Report # C4-30R-02

Guide to Securing Microsoft Internet Explorer 5.5 Using Group Policy

The Network Applications Team
of the
Systems and Network Attack Center (SNAC)

Author:
Curt Doernberg

Updated: July 2002
Version 1.0

W2Kguides@nsa.gov

This Page Intentionally Left Blank

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- Many of the security related issues associated with Internet Exp lorer are interrelated. The reader is encouraged to gain familiarity with the entire document before implementing the recommendations in this guide.
- 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.
- **This document is current as of the date listed on the cover page. Please keep track of the latest security patches and advisories on the Internet Explorer home page at http://www.microsoft.com/windows/ie/default.asp and the Microsoft security bulletin page at http://www.microsoft.com/technet/security/current.asp**

This Page Intentionally Left Blank

Trademark Information

Acknowledgements

The author would like to acknowledge several others whose Internet Explorer work was built upon in this paper.

The author would like to acknowledge Brett Sovereign, Ken Katano, and others for help in dealing with ActiveX and Scripting issues.

The author would like to acknowledge James Hayes for help with Certificate and Authenticode issues.

The author would like to acknowledge all those who proofread this document.

This Page Intentionally Left Blank

Chapter 1: Introduction

Intended Audience

This paper is written for administrators of Windows 2000 networks as a configuration guide for Internet Explorer 5.5. Internet Explorer 6.0 is covered in Appendix B. This guide provides recommendations and rationale for security-relevant settings. The mechanism used to implement these recommendations is Group Policy. It is assumed that the administrator is familiar with using Group Policy in general, such as how to edit a group policy, how to link a group policy to an object, how to exclude someone from a group policy, and how to ensure that a group policy interfaces correctly with other group policies. It is recommended that the reader first read the *Guide to Securing Microsoft Windows 2000 Group Policy*[1] for additional information on these subjects.

Worksheets are provided in Appendix D summarizing the configuration options. These worksheets should be completed while reading this document to assist in making appropriate decisions for your network. This will help in configuring all systems on the network to the same settings, as well as being a reference for reconfiguration.

All options in this document comply with the DoD mobile code policy. In order to be completely compliant with the DoD mobile code policy, decisions concerning what sites, certificates, and programs to trust must be made in accordance with that policy, as well as with any relevant local implementation guidelines.

About Internet Explorer

For the purposes of this guide, Internet Explorer is considered securely configured when the following four statements are true:

- Requests are not made by Internet Explorer to the Internet except in direct response to a user's action. Internet Explorer only requests what is necessary to satisfy the user's request.
- Information sent to a specific web site using Internet Explorer only exists in the context of that web site, unless the user takes a specific action to allow that information out.
- Internet Explorer provides trusted channels to servers/sites when appropriate, and clearly identifies when such a channel exists and who is on the other end of that channel.
- Any script or program running within Internet Explorer is run within a restricted environment. Programs delivered through trusted channels may be allowed to leave this restricted environment.

Note: An administrator is constantly balancing protecting the information on the network and allowing users to do their jobs. For this reason, the definition of *securely configured* does not mean that Internet Explorer cannot do anything harmful or inappropriate. The above definition focuses on Internet Explorer not doing anything potentially dangerous without user action and intent. This places a large portion of the network security in the hands of the users. As is noted in other sections of this guide, user education is a very important part of network security. The following two examples illustrate this point.

Example 1: A user wonders if there is a public web page listing the classified top speed of a particular plane. The user then searches for the plane's name and classified speed. The user has just exposed their query to the search engine, which may log or publish this query.

Example 2: A con artist provides a secure form at a bogus corporate web site in which to enter a credit card number. The user obliges by filling out the form, including their credit card number. The con artist has just gotten the credit card number through no fault of Internet Explorer.

[1] This document is part of the NSA Security Recommendation Guides, available from www.nsa.gov

Levels of Configuration

There are several configuration levels that can be applied. The first level is those settings included by Microsoft in Group Policy. This only covers those things that Microsoft designed to be configured by the administrator. Settings set in this way are distributed into special policy sections of the registry and are, therefore, unchangeable by the user.

The second level of protection includes settings not included by default in Group Policy. These settings can be configured with the aid of ADM files imported into the Administrative Template sections of Group Policy. The ADM files in Appendix C should work for these settings, although it is strongly recommended that you verify each ADM file's functionality in your environment or design your own ADM files. After importing the ADM templates, most settings should become as easy to administer as those in the first level; a few require registry probing to get the correct value.

The settings in the second level are considered "preferences", not "policy". Normally, those things that are "preferences" are propagated to the user once, and if the user changes them, they remain changed. Since the settings covered here have security implications, it would be preferable if user changes to these settings were not persistent. Group Policy can be altered to propagate "preferences" with each logon. To do this, enable the following policy, and check the option "process even if the Group Policy objects have not changed".

<Specific Group Policy>:Computer Configuration:Administrative Templates:System:Group Policy:
Registry Policy Processing

The third level of protection involves locking down registry settings used in the second level so that users no longer have the ability to change their values. Windows 2000 provides no automated mechanism for doing this; therefore, it must be done manually or via a specialized application. In case this option is desired, the names of relevant registry keys are provided with each setting.

Chapter 2: Linked Decisions

While there are many policies whose choices are mostly independent, there are some policies that only make sense when combined. To deal with these combinations, there are four decision groups explained in the next four pages. It is strongly recommended that you choose a single option for each decision group and apply it throughout the document. Mixing decisions within the same group letter may create problems or flaws.

The decision groups are called A, B, C, and D. Groups A and B cover ActiveX controls, Group C covers Downloading Files, and Group D covers Connection Settings. The recommended options are A2, B1, C1, and D1; however, the specific selections will be dependant on the environment. To implement the chosen options, select all settings in this document that are linked to the selected options. For example, to implement the recommended settings, select all settings in this document that contain the key phrases **Linked to A2**, **Linked to B1**, **Linked to C1**, and **Linked to D1**.

About ActiveX Controls

ActiveX Controls are programs that are run within the web browser with all the privileges of the user. The ActiveX security model is binary – code is either run or not run. This is vastly different from architectures such as Java applets, which have an internal security model to reduce the privileges available to downloaded code.

One security issue for ActiveX that has drawn a lot of attention is the issue of code being marked as safe for scripting. Code that is not marked safe is not appropriate to run in a web browser, and so Internet Explorer can prevent this type of code from running with relative ease. The problem with this mechanism is that marking an ActiveX Control as safe does not require any testing or validation. Microsoft provides a list of recommended things to check for in a control before marking it safe. Since these are only recommendations, and/or because programmers make mistakes, there have been some serious security problems with controls being improperly marked safe and installed as part of Microsoft product distributions.

There are two major risks from ActiveX controls. The first risk is that a maliciously designed control will be installed and run on a protected system. This risk can be reduced by only installing controls from trusted sources that are provided through trusted channels. The second risk is from the misuse of a control that was thought to be safe. This risk increases multiplicatively as both the number of controls on the system and the sites that are allowed to run these controls increase. This risk can be reduced by applying the updates and service packs designed to fix improperly marked controls as they are released.

