component that provides this connectivity.

There are a few security-related considerations associated with allowing HTTP access to an Exchange server. First, a hot fix is necessary for those installations that are using IIS 3.0. Second, in order for web access to function, it is necessary to make a few modifications to the default configuration invoked by the "*Guide to Secure Microsoft Windows NT Networks*." Third, selection of the proper mechanism for authenticating access via the web is necessary. The final security issue relates to anonymous (unauthenticated) access that Exchange supports for access to public folders and the global address book. Obviously, if one is to allow anonymous access, care should be taken to restrict anonymous users to only that data they are authorized to see.

Hot Fixes

- If you are using IIS 3.0, a hot fix is required to address a memory leak issue. Details are available in Microsoft knowledge base article Q179258.

Changes to the Default OS Settings

- On the Exchange Server, give Authenticated Users Modify access to all files and sub-directories to the directory or directories where the Exchange Server was installed.
- On client machines, give Authenticated Users Modify access to %SystemRoot%\System32\Mapisrv.inf
- Make certain that Authenticated Users have the right to *Log on Locally* to the Exchange Server computer.

☑ Exchange 5.0 ☐ Exchange 5.5

- Using the registry editor, go to the following Key:

  HKEY_Local _Machine/Software/Microsoft/Windows Messaging Subsystem

  On the Edit Menu, click Add Value and enter the following:

  Value Name - ProfileDirectory

  Data Type - REG_SZ

  For the String enter “C:\TEMP”

This change is not required if using Exchange server 5.5.

☑ IE 3.0 ☐ IE 4.0

- If using Internet Explorer, version 3.0 give Authenticated Users Modify access on the following on the client computer:
  - %SystemRoot%\Cookies
  - %SystemRoot%\History
  - %SystemRoot%\Temporary Internet Files

This change is not required if using Internet Explorer 4.0.

Authentication

Installation of Outlook Web Access automatically installs the Active Server Pages and creates the appropriate virtual directory within IIS to access it. Configuration of IIS is well beyond the scope of this document; however, it is important to note that authentication mechanisms for web access are controlled by IIS, not the Exchange Administrator tool. There are three options:

- Allow Anonymous Access. This allows users to access public folders and the global access list via the web without authentication.
- Basic Authentication. This option will result in the user being prompted for a user name and password as a means of authentication. It is not secure because the password is sent in the clear; however, combining this option with Secure Sockets Layer (SSL) encryption would provide protection.
- Windows NT Challenge/Response. This is the native Windows NT authentication mechanism. Like SSL encrypted basic authentication, this option provides a

protected means of authentication. Only the Internet Explorer browser supports this option.

If IIS and Exchange Server are on the same computer, then you can use any of the above authentication methods. If IIS and Exchange Server are on separate computers, you will not be able to use NTLM authentication; however, using SSL will ensure that all information passing between the client and the IIS computer is encrypted.

- Select the appropriate authentication mechanism for the environment. Remember that anonymous access provides no authentication, basic authentication results in passwords being sent in the clear unless combined with SSL, and Windows NT Challenge/Response only works with Internet Explorer. Windows NT Challenge/Response or Basic Authentication combined with SSL encryption are the recommended authentication mechanisms.

Anonymous Access

HTTP access can be controlled for all servers in a site at the site level in the Exchange Administrator tool or can be controlled individually on a mailbox-by-mailbox basis. To control HTTP access at the site level, go to the **Protocols** container under the site Configuration container. Select **HTTP (Web) Site Settings** and **File/Properties** and the "**General**" tab.

- To allow anonymous access to public folders, enable "Allow anonymous users to access the anonymous public folders."

- To allow anonymous access to the global address list, enable "Allow anonymous users to browse the global address list."

If anonymous access is allowed, Exchange Administrators can also control which public folders are enabled for anonymous access. To do so:

- Select the **HTTP (Web) Site Settings** object as described above. Select the "Folder Shortcuts" tabs. Use the "new" and "properties" buttons to enable or disable public folders for anonymous access. Note: Remember that users can manipulate the access controls on folders they own from the client. Once again, it is important to consider who should be allowed to create public folders, as detailed in Chapter 4.