The risks associated with Active Scripting are similar to those of controls marked safe for scripting; therefore, Active Scripting is also included in this category. Active Scripting is designed to be limited to functions appropriate to a web page. One additional limit is the “same origin” rule, which allows scripts to only access information on the site that provided the script and other pages from that site. There have been some flaws associated with Active Scripting making inappropriate functionality available to a script, for which Microsoft has released patches. More information on this can be found in the Active Scripting section of Appendix A.

Linked Decision Group A: Who Can Run ActiveX Controls and Plug-ins?

Option A1: Only Allow Trusted Sites to Run ActiveX Controls and Plug-ins

Most web pages that use ActiveX controls will degrade gracefully and display the remainder of their content without them. If there is a specific need to view a web page with ActiveX controls or content that requires plug-ins, proper procedure can be followed for the Administrator to add this site to the trusted sites list.

WARNING: Adobe Acrobat is one commonly used plug-in that will not work for sites in the Internet Zone if this option is selected. Users can instead view PDF documents by downloading them, if such an action is permitted in Linked Decision Group C.

Option A2: Allow All Sites to Run ActiveX Controls marked "Safe for Scripting" and Plug-ins (Recommended)

Although there is still a risk that a future control marked safe will prove to be unsafe, controls that are marked safe should add functionality to web pages without being able to do anything harmful to your system. There are numerous public web pages that enhance the user's experience using these controls, and some pages and document types that require this functionality.

Linked Decision Group B: Who Can Install ActiveX Controls?

Internet Explorer pre-installs many ActiveX controls. Many of the web pages that use ActiveX controls use just the controls installed by Internet Explorer. For those that do not, ActiveX includes a feature for installing more controls as needed.

WARNING: Installing an ActiveX control requires writing entries to the registry and files to a system directory. By default, and for good reason, a Windows 2000 user does not have the permissions needed to do this[2]. Therefore, consider preloading any additional ActiveX controls that may be used.

If there is a need for this functionality, the minimal permissions required are provided here. The following three items need to have full control given to an Administrative Group and Creator Owner, and the designated users for this functionality should have permissions set as follows:

Object Type	Object Name	Permissions
Registry Key	HKLM\Software\Microsoft\Code Store Database	RWX
Registry Key	HKCR	RX + Create Subkey
Folder	WINNT\Downloaded Program Files	All Except Full Control and Delete

Option B1: Do Not Allow ActiveX Control Installation (Recommended)

This option limits the available ActiveX controls to those pre-installed with Windows and by other application distributions. This does not prevent custom ActiveX development; it just requires that these controls be delivered through a mechanism other than Internet Explorer.

Option B2: Allow Trusted Sites to Install ActiveX Controls

This option allows Internet Explorer to install ActiveX Controls from servers in the Trusted Sites zone. Be aware that these controls will be available to anyone allowed to run ActiveX controls (Linked Decision Group A).

Option B3: Allow ActiveX Controls to be Installed from Approved Cache

A mechanism for fine-grained control of approved ActiveX Controls can be based on maintaining a store of additional controls that the user may download. Controls placed into the store are those trusted as benign. Information about how this store could be implemented is discussed under the Controlling Sources of ActiveX Downloads section.

Option B4: Allow ActiveX Controls based on Authenticode Certificate

Internet Explorer has a concept called Trusted Publishers. By placing approved certificates on this list, any controls signed by these certificates can be installed automatically. This feature has a significant shortcoming in that it also allows the installation of untrusted controls with user approval. Such a control would then pose a risk to all users of the system. For this reason, this method is not recommended, and there is no implementation guidance provided.

[2] See Microsoft Knowledgebase article Q240897 for more information.

Linked Decision Group C: What files can users download?

Internet Explorer automatically displays content such as HTML pages, images, and text files, as well as those files for which it has plug-ins. Internet Explorer does not automatically display other file types; instead it provides an interface to download and view/execute/edit them using what Windows considers the appropriate application. These other files could be documents infected with macro viruses, Trojan horse programs, or the mission critical information needed to perform an assigned task. Three options for controlling file downloads are offered:

Option C1: Do not allow file download, only allow viewing by plug-in (Recommended)

This option will only allow those files associated with a pre-established plug-in to be viewed. Adobe Acrobat Reader comes with a plug-in of this type allowing users to view PDF documents under this option. Microsoft Office does not, preventing users from viewing Microsoft Office documents through Internet Explorer when this option is chosen. (As a rule of thumb, things that are considered plug-ins use this term in describing themselves; Microsoft Office instead connects to Internet Explorer after the file has been downloaded.) All files of types that do not have an associated plug-in will be denied to the user. This option is more likely to err on the side of being too restrictive.

Option C2: Allow opening files but disallow saving them

This option will allow all files to be opened in place. This will allow some file types to be viewed using their plug-ins, some file types such as Microsoft Office documents to be opened within the web browser, and even allows applications to be run in place (although there is an Authenticode warning that pops up for an unsigned or untrusted application – see Check for Signatures on Downloaded Programs in Appendix B). The only thing disallowed is saving files directly to disk. The advantage of this option is that Internet files are only accessible while the user has just downloaded them; therefore it would be more difficult for an unwitting user to further disseminate them. This option is more likely to err on the side of being too lenient, potentially opening up security risks with only a small chance of preventing users from accessing files that they might legitimately need.

Option C3: Allow all file downloads

This option will allow all files to be opened in place or downloaded, as the user desires. This option obviously requires the most trust in the users, and does nothing to prevent the user from doing something risky.

There are five additional ways to mitigate these risks. These techniques are briefly mentioned here, however, a detailed discussion is outside the scope of this document. First, maintain up-to-date virus scanning software that scans downloading files. Second, keep up-to-date on all service packs and security patches for applications that might view documents downloaded from the Internet. Third, consider blocking potentially harmful file types at the firewall. Fourth, consider installing viewers that cannot process macros for document types that might include macros. Finally, users should be aware of the risks associated with downloading various types of files, and the measures they can take to manage the risks associated with these files.

Linked Decision Group D: Are network connection settings a security concern?

Internet Explorer is closely tied to Windows 2000 network settings. As a result, there are some options inside Internet Explorer that are closer to operating system settings than application settings. These include the choice of proxy server, dial-up settings, and other network settings.

Option D1: Network Settings should be set now (Recommended)

Choose this option if you would like to use the mechanisms provided by Internet Explorer to set these types of settings as appropriate to your network and to prevent users from changing them.

WARNING: Large organizations typically have a variety of network settings that apply to various parts of their network, particularly in relation to proxy server settings. If this is the case, it will not be possible to implement these settings from a single group policy; group policies for multiple organizational units might be required for these situations. Be aware that comprehensive knowledge of how Connection Settings apply throughout your network, as well as how to use Group Policy, are required for an implementation of this option across multiple organizational units. If this is not appropriate or practical, selection of Option D2 is instead recommended.

Option D2: Network Settings should be hidden but not set

Choose this option if you would like a policy that hides interfaces to network settings from the user but does not do anything to change the current network settings. One would use this option when the settings have already been configured and it is desired to prevent further changes on the part of the user.

Option D3: Network Settings should be changeable by the user

Choose this option if your users need to be able to change network settings themselves. For example, users that connect laptops at different parts of the network may need to do this.

Chapter 3: Group Policy Settings Provided by Microsoft

The following are the places where Group Policy can be used to configure Internet Explorer security settings. This chapter deals with those settings that are exposed by Microsoft by default. The section entitled "Chapter 4: Group Policy Settings provided by ADM Template" covers recommended additions to the default Group Policy settings. Be aware that for some settings, the local copy of Internet Explorer is used to provide the interfaces to the security settings. For this reason, the same version of Internet Explorer should be installed on the server as the clients.

Many of the settings detailed in this section and the next relate to Internet Explorer's security zones. These zones are described in Appendix A.

The recommendations made here are based upon the assumption that it is desired to give the administrator maximum control over these settings. However, in some environments, it may be necessary to grant more authority to the end user. In this case, these settings should be relaxed accordingly.

Settings in the "Computer" Area

<Specific Group Policy>:Computer Configuration:Administrative Templates:Windows Components:Internet Explorer

Security Zones: Use only machine settings.

This policy should be set at **Disabled**. Setting this at disabled creates settings for each user, and therefore prevents one user from modifying the settings of all users.

Security Zones: Do not allow users to change policies.

This policy should be set at **Enabled**. Setting this at enabled prevents users from changing the preferences for security zones.

Security Zones: Do not allow users to add/delete sites.

This policy should be set at **Enabled**. Setting this at enabled prevents users from adding or removing sites from security zones. This prevents a user from bypassing security restrictions by placing untrusted sites in the trusted zone.

Make proxy settings per-machine (rather than per-user)

This setting is related to Discussion Group D. If opting for D1 or D2, then this setting is superfluous, since the user does not have access to the proxy settings – any setting selected for this option will have no practical effect on the system. Therefore, it is recommended under this scenario to simply leave the setting not configured.

If opting for D3, this policy should be set at **Disabled**. Setting this at disabled creates proxy settings for each user and allows them to change the settings as assumed under D3.

If your environment requires the same user to use a different proxy server when they go to a different machine, this setting can be set at **Enabled**. This is most likely if the same user profiles are shared across multiple enclaves. Per-machine proxy settings are enabled via the following registry keys:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

ProxyEnable = 1 (REG_DWORD)

ProxyServer = xxx.xxx.xxx.xxx:yyyy (REG_SZ where x is the IP address and y is the port number)

Disable Automatic Install of Internet Explorer components

This policy should be set at **Enabled**. Setting this at enabled prevents a user from downloading and installing a plug-in or other component.

Settings in the Windows Settings portion of the "User" Area

Connection Settings

<Specific Group Policy>:User Configuration:Windows Settings:Internet Explorer Maintainance:Connection

These settings control how the computer connects to the network. This includes the proxy server and sites that bypass it, the automatic configuration script, and dial-up settings. This dialog box also allows the administrator to delete any existing connection settings that the user might have. Although these settings are more likely thought of as relating to setting up the network, they do have security implications.

These settings should be set as appropriate to your network. (**Linked to D1**)

These settings should be untouched. (**Linked to D2 or D3**)

Security Zones and Content Ratings

<Specific Group Policy>:User Configuration:Windows Settings:Internet Explorer Maintainance:Security:Security Zones and Content Ratings

This is the place where the most important security settings are found. First, check the box that reads, "Import the current security zones settings". Then, click the Modify Settings button. Finally, set the settings for each specific zone. Appendix A describes these settings and gives their recommended values.

Authenticode Settings

<Specific Group Policy>:User Configuration:Windows Settings:Internet Explorer Maintainance:Security:Authenticode Settings

This section allows you to specify code-signing certificates that are trusted enough to download code without prompting the user. This feature has a significant shortcoming in that it also allows the installation of untrusted controls with user approval. Such a control would then pose a risk to all users of the system. For this reason, relying solely on Authenticode is not recommended.

Settings in the Administrative Template portion of the "User" Area

Internet Control Panel

<Specific Group Policy>:User Configuration:Administrative Templates:Windows Components:Internet Explorer:Internet Control Panel

This controls access to the panes of the Internet Explorer control panel that is accessed via the Tools/Internet Options menu selection.

The policies "Disable the Security Page" and "Disable the Advanced Page" should be set at **Enabled**. This will prevent users from being able to see or modify these pages that contain security settings. Note that this setting will also prevent the user from modifying some settings on the Advanced Page that legitimately should be user preferences, such as the ability to turn off animations and sounds.

The policy "Disable the Connections Page" should be set at **Enabled** (**Linked to D1 or D2**) or **Disabled** (**Linked to D3**).

Offline Pages

<Specific Group Policy>:User Configuration:Administrative Templates:Windows Components:Internet Explorer:Offline Pages

This is where you can prevent Internet Explorer from automatically downloading various items. As a rule of thumb, it is preferred that a computer only connects to the Internet and download pages when there is a user actively making requests. If these features were enabled, Internet Explorer could automatically download pages designated offline, information from channels, subscription content, and schedule groups. To disable these features, set each of the following policies to **Enabled**:

- Disable adding channels
- Disable removing channels
- Disable adding schedules for offline pages
- Disable editing schedules for offline pages
- Disable removing schedules for offline pages
- Disable offline page hit logging
- Disable all schedule offline pages
- Disable channel user interface completely
- Disable downloading of site subscription content
- Disable editing and creating of schedule groups

Browser Menus

<Specific Group Policy>:User Configuration:Administrative Templates:Windows Components:Internet Explorer:Browser Menus

"**Disable Save this program to disk option**" prevents using the Save Target As from a right click menu or as an option for processing a file. It still allows the target of a link to be opened in place. Applications can be opened in place, although applications without Authenticode signatures generate an additional warning prompt.

This option should be set at **Enabled** if you would like to add an extra precaution against downloading malicious files. (**Linked to C1, C2**)

This option should be set at **Disabled** if you trust your users to download files.

(**Linked to C3**)

Administrator Approved Controls

<Specific Group Policy>:User Configuration:Administrative Templates:Windows Components:Internet Explorer:Administrator Approved Controls

This setting only has an effect in zones where the Run ActiveX Controls setting is Administrator Approved. By default, there are roughly 10 groups of ActiveX controls provided by Microsoft that can easily be placed on the approved list. Creating a more diverse selection of Administrator Approved controls requires creating or modifying a custom ADM file to reflect each approved control. This mechanism does provide a finer grain of control than otherwise provided. However, other settings throughout this document are based on the Run ActiveX Controls setting being set at different values; therefore, this feature does not fit into any of the groups outlined above.