- To control access via HTTP on a mailbox-by-mailbox basis, select the **Recipients** container and then the mailbox. Select **File/Properties** and the "Protocols" tab. Highlight **HTTP (Web)** and click on "settings" to enable or disable HTTP for the mailbox. Note that disabling HTTP access to a mailbox does not restrict that user from accessing public folders that allow anonymous access.

Data Confidentiality

It is important to remember that the Advanced Security features discussed in Chapter 7 will not function when accessing messages via HTTP. A user cannot decrypt messages in his/her inbox and cannot encrypt or sign messages being sent to others.

Secure Sockets Layer encryption can be used to provide protection for the messages in transit. SSL is setup via Internet Information Server settings which are covered our *"Guide to the Secure Configuration and Administration of Microsoft Internet Information Server 4.0*".

Chapter

9

POP3/IMAP4/LDAP/NNTP

This chapter presents the security considerations associated with access to an Exchange Server via the Post Office Protocol version 3 (POP3), Internet Message Access Protocol (IMAP), Lightweight Directory Access Protocol (LDAP), and the Network News Transport Protocol (NNTP). The security concerns associated with these four protocols are similar, as is the manner in which they are configured.

POP3

POP3 is a mail access protocol typically used to access mail via the Internet. It actually works in conjunction with the Standard Mail Transport Protocol (SMTP) for message transfer. SMTP is used to send messages from a client and POP3 is used to retrieve messages. Exchange Server support the use of POP3, where the primary security concern relates to the manner in which user authentication is performed. There are four options:

- Basic (clear text). When this option is selected, passwords are passed in the clear. The potential security concerns are obvious.
- Basic (clear text) with SSL. This option is identical to the first option with the exception that SSL is used to encrypt the link between the client and the server. SSL encryption is enabled via the key manager that is assessable via the Internet Information Server (IIS) Internet Service Manager.
- Windows NT Challenge/Response. This option uses cryptographic processes to ensure that passwords are not sent in the clear.
- Windows NT Challenge/Response with SSL.

In addition, Exchange Server 5.5 offers authentication via the Microsoft Commercial Internet Server (MCIS) membership system. The MCIS is intended for commercial Internet providers with a huge membership base and will not be covered in detail in this document.

To set the allowed authentication mechanisms for POP3, from the Exchange Administrator:

- Select the **Protocols** container under the site Configuration container. **Select POP3 (Mail) Site Defaults** and **File/Properties** and the “Authentication” tab. Select the

allowed authentication mechanisms appropriate for the Exchange installation remembering the risk associated with Basic (clear text) passwords.

- If using Basic (clear text) passwords, grant the Exchange services account the "bypass traverse checking" right on the computer where the Exchange Server is installed. This is necessary as a consequence of invoking the "*Guide to Secure Microsoft Windows NT Networks*."

When using Outlook 97/98 or the Exchange client for POP access, a change to the file permissions on the client machine invoked by the "*Guide to Secure Microsoft Windows NT Networks*" is necessary.

- Give "Authenticated Users" Modify Access to the %SystemRoot%\SYSTEM32 directory. It is very important NOT to replace permissions on subdirectories or existing files. The client needs this permission to allow it to create a .RHC file within the system32 directory. Note: This change IS NOT necessary if installing Outlook 98 using the Internet Mail Option.

- Give "Authenticated Users" Modify access rights to the file %SystemRoot%\ SYSTEM32\MAPISVC.INF.

IMAP

The Internet Message Access Protocol (IMAP) is a successor to POP3. Just like POP3, it works in conjunction with the Simple Mail Transport Protocol (SMTP). SMTP is used by the client for message uploads, IMAP4 is used for downloads. The primary security consideration is the type of authentication that is required. The options are identical to that presented for POP3 and will not be repeated here.

To set the allowed authentication mechanisms for IMAP, from the Exchange Administrator:

- Select the **Protocols** container under the site Configuration container. Select **IMAP (Mail) Site Defaults** and **File/Properties** and the "Authentication" tab. Select the allowed authentication mechanisms appropriate for the Exchange installation remembering the risk associated with Basic (clear text) passwords.

LDAP

LDAP is used by clients to access Information Stored in the Directory Store (DS) component of Microsoft Exchange. It allows the client to read, sort, and delete objects stored in the DS.