Disable Changing Advanced Page Settings

Disable Changing Certificate Settings

Disable Changing Automatic Configuration Settings

<Specific Group Policy>:User Configuration:Administrative Templates:Windows Components:Internet Explorer

All of these policies prevent the user from overriding those settings made by the Administrator. All of these policies should be **Enabled**; however, there are a few items to consider:

- If the "Disable the Advanced page" policy is enabled, this setting is superfluous and does not need to be set, because the "Disable the Advanced page" policy removes the Advanced tab from the interface.

  (located in <Specific Group Policy>:User Configuration:Administrative Templates: Windows Components:Internet Explorer:Internet Control Panel)

- There are settings on the Advanced Page that are not security relevant, and this will prevent users from changing those as well.

Disable Internet Connection Wizard

Disable Changing Connection Settings

Disable Changing Proxy Settings

<Specific Group Policy>:User Configuration:Administrative Templates:Windows Components:Internet Explorer

All of these policies prevent the user from changing those settings that are associated with the connection page and their Internet connection.

These options should be **Enabled** to prevent users from changing these settings (**Linked to D1 and D2**). These options should be **Disabled** if you want to permit the users to change these settings (**Linked to D3**).

WARNING: The first time Internet Explorer is run, it will run the Internet Connection Wizard instead. If your users will receive this group policy before running Internet Explorer, then you must set the “Disable Internet Connection Wizard” setting to **Disabled** in order to run this wizard and thus allow access to Internet Explorer. This setting leaves the Internet Connection Wizard accessible from the start menu. Users that have run Internet Explorer prior to application of this policy will not require this.

Do not allow AutoComplete to save passwords

This option prevents Internet Explorer from remembering passwords entered into forms. To prevent these passwords from being stored on your computers, this policy should be **Enabled**.

Chapter 4: Group Policy Settings provided by ADM Template

Most of these settings can be found in a user's web browser at Tools:Internet Options:Advanced. These settings do not appear in the Group Policy controls. An ADM template must be added to both the machine and user sections of Administrative Templates in order to have access to these settings. One such template is provided in Appendix C.

ADM files are invoked via the Active Directory Users and Computers MMC snap-in. Right click on the organizational unit for which the ADM file is to be applied and select *properties*. Select the group policy object (or create a new one if none exists) and click on *edit*. This will open the Group Policy Editor. Navigate to <Specific Group Policy>:User Configuration:Administrative Templates, right click, and select Add/Remove Templates. Add the .ADM file. Note that the "show policies only" option must be disabled within the Group Policy editor. To do so, right click in the *Policy* pane, click on *View*, and disable the *Show Policies Only* option. Navigate to <Specific Group Policy>:User Configuration:Administrative Templates:Windows Components:Internet Explorer:Advanced Internet Explorer Settings to view the settings configurable via the template. Repeat these steps for the Machine settings instead of User settings.

After doing this, the following settings should become available. As mentioned in Levels of Configuration in Chapter 1, it is necessary to enable the option "process even if the Group Policy objects have not changed".

Registry Settings under HKey Current User

Checking for Certificate Revocation (next two options)

Security services, such as SSL and Authenticode, rely on Internet Explorer's ability to verify the source using certificates. If for some reason a source is compromised, that certificate can be revoked. Since a malicious person is unlikely to stop using the certificate of their own volition, a list of revoked certificates is maintained. Revoking a certificate does not prevent a person from using it; it prevents a browser from accepting it. Notification of revocation is placed at the appropriate CDP (CRL (Certificate Revocation List) Distribution Point). Absence of a CDP for a given CA (certification authority) or lack of access to the CDP will prevent this feature from working.

Check Certificate Revocation: Publisher Certificates

This check should be enabled. Checking for certificate revocation occurs when a publishing certificate is used as part of Internet Explorer's process in granting Java or ActiveX code additional privileges. The effectiveness of this check is based on the existence of a server reachable over the network with up-to-date revocation lists; not all CAs provide such a server. The mechanism included here is the least elegant mechanism used in this document for helping to ensure the trust associated with a piece of mobile code. In cases where no code is granted additional privileges based on a publishing certificate, such as if mobile code is run exclusively from trusted sites, this check is irrelevant.

To implement this policy, set the policy to **Enabled**, and follow the instructions to determine the correct value for the **Software Publishing State** bitfield. A bitfield is a value that specifies one setting in each bit of a number. The possibility exists that other bits of this bitfield will be changed, thus creating side effects. For this reason, it is not recommended that my value (listed below) be used without at least verifying that this value is identical to that found on your network. From an unsecured machine, check the "Check for server certificate revocation" checkbox in the advanced tab, apply the settings, and then read the value from the following registry key:

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\
Software Publishing\State

Alternatively, the Windows Calculator, with Scientific Mode's ability to convert between binary and decimal, can help you accomplish this task. Within the above value, the 10th bit from the right is this setting. This particular bit should be set to 0, and no other bits should be changed from their current state.

{One corresponding value is 141312 (decimal) = 10 0010 1000 0000 0000 (binary)}

Check Certificate Revocation: Server Certificates

This policy should be **Enabled**. Server certificates are an important component of web server encryption and authentication. It is important that before trusting a web site based on its certificate that a check be made to verify that its certificate has not been revoked.

(the registry flag HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\
Internet Settings\CertificateRevocation set at 0x1)

Do not save encrypted pages to disk

This policy should be **Enabled**. This will prevent pages sent over an encrypted channel, such as SSL, from being cached on the hard drive. If they were worth encrypting, then it probably makes sense not to store the plaintext.

Note: This may cause unexpected behavior if a server side scripting page is reloaded instead of read from cache. For example, if part of a server side script generated a connection to a database to be used later, and the user returned to this page, the page would be reloaded and a

second connection would be made to the database. If the page had been cached, returning to the page would instead load the cached page on the local machine, and thus only one connection to the database would exist.

(the registry flag HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ DisableCachingOfSSLPages set at 0x1)

Empty Temporary Internet Files folder when browser is closed

This policy should be **Enabled**. This option determines whether or not web pages and other objects are saved locally. Enabling this option will not allow saving of Internet files by the browser. Instead, files will be deleted and may limit, but not preclude, attacks which rely on pre-placement of content in the cache.

In cases where the users download the same pages every day, and bandwidth a bigger concern than security, it might be necessary to enable persistent caching. To do so, set this setting to disabled. On the other hand, if users have roaming profiles, then there is local network bandwidth consumed by transferring the profile on logon/logoff, so there is also an operational reason to leave this feature enabled.

(the registry flag

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Persistent, set at 0x0)

Use Fortezza

This policy should be **Enabled** if operating in a Fortezza environment. IE 5.5 supports a cryptographic service provider (CSP) plug-in that supports Fortezza.

(the registry flag HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ Fortezza set at 0x1)

Cryptographic Protocols

You should select the approved cryptographic protocols. To do this, set this policy to **Enabled**, and follow these instructions to determine the correct value for the Software Publishing State bitfield.

From a machine that has unrestricted access to Internet Explorer, go to the Advanced Page of Internet Explorer's Internet Options, check or uncheck the Cryptographic Protocols as indicated in Table 1, apply the settings, and then read the value from the following registry key using the decimal value:

(the registry value HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ SecureProtocols)

{The value corresponding to the following recommendations is 160}

Table 1: Cryptographic Protocol Recommendations

Protocol	Recommendation	Comment
PCT 1.0	Disabled	PCT 1.0 is proprietary to Microsoft and has not been properly reviewed by the security community.
SSL 2.0	Disabled	SSL 2.0 was reviewed and found lacking by the security community.
SSL 3.0	Enabled	SSL 3.0 was developed by Netscape Communications Corporation and is the leading secure communications protocol for web content. It is the successor to SSL 2.0 and the predecessor for TLS 1.0.
TLS 1.0	Enabled	TLS 1.0 is based on SSL 3.0 and was developed through the Internet Engineering Task Force (IETF). It is an Internet standard (RFC 2246) and has received extensive review.

Warn About Invalid Certificates

This policy should be **Enabled**. The warning related to certain types of bad certificates will be displayed regardless of this setting, but presenting all relevant warnings to the user is preferred. It is important that the user see these warnings, as they can be indicative of a possible problem with the web server to which the user has connected.

These warnings can occur for three reasons:

- The CA's key is not on your trusted CA list. While it is possible that a trusted CA changed their key or a new trusted CA was created, it is more likely that the server certificate was signed with a fictitious or non-authoritative CA and the site should be avoided. If the site must be visited, then it should be treated as a non-secure connection.
- The certificate is being used before or after its validity date. This *may* be an administrative mistake rather than a security concern, but it could represent an expired certificate that was compromised.
- The certificate does not match the name of the site. A legitimate web site's certificate should always contain the correct name, so this warning could indicate malicious activity.

(the registry flag HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ WarnonBadCertRecving set at 0x1)

Warn if forms submittal is being redirected

This policy should be **Enabled**. Most sites receive form input from the forms that they send the client. There is a concern that a form could send data to a site other than the originating site. This is of particular concern when sending sensitive data. Enabling this causes a warning to appear so that the user can reconsider whether the form data should be sent to a second site.

(the registry flag HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ WarnOnPostRedirect set at 0x1)

Disable Password Caching

This policy should be **Enabled**. Internet Explorer has a feature that allows passwords to be stored locally as a convenience for users who access password-protected web pages. Enabling this policy prevents passwords from being stored on local machines.

(the registry flag HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings\ DisablePasswordCaching set at 0x1)

Registry Settings Under HKLM

Controlling Sources of ActiveX Downloads

This setting should be cleared (**Linked to B1**), left alone (**Linked to B2**), or set to specific locations not including CODEBASE (**Linked to B3**). To configure this setting, the policy must be set to **Enabled**, and the CodeBaseSearchPath value must be set.

When Internet Explorer sees a reference to an ActiveX Control, it first looks locally on the computer. If allowed, it will attempt to download the Control by following the search path in the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Internet Settings\CodeBaseSearchPath

By default, this key contains the following value:

CODEBASE;<http://activex.microsoft.com/objects/ocget.dll>;
<http://codecs.microsoft.com/isapi/ocget.dll>

If this setting includes CODEBASE, and Internet Explorer encounters a web page that is allowed to download and run ActiveX controls, it will attempt to follow the link specified on the web page. This is useful behavior if you trust the web page to provide you with a trustworthy control.

If this setting includes the URL of a .dll or .cab file, and Internet Explorer encounters a web page that is allowed to download and run ActiveX controls, it will follow the link, download the file, and see if it includes the desired control. This is useful because you get to specify where the controls come from.

As effectively using a Code Base Search Path that does not contain CODEBASE (as per option B3) is uncommon, consider this example where it would be useful: Assume that there is a single web application that is in the beta stage and requires dynamic updates of its ActiveX controls, and all other applications only use the ActiveX controls preinstalled on network computers. The application developers could create a CAB file containing all relevant controls (using the CAB SDK) and place this file at a known location. The administrator could then change the Code Base Search Path to replace the default setting (which includes CODEBASE) with this fixed location. This will only allow installation of new controls from this specific CAB file.

As a concept, this can be extended. The Code Base Search Path could contain additional entries specifying the locations of all CAB files whose controls are approved. An additional CAB file could be created on the Intranet to include those controls that have been approved individually. This would allow very strong administrative control of the ActiveX Controls that can be downloaded and installed. Having outlined the possibility, the actual implementation is non-trivial and beyond the scope of this paper.

Appendix A: Security Settings By Zone

Internet Explorer utilizes the concept of security zones to control many of the permissions given to web sites. There are five applicable zones: Internet, Trusted Sites, Restricted Sites, Local Intranet, and My Computer. The placement of sites into the various zones can be controlled and unique security settings defined for each.

It is important to consider which zone web sites will fall into. If a page is not explicitly placed in one of the other zones, it will be in the **Internet Zone**. This includes most pages that users see, and most of these pages are not trusted. Therefore, setting permissions for this zone is the most important.

Sites can be placed in a zone called **Trusted Sites**, although no sites are there by default. This zone is for those few sites that are believed to be trustworthy and should have more privileges than most sites on the Internet. If there is a policy on what sites are considered trustworthy[3], then sites should be added to this zone in compliance with this policy. There is an option called "Require server verification (https:) for all sites within this zone." This option should be enabled, causing Internet Explorer to verify the server certificate before granting extra permissions associated with this zone.

Sites can be placed in a zone called **Restricted Sites**, although no sites are there by default. Sites in this zone are considered extremely threatening, and all features that might pose a risk should be disabled. Recent patches to Outlook force this zone to be used for e-mail, because this reduces the risk from e-mail worms.

The **Local Intranet** zone includes only those sites that are within your organization's network. It can distinguish these using any or none of the following three methods:

- It was configured as part of the Intranet by the administrator.
- It is a site that bypasses the proxy server.
- It is accessed by a UNC, i.e. \\SERVER\DIRECTORY\PAGE.html

It is recommended that you limit the definition of the **Local Intranet Zone** to those methods that only reach sites that are part of the Local Intranet.

The zone called **My Computer** only appears in Group Policy, it does not appear in the Internet Explorer configuration. It is presumed that anything that is already on the computer is safe; therefore, no further security restrictions should be added to this zone.

This document specifies settings for the zones **Internet**, **Trusted Sites**, and **Restricted** zones. If no zone is specifically named, then the recommendation applies to all three zones. It may be appropriate to grant additional permissions and/or weaken the restrictions associated with the **Trusted Sites Zone**, assuming that there are clear needs to do so. However, weakening the restrictions associated with the **Internet Zone** and **Restricted Sites Zone** is not recommended.

Since files on the local computer and intranet are generally considered to have a higher level of trust, it is generally recommended to utilize the default settings for the zones **Local Intranet** and **My Computer**. If it is desired to modify these settings in deference to local policy, please be aware that there are relationships between the Internet Explorer settings and user operations conducted via Windows Explorer. For example, prohibiting *Drag and Drop or Copy and Paste Files* for the Local Intranet zone might preclude copying a file from a network share.

[3] For the DoD, using an SSL certificate issued by the DoD PKI is one method of demonstrating trustworthiness.