There are two items of interest in relation to LDAP. As with POP3, the authentication mechanism is important, as well as the choice to allow or disallow anonymous access. The concerns with the latter relate to the fact that with anonymous access there is the potential for information stored in the Directory Store to be accessed by anyone.

To set the allowed authentication mechanisms for LDAP, from the Exchange Administrator:

- Select the **Protocols** container under the site Configuration container. **Select LDAP (Directory) Site Defaults** and **File/Properties** and the "Authentication" tab. Select the allowed authentication mechanisms appropriate for the Exchange installation.

NOTE: If one is wishes to utilize Basic (Clear Text) authentication, or Basic (Clear Text) using SSL, the client must specify in the user profile the account name in the following format in order to establish a successful connection:

dc=[domain name], cn=[account name]

or

cn=[account name], cn=[domain name]

To control anonymous access:

- Select the **Protocols** container under the site Configuration container. **Select LDAP (Directory) Site Defaults** and **File/Properties** and the "Anonymous" tab. The decision to enable or disable anonymous access will vary depending on the installation.

NOTE: If users are allowed to access mailboxes or public folders via a web browser, the Lightweight Directory Access Protocol (LDAP) must be enabled for anonymous access or web access will not function.

NNTP

NNTP is used for transferring USENET newsgroups on the Internet. Exchange allows you to receive a newsfeed from the Internet via the use of the NNTP. NNTP is also used for client access to the newsgroups.

The security relevant concerns for NNTP are identical to those of LDAP – authentication mechanisms and anonymous access.

To set the allowed authentication mechanisms for NNTP, from the Exchange Administrator:

- Select the **Protocols** container under the site Configuration container. Select **NNTP (News) Site Defaults** and **File/Properties** and the "Authentication" tab. Select the allowed authentication mechanisms appropriate for the Exchange installation.

To control anonymous access:

- Select the **Protocols** container under the site Configuration container. Select **NNTP (News) Site Defaults** and **File/Properties** and the "Anonymous" tab. The decision to enable or disable anonymous access will vary depending on the installation.

Disabling Unnecessary Service

All of these services should be disabled if they are not in use in the organization. To disable the services:

- Select the **Protocols** container under the site Configuration container. Select the appropriate protocol and **File/Properties** and the "General" tab. Clear the "Enable protocol" option.

Chapter
10

Custom Applications

The Microsoft Exchange environment can be enhanced through the use of custom applications. Custom applications entail the creation of custom forms that are used in place of, or as an augment to, the forms delivered with Exchange. The custom forms can, and many times do, include the addition of Visual Basic code. Visual Basic is a powerful programming language that, in the hands of the malicious, could create security concerns. Visual basic programs have nearly unlimited potential to wreak havoc on a computer and they execute with the full set of access rights enjoyed by the user who initiated the execution of the code.

A variety of tools are available as optional installations with the Exchange Server which are used to design custom applications in Exchange. These include the Exchange Forms designer, Form Template Wizard, and Visual Basic for Exchange Server. Forms can also be designed directly from the Outlook client.

Once designed, a form must be published for access. There are four options. The form can be published locally to a personal forms library, it can be published to a client folders (such as the Outlook inbox, for example), it can be published in a public folder, or it can be published in the Organization Forms library. Forms that are stored locally are typically user-specific customizations that a user has made to forms, such as the e-mail "send" form. Forms stored in a public folder are typically used in a manner that resembles a database entry screen – the completed form is not sent to a user but, instead, posted to the folder. The Organization Forms library is for general-purpose forms that you want to make available to the entire organization. An example of such a form might be a "While You Where Out" form.

File Permission Issues

There is one file permission issue related to the publication of forms to public folders and to the Organization Forms library as a consequence of invoking the *"Guide to Secure Microsoft Windows NT Networks*."

Publishing Forms in Public Folders or the Organization Forms Library

When a user accesses a custom form that was published to a public folder or the Organization Forms library, the client tries to install a copy of the form in the %SystemRoot%\forms directory of the local machine. A user without Windows NT administrative rights does not have the appropriate permissions to do this.

This issue can be overcome simply by modifying the permissions on the forms directory:

- Give “Authenticated Users” Modify rights to the %SystemRoot%\forms directory, applying the change to all subfolders and files.