ActiveX Controls

There are five options for enabling and disabling various classes of ActiveX controls.

Download Signed ActiveX Controls

In the **Restricted Zone**, this should always be set at **Disable**.

In the **Internet Zone**, the security setting should be set at **Disable** (**Linked to B1 or B2**) or **Enable** (**Linked to B3**).

In the **Trusted Sites** zone, this security setting should be set at **Disable** (**Linked to B1**) or **Enable** (**Linked to B2 or B3**).

This setting relates to a commercial PKI (Public Key Infrastructure) service called Authenticode that can be used to sign ActiveX controls with their creating organization's key. What this guarantees is that this organization's key was used to sign the program and the program has not been changed since it was signed. An Authenticode signature does not guarantee that the program is not malicious in some way, it does not guarantee against misuse of the organization's key, and it does not guarantee that the program will work correctly. In addition, while Internet Explorer warns the user about failed certificate verification, a user may ignore the warnings to "make it work" . For this reason, there is currently no recommended method for users to install ActiveX code based solely on an Authenticode signature. However, an Authenticode signature combined with a site meeting the criteria for trusted sites is considered sufficient.

Download Unsigned ActiveX Controls

This security setting should be set at **Disable**.

This security setting allows Internet Explorer to download ActiveX controls that have no Authenticode signature. If the control's author is either unable or unwilling to put their organization's seal of approval on their program, then the security risk presented by running it is unacceptable.

Initialize and Script ActiveX Controls Not Marked as Safe

This security setting should be set at **Disable**.

Many Microsoft products include some ActiveX Controls in a default installation. Some of these perform actions that their creators considered unsafe when used by untrusted code, such as working with your file system. If the creator of the control saw an unsafe action that could occur within this control, then you should take their word for it and not allow pages and scripts running in Internet Explorer to use it.

Run ActiveX Controls and Plug-ins

In the **Restricted Zone**, this setting should be set at **Disable**.

In the **Internet Zone**, this security setting should be set at **Disable** (**Linked to A1**) or **Enable** (**Linked to A2**).

In the **Trusted Sites Zone**, this security setting should be set at **Enable**.

This setting allows a page to invoke and run any ActiveX controls or Plug-ins that are currently installed on the computer. Precautions recommended elsewhere in this document limit ways that controls install on the computer, as well as prevent unsafe controls from running.

Script ActiveX Controls Marked Safe for Scripting

In the **Restricted Zone**, this setting should be set at **Disable**.

In the **Internet Zone**, this security setting should be set at **Disable (Linked to A1)** or **Enable (Linked to A2)**.

In the **Trusted Sites Zone**, this security setting should be set at **Enable**.

This setting allows Active Scripting languages to interact directly with ActiveX controls that have been marked “Safe for Scripting”. This title simply means that the control does not contain any methods that could compromise system security, such as the ability to read critical information from the system directories, overwrite files, etc. As was the case with Authenticode, the user is trusting that the author of the control properly verified that the control is indeed safe. Once again, this feature is best used in conjunction with a trusted site.

Cookies

Cookies, when used correctly, are more of a threat to anonymity than security. HTTP is by nature a stateless protocol meaning that information is not persistent as a user navigates between pages. Cookies are used to keep record of state information and pass it back to the web server as needed. This information can be used in positive ways, such as keeping track of user entries as they navigate through a multi-page wizard or providing customers with personalized pages tailored to their browsing habits.

There are three ways that cookies can be used that cause security and anonymity concerns. The first is using a cookie as the sole authentication mechanism. On some web sites, there exists an option to have a computer remember your password. When this option is chosen, the web site then accepts your stored cookie rather than actually authenticating you every time. This allows anyone with the cookie to authenticate, even if they could not do so otherwise.

The second is a web site actually storing a password or personal information inside a cookie. There have been a large number of cookie-stealing vulnerabilities discovered in a variety of web browsers. Given this track history, one should not assume cookies are secure, and so should not have sensitive information contained in them. Storing sensitive information in cookies goes against best practices, but it still could happen on some web sites.

The third is cookies that have a larger scope than a single web site. A cookie sometimes is created to keep track of what banner ads have been displayed. However, this cookie could allow an organization that places or displays ads across multiple web sites to track user's movements across all of these sites. This poses a much larger threat to anonymity.

Although a detailed discussion is outside of the scope of this paper, it is also important to briefly mention that there are other ways which anonymity can be compromised on the web. A web server can (and often does) log all requests made of it, without the use of cookies. The web server typically receives from your computer and web browser such information as your computer type, your browser type and version, your IP address, and the links you enter from and leave to. This might be a security concern depending on the environment.

Allow Per Session Cookies

In the **Restricted Zone**, this setting should be set at **Disable**.

In the **Internet Zone** and **Trusted Sites Zone**, this security setting should be set at **Enable**.

There are some small security and anonymity risks associated with per session cookies, but they are often required for functionality. This type of cookie allows a web server to preserve state between web pages that are generated for the user. This can occur in such common applications as search engines, multi-page forms, shopping carts, and almost anything that requires login. These cookies are deleted whenever the web browser is closed.

Allow Cookies That Are Stored On Your Computer

In the **Restricted Zone**, this setting should be set at **Disable**.

In the **Internet Zone**, this security setting should be set at **Disable** or **Enable**.

In the **Trusted Sites Zone**, this security setting should be set at **Enable**.

This setting should be set at **Disable** if protecting anonymity of the user or the organization is more important than the added convenience provided by some web sites remembering their name and/or preferences, of if the possible misuses of cookies pose an unacceptable risk.

This setting should be set at **Enable** if users make use of web sites that remember their name and/or preferences, anonymity of users is not a major concern, and users know enough not to use cookies as their authentication for resources critical to the user or the organization.

Prompt is not recommended, because the prompts created will come up too often, and the user's response will most likely not reflect a consistent policy.

Downloads

This category contains two options that are not closely related. The first allows the download of files of virtually all types to be used outside of your web browser; the second allows the download of fonts for use within the web browser.

File Download

For the **Restricted Zone**, this setting should be set at **Disable**.

For the **Internet Zone**, this security setting should be set at **Disable** (**Linked to Group C1**) or **Enable** (**Linked to Group C2 or C3**).

For the **Trusted Sites Zone**, this security setting should be set at **Enable**.

Viewing a document using a plug-in, such as the Acrobat Reader, is not considered a File Download. Saving this document from the plug-in is also not considered a File Download.

If downloading files is allowed, users must be trusted to make valid risk management decisions every time a file is downloaded. For this reason, disabling (unchecking) the option "Always Ask Before Opening This Type Of File" is dangerous, and unchecking it for a risky file type is extremely dangerous.

Font Download

This security setting should be set at **Disable**.

Few sites actively use this feature, and they should degrade gracefully into the default font if this setting is disabled.

Java

Java is very similar in appearance to ActiveX; however, Java has security controls at a finer level of detail than ActiveX's run/do not run model. Java programs can be configured to run in a sandbox where they can only do those things that Internet Explorer considers safe operations.

Signed Java programs can ask in advance for privileges beyond the sandbox. A message appears listing the program's author as well as the privileges required. If the user grants permissions to this program, then the program has the capability to do things considered unsafe.

Java Permissions

In the **Restricted Zone**, this setting should be set at **Disable Java**

In the **Internet Zone**, this setting should be set at **Disable Java** or **High Safety**.

In the **Trusted Sites Zone**, this setting should be set at **High Safety**.

This setting should be at **Disable Java** if users have no need to use Java, if you consider those features that Internet Explorer places in the sandbox to be an unacceptable risk, or if there is a concern about letting inappropriate programs out of the sandbox.

For most installations, it is generally recommended to use the **High Safety** option. This allows users access to most of the Java applets in fairly common usage on the Internet, but will prevent unsigned Java programs from doing things that Internet Explorer considers to be outside of the sandbox. Note that utilization of the setting implies that you trust your users to only let appropriate signed programs out of the sandbox, and that there is a risk of compromise due to errors in the technology that enforces the sandbox.

There is also a setting called *custom*, where the administrator can specify actions that are allowed in the sandbox and actions that are not. Because of the possibility of making a serious mistake in these settings, this is not recommended – simplicity is the friend of security and simply configuring this setting to High Safety or Disable will suffice for the vast majority of users.

Miscellaneous

Access Data Sources Across Domains

This security setting should be set at **Disable**.

This refers to the ability of a web page to use data sources (such as ODBC database connections) installed on the system. If this were allowed, a script could be written that transparently uses the user's data sources. It is undesirable for a web page to be able to transparently access a user's database login, whether the database is on the Intranet or on a web server with a different DNS domain.

Don't Prompt for Client Certificate Selection When No Certificates or Only One Certificate Exists

This security setting should be set at **Disable**.

The double and triple negatives inherent in this policy are confusing. When it is set to Disable, Internet Explorer will always prompt the user before providing a certificate. Authentication is such a fundamental security issue that users should always be aware of how it is performed by the sites they visit.

Drag and Drop or Copy and Paste Files

This security setting should be set at **Disable**.

This setting is more likely to impact Windows Explorer than Internet Explorer. It refers to moving files across the security zones.

Installation of Desktop Items

This security setting should be set at **Disable**.

This setting refers to the creation of an active desktop whereby a web page is loaded upon login and refreshes automatically. Although this does not bypass other security features, it still downloads pages without an action on the part of the user and, therefore, should be disabled.

Launching Applications and Files in IFRAME

This security setting should be at **Disable**.

This setting refers to invisible frames or layers within a web page. It should be disabled because of the risk of confusing a trusted page with an overlay of an untrusted page.

Navigate Sub-Frames Across Different Domains

This security setting should be at **Disable**.

This setting refers to the ability for one document to contain within a frame a document from a different security zone. It should be disabled for the same reason above, the possibility of confusing a trusted page with an untrusted page.

Software Channel Permissions

This security setting should be at **High Safety**.

This setting refers to a rarely used feature called channels. A channel can be used to automatically download or update web pages and software while the user is offline. The high safety setting allows the concept of channels to work, but requires that the user actively authorize downloading the next version from a channel.

Submit Non-Encrypted Form Data

In the **Restricted Zone**, this setting should be at **Disable**.

In the **Internet Zone** and the **Trusted Sites Zone**, this security setting should be at **Prompt**.

Many web sites require the use of Secure Sockets Layer (SSL) encryption for the submittal of form data. This protects the data from being read in transit between the source computer and the destination computer. Some sites do not require the use of encryption, which means that any computer between your computer and the destination computer can read the data. This setting controls what happens in the case when SSL encryption is not required. By selecting prompt, the decision is placed in the hands of the user as to whether the data they placed in the form is something that should be transmitted over a unencrypted link. This helps ensure that sensitive data, such as a Social Security Number or an important password is not sent in the clear.

UserData Persistence

This security setting should be at **Disable**.

The UserData feature is used for storing data between HTTP sessions in ways similar to cookies. Internet Explorer supports it, but other browsers do not. For this reason, few if any web sites actively use this feature. Good security practices dictate the disabling of unnecessary features. Since there are no perceived benefits for allowing this capability, it should be disabled.

Scripting

Scripting relates to the ability of the browser to run small quantities of code that are included in the content of the web page. The languages covered here run within the web browser, and omit features that are considered dangerous, such as accessing the file system and performing raw network access.

Active Scripting

In the **Restricted Zone**, this security setting should be at **Disable**.

In the **Internet Zone,** this setting should be at **Disable** (**Linked to A1**) or **Enable** (**Linked to A2**).

In the **Trusted Sites Zone**, this security setting should be at **Enable**.

Active Scripting covers all forms of scripting that can be included in a <script> tag, such as VBScript or JavaScript. These scripting languages are designed to only refer to data within the web browser and are, therefore, generally considered safe. Both the design and implementation of this security model walks a fine line between adding valuable content and adding security risks, and some flaws have crossed this line. Seemingly insignificant flaws combined with intended features can create dangerous combinations. For this reason, it is important to quickly apply all patches related to Active Scripting. Some examples of bad script behavior follow:

One rule that limits the scope of scripts is the "same origin" rule. The default behavior is that scripts can only communicate within their window and other pages of the same origin (determined by the web server domain name). This has been bypassed by opening a page in a subframe and having scripts access this subframe. This security feature has also been bypassed by injecting code into other web pages. The result of this is the ability to run scripts and access data outside of their original location.

Other features of scripting languages can be misused. The behavior to create a new window is a good example. Used sparingly, it can be useful. However, its use in displaying masses of banner ads is annoying and, carried to an extreme, can result in a denial of service by consuming too many resources.

Allow Paste Operations Via Script

This security setting should be at **Disable**.

This setting controls a script's access to the clipboard. There is very little need for two scripts to use this as a legitimate communication channel. There is also a legitimate concern that some important sensitive data may remain on the clipboard as you travel to an untrusted site and, therefore, this feature should always be disabled.

Scripting Java Applets

In the **Restricted Zone**, this security setting should be at **Disable**.

In the **Internet Zone**, this security setting should be at **Disable** or **Prompt**.

In the **Trusted Sites Zone**, this security setting should be at **Enable**.

If scripts are limited to a safe set of operations, and Java applets are limited to a safe set of operations, then the combination should still be limited to a safe set of operations. Unfortunately, knowing that these two items are safe individually does not *prove* that there are no unsafe ways to use them in combination. Since this is not a commonly used feature, it is generally recommended to disable the feature if practical, or limit it by requiring user confirmation.

User Authentication

Logon

In the **Restricted Zone**, this setting should be set at **Anonymous Logon Only**, to prevent the user from accidentally giving their password to a dangerous site.

In the **Internet Zone** and the **Trusted Sites Zone**, this security setting should be set at **Prompt for Username and Password**.

The overall security setting allows four choices that control what Internet Explorer should do in response to a 401:Unauthorized error.

The one completely unacceptable option for non-Intranet sites is "Automatic Logon with Current Username and Password". If this option is selected, Internet Explorer will attempt to log on to web sites by providing the user's Windows username and password as a first attempt without consulting the user. This could compromise the user's logon credentials.