Protection Against Malicious Visual Basic Code

Both the Outlook 97/98 and Exchange clients provide a level of protection against malicious Visual Basic code. The clients are able to detect the presence of Visual Basic in a form and will give the user the option to disable execution, provided the form was not posted to the Organization Forms library or a public folder. The clients assume these are trusted locations and the Visual Basic check is not implemented in these cases. Obviously, this implies the need to control who can post forms to the Organization Forms library and controlling whom can create public folders, as detailed in Chapter 4. Remember that anyone who creates a folder is given owner rights and the owner of a folder can publish any form to it they wish.

To provide protection against malicious custom applications, the following recommendations are offered:

- Avoid putting clients onto server machines or at least avoid logging in as a Windows NT administrator except when absolutely necessary.

- Only install the Exchange Forms Designer and Visual Basic design tools for users trusted to create applications.

- Restrict who can post forms to the Organization Forms Library. To do so, access the **Organization Forms** object in the Exchange Administrator under “Organization/Folders/System Folders/EFROMS REGISTRY”. Select **File/Properties**, the “General” tab, and click “client permissions.” Owner rights are required to publish to the Organization Forms folder – a right that should be given judiciously.

- Restrict who can create public folders. Remember that anyone who is given the right to create public folders has the owner permissions necessary to post forms to the folder. Administrators can only control who has the right to create folders, as discussed in Chapter 4.

Chapter
11

Final Thoughts

This final chapter of the "*Guide to the Secure Configuration and Administration of Microsoft Exchange*" deals with various miscellaneous topics of interest – changing the Exchange service account password, backup procedures, anti-viral precautions, and network security considerations.

Changing Exchange Services Account Password

It is recommended that the Exchange services account password be selected and managed in accordance with the "Guide to Secure Microsoft Windows NT Networks". This means that the Exchanges services account password will expire every 90 days.

The password must be changed in two locations. First, and most obviously, it must be changed as the operating system level via User Manger. Additionally, the password must be changed at the application level using the Exchange Administrator. Updating the password here will effect a change on all Exchange related services so that they will log in using the new password.

- When changing the Exchange services account password, be sure and change it under the Exchange Administrator as well. To do so, go to the properties page of the **configuration** container and select the "Service Account Password" tab.

Backup Procedures

The disaster recovery section of the "*Guide to Secure Microsoft Windows NT Networks*" discusses general guidelines for backing up Windows NT servers. The same general procedures are applicable when backing up the Exchange server, but there are a few important considerations to keep in mind in relation to Exchange's use of transaction logs.

All message transactions are written first to transaction log files and then to the database files. This is done for performance and to improve recoverability should the database become corrupt. Since log files are written sequentially, Microsoft Exchange clients experience a higher level of performance. Writing data directly to the randomly-accessed database files would entail greater overhead and, therefore, diminished performance.

For recoverability, log files can be used to recover message transaction data in the event of corruption of the Information Store or Directory database files, provided that you have either backed up the logs or the logs are intact. As an added layer of protection, log files are typically kept on a separate physical disk drive from the actual Information Store and Directory database files. If the database files are damaged, a backup of the database files can be restored and any data that has not been backed up but that has been recorded in the transaction logs can be "played back" to complete the restore.[1]

By default, the Exchange Server uses "circular logging" in the creation and storage of transaction logs. Circular database logging is a method that utilizes a fixed number of log files. As new log files are created, they overwrite old log files provided of course those log files have been fully committed (written) to the database file. Four log files are typically used for each of the various databases, but this number will increase if the server load is high. This approach saves disk space by reducing the number of log files but does leave the Exchange server more vulnerable to data loss. If a database is corrupted and some of the transaction logs created since the last backup have been overwritten, it will be impossible to fully recover the data.

When circular logging is disabled, the log files will accumulate until the next backup. An Exchange compliant backup program will then delete all fully committed transaction logs whenever a normal or incremental backup is performed.

To setup the Exchange Server for robust data recovery mechanisms:

- Disable circular logs. This is accomplished at the server level in the Exchange Administrator. Select the appropriate **server** under the server container. Select **File/Properties** and the "Advanced" tab. Disable circular logging by clearing the two check boxes.

- Place transaction logs on a drive separate from the database files. This will protect the transactions logs in the event the drive containing the database files fails. Run the Exchange optimizer program to determine the location of the files and to move them if necessary.

- Use an Exchange-compliant backup program. The Exchange Server installation routine automatically upgrades the NT backup program for Exchange compliance. Backup tools are also available from 3rd party vendors.

Antiviral Program

Viruses are a leading threat to information systems. Several antiviral programs exist that are designed specifically for the Exchange environment and can help counter the threat.

Using a product especially designed for Exchange can have numerous benefits. A well designed antiviral solution will integrate with Exchange so that new messages are automatically scanned. Another important feature is the ability to scan attachments, including compressed files.

[1] Source: MS Exchange Disaster Recovery, Joseph Pagano, Microsoft Consulting Services (MCS), New Jersey. (highly recommended)>

There are numerous public sector sources for information on antiviral products. A suggested starting point is the International Computer Security Association at http://www.ncsa.com. This web page does not, at the time this was written, delve specifically into groupware antiviral products; however, it does contain a lot of generic information about viral solutions and hot links to the major vendors.

- Implement a robust anti-viral program for the Exchange environment.

Distribution List Security

As reported on NTBugtraq mailing list (http://ntbugtrak.ntadvice.com), a possible denial of service attack can be levied against an Exchange server by an attacker who takes advantage of a general distribution list (such as all_employees@vulco.com). This denial of service attack can be launched by individuals internal to the Exchange environment or can be launched by external parties with connectivity to the Exchange Server (via the Simple Mail Transport Protocol, for example.)

In order to invoke this attack the attacker sends an e-mail to a general distribution list with a request for a read receipt. The attacker uses a spoofed returned e-mail address such that the distribution list is used as both the destination address and return address as shown the following illustration:

> From: <all_employees@vulco.com>
> To: <all_employees@vulco.com>
> Subject: Important message!

Since a read receipt has been requested, a message will be send back to the originator (all_employees@vulco.com) each time a user reads the attacker's message. Since the receipt is addressed to the distribution list, the receipt will be sent to all members of that list. This can result in an extraordinary amount of traffic and result in a denial of service. For example, if the all_employees distribution list has 1000 members, 1000 read receipts could be generated, each of which will be sent to all 1000 members of all_employees. This means that one message from an attacker could result in the generation of over 1 million messages!

1 + 1000 + 1000 * 1000 = 1,001,001

(1 original message + sent to 1000 users + 1000 users send a read receipt to 1000 users)

While in all likelihood some of the members would elect not send a receipt (a feature not supported by all clients and optional on others) the attacker could compensate by simply sending out a series of messages and quickly create a plethora of traffic as some subset of users respond.

Fortunately, there are some simple configuration settings which will significantly reduce the threat. First, one should restrict the users that are authorized to send messages to a distribution list. To do so, open the distribution list's property page and select the Delivery Restrictions tab. At a bare minimum, one should add a distribution list into the “Accept Messages From” box of its own property page to restrict its use to its own members. This will preclude individuals without a valid account on the Exchange server

from using the distribution list, thwarting the outsider threat. Ideally, access to the distribution list should be much more restrictive, limited to those who have a clear need to use the list. This will help counter the internal threat as well. This setting is accessed via the property page for the distribution list, “Delivery Restrictions” tab.

Second, clear the “Report to Message Originator” check box under the Distribution List options. This will preclude read receipts messages from being generated for messages sent to the distribution list under some (but not all) circumstances. In tests conducted by the author, this setting had no effect on potential attackers accessing the Exchange server via the Simple Mail Transport Protocol, so it is important to use it in conjunction with the first recommendation. This setting is accessed from the distribution list's property page, “Advanced” tab.

In summary:

- Restrict users that are allowed to send to general distribution lists. This is accomplished by selecting the distribution list and selecting **File/Properties** and the “Delivery Restrictions” tab
  - Minimally: Only allow members of the distribution list
  - Ideally: Only allow those with a legitimate business need
- Clear the Report to Message Originator check box. This setting is accessed by selecting the distribution list and selecting **File/Properties** and the “Advanced” tab

Network Security Considerations

It is important to remember that the overall security of your Exchange server can be enhanced beyond what is possible with operating system and application level security. There are numerous well-known network security techniques that can enhance your overall security posture. The following is just a few of these techniques. They will be mentioned only briefly -- to go into depth on each is well outside of the scope of this document.

Firewalls are used to separate the internal network from external networks. They can be programmed to restrict incoming and outgoing access per rules defined by the administrator. Firewalls can range in capability from simple packet filtering (denying or granting access based on IP address) to more complex arrangements where detailed analysis is performed for each application type. *It is always a good idea to block access to unused ports from the external network.*

Proxy servers are used to access the external network on behalf of the client. Clients talk to the proxy server who talks to external servers on behalf of the client. External hosts are never directly connected to the client.

Dual homed servers are simply computers with multiple network connections - one for the internal network and one for the external providing a level of isolation.

Appendix A: Implementation of the "*Guide to Secure Microsoft Windows NT Networks*" after Installation of Exchange Server

If implementing the OS guide after a client has been installed, it may be necessary to give Authenticated Users Modify rights over *.rhc files in the %SystemRoot%\System32 directory. These files will only be present if the computer is used for client POP3 access, and then only certain circumstances. Look for the files -- if they are there, change the permissions. If they are not there, move on.

If implementing the OS guide on top of an Exchange Server installation be certain to use the exchange.inf file provided with the OS guide. Note that this .inf file is intended for use for Exchange Servers installed on member servers, not domain controllers. After implementing exchange.inf, verify the following:

- Make certain Authenticated Users have the right to log in locally on the Exchange Server computer if Outlook Web Access is used for client access.
- Make certain the Exchange Services Account has the following rights:
    - Act as part of the operating system
    - Log on as a service
    - Restore files and directories
- On the Exchange Server computer, give authenticated users *modify* access rights to the file %SystemRoot%\SYSTEM32\mapisvc.inf

Revisions:

Version 1.1 – Cleaned up two typos. Neither had substantive impact on the content of the document.

Version 2.0 – Expanded discussion to cover Exchange Server 5.5 and Outlook 98.

Version 2.01 – Clarified the functionality of the settings under the Delivery Restrictions tab on the property page for the Internet Mail Service. The restrictions set up here do not apply to individuals accessing the Exchange server via SMTP.

Version 2.1 – Modified the document to reflect version 2.06 of the "*Guide to Secure Microsoft Windows NT Networks*". The primary changes related to new file permissions terminology that is invoked when the Security Configuration Editor included with Windows NT Service Pack 4 is installed. Also, this version reflects a decrease in the number of instances where the file permissions invoked by the OS guide have to be relaxed in order for Exchange to function properly.

Version 2.11 – Removed the "For Official Use Only" marking.

Version 2.2 – Added discussions of new hotfixes in the section Exchange Server Installation.

Version 2.3 – Added discussions of new hotfixes in the section Exchange Server Installation and additional clarifying remarks concerning the use of SSL for web access in Chapter 8.

Version 2.4 – Added a recommendation to install the latest service pack for Exchange Server, Service Pack 3.

Version 2.5 – Added more specific recommendations regarding the control of active content in the section entitled Security Zones.

Version 2.6 – Added a series of recommendations to counter a potential denial of service attack under the section "Distribution List Security"

Version 2.7 – Added numerous recommendations to counter attacks that utilize the Windows Scripting Host.

Version 2.8 – Described Microsoft's e-mail security patch which was released in response to the ILOVEYOU worm and similar threats.

Version 2.9 – Updated the procedures in Appendix A for installing the OS security guide on top of an Exchange Server.

Version 2.92 – Expanded Appendix A and included details on a recent security patch from Microsoft.

Version 2.93 – Added a recommendation to install the first SP4 security patch for Exchange 5.5.

Version 2.94 – Updated recommendations to include one additional security setting available under IE 5.5. This version also deletes references to a more detailed set of PowerPoint slides which contained the same basic material as this document but in more detail. These documents were written for an audience less familiar with Exchange but they are no longer being supported.

Version 2.95 – Updated the warning page.

Version 3.0 –

- Updated several URL references to reflect the new location of items on the Microsoft web site.

- Deleted references to specific patches – the reader is pointed instead to the Microsoft security home page for the very latest patch information.

Version 3.1 –

- Corrected a reference to RC2 being a stream cipher. It is, of course, a block cipher.
- Cleaned up a superfluous reference to changing permissions on a registry key in the *post installation* section.
- Add details regarding how to disable unnecessary Exchange services.