The **Anonymous Logon Only** setting prevents the user from supplying a username and password.

The **Automatic Logon in Intranet Zone** setting uses your Windows logon within the Intranet Zone, and may be appropriate for that zone.

The **Prompt for Username and Password** setting allows for the possibility of having usernames and passwords differ for different sites within the intranet.

Appendix B: Differences in Configuring Internet Explorer 6.0

Although this guide is intended for Internet Explorer 5.5, there are not many differences between the secure configuration of 5.5 and 6.0. These differences are outlined below.

New Security Zone Options

Meta Refresh

This tag causes Internet Explorer to reload a page after a specified number of seconds have passed. This tag also is used to automatically redirect the user. While automatic redirection is convenient when a web site has moved, web sites that move usually give a clickable link to the new version of the web site. Because of the potential of being automatically redirected from and to malicious sites, this option should be set at **Disable** in the **Restricted Zone** and the **Internet Zone**. This option can be set at **Enable** in the **Trusted Sites Zone**. Note that if Active Scripting is enabled, redirects can occur through that mechanism.

Display Mixed Content

This option gives control over a behavior that used to be preset. When a frameset contains both encrypted pages and unencrypted pages, there is a risk of data leaking from the encrypted page to the unencrypted page. The behavior prior to Internet Explorer 6.0 was to prompt the user. This prompt allows the user to prevent the loading of the unencrypted data. In the **Restricted Zone**, this should be set at **Disable**. In the **Trusted Sites Zone** and the **Internet Zone**, this should be set at **Prompt**. This provides the user a warning that the entire page is not encrypted, as well as allowing them to deny access when appropriate.

New Advanced Page Options

Enable 3rd Party Browser Extensions

A third party extension is a program loaded with Internet Explorer and Windows Explorer in order to add functionality. Added functionality also adds the potential for malicious or unknown behavior. Unless there is a clear need for the functionality provided by such an extension, they should be disabled.

The **Enable 3rd Party Browser Extensions** option should be set at **Disable**.

\HKCU\Software\Microsoft\Internet Explorer\Main\Enable Browser Extensions

Check for Signatures on Downloaded Programs

This option gives control over a behavior that used to be preset. When an application is downloaded, it may be checked for an Authenticode signature. If there is no signature, then a warning prompt is given (in addition to any other messages associated with downloading files).

When implementing **Linked to C1**, this option is superfluous and can be **Disabled**.

When implementing **Linked to C2** or **Linked to C3,** this option should be **Enabled.**

\HKCU\Software\Microsoft\Internet Explorer\Download\CheckExeSignatures

New Privacy Options

Internet Explorer 5.5 limits cookies by zone and type. A brief summary of Internet Explorer 6.0's cookie policy is provided here. With Internet Explorer 6.0, cookies are automatically allowed in the Trusted Sites Zone and Intranet Zone, and are automatically prohibited in the Restricted Zone. A slider in the Privacy panel of Internet Options controls cookies in the Internet Zone. By default, Internet Explorer 6.0 accepts 1st party cookies but rejects 3rd party cookies if a compact P3P (Platform for Privacy Preferences) policy is missing or unacceptably permissive. Group Policy, as provided by Windows 2000, does not provide a convenient mechanism for controlling the Privacy setting. Fortunately, it can be safely left at the default in most instances. See the section entitled *Allow Cookies That Are Stored On Your Computer* for a discussion of the risks associated with cookies.

Appendix C: ADM Files

These ADM files are not written for internationalization. These ADM files are not intended for use with any Active Directory other than that provided with Windows 2000. These ADM files also do not have the recommended amount of help information. It is assumed that enough explanation of these settings is included in the earlier parts of this document.

A sample Group Policy ADM file for Internet Explorer 5.5 Settings under HKLM:

```
CLASS MACHINE
   CATEGORY "Windows Components"
   CATEGORY "Internet Explorer"
   CATEGORY "Advanced Internet Explorer Settings"
      POLICY "Code Base"
         KEYNAME "SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings"
         VALUEON NUMERIC 0 VALUEOFF NUMERIC 0
         PART
            "This setting controls where the code base is for ActiveX controls." TEXT
         END PART
         PART "Code Base Search Path"
            EDITTEXT
            VALUENAME "CodeBaseSearchPath"
         END PART
      END POLICY
   END CATEGORY
   END CATEGORY
   END CATEGORY
```

A sample Group Policy ADM file for Internet Explorer 5.5 Settings under HKCU:

```
CLASS USER
   CATEGORY "Windows Components"
   CATEGORY "Internet Explorer"
   CATEGORY "Advanced Internet Explorer Settings"
      POLICY "Check Certificate Revocation: Publisher Certificates"
         KEYNAME "SOFTWARE\Microsoft\Windows\CurrentVersion\WinTrust\Trust
Providers\Software Publishing\"
         VALUEON NUMERIC 0 VALUEOFF NUMERIC 0
         EXPLAIN "Be very careful in setting this bitfield.  This bitfield may
control things other than this setting, so make sure you follow instructions in the
documentation."
         PART
            "READ the documentation before setting this." TEXT
         END PART
         PART "Software Publishing State"
            NUMERIC
            MIN 500
            MAX 10000000
            VALUENAME "STATE"
         END PART
      END POLICY
      POLICY "Check Certificate Revocation: Server Certificates"
         KEYNAME "SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings"
         VALUENAME "DisableCachingOfSSLPages"
         VALUEON NUMERIC 1 VALUEOFF NUMERIC 0
         PART
            "Advice: This should be enabled." TEXT
         END PART
      END POLICY
      POLICY "Do Not Save Encrypted Pages to Disk"
         KEYNAME "SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings"
         VALUENAME "DisableCachingOfSSLPages"
         VALUEON NUMERIC 1 VALUEOFF NUMERIC 0
         PART
            "Advice: This should be enabled." TEXT
         END PART
      END POLICY
      POLICY "Empty Temporary Internet Files folder when browser is closed"
         KEYNAME "SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache"
         VALUENAME "Persistent"
         VALUEON NUMERIC 0 VALUEOFF NUMERIC 1
         PART
            "Advice: This should be disabled." TEXT
         END PART
      END POLICY
      POLICY "Use Fortezza"
         KEYNAME "SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings"
```

```
            VALUENAME "Fortezza"
            VALUEON NUMERIC 1 VALUEOFF NUMERIC 0
            PART
               "Advice: This should be enabled." TEXT
            END PART
         END POLICY
         POLICY "Cryptographic Protocols"
            KEYNAME "SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings"
            EXPLAIN "Advice: This should be set to enable SSL 3.0 as well as TLS 1.0,
and disable SSL 2.0 and PCT 1.0.  The number 160 might do this."
            PART
               "Bitfield of Cryptographic Protocols" NUMERIC
               VALUENAME "SecureProtocols"
            END PART
         END POLICY
         POLICY "Warn About Invalid Certificates"
            KEYNAME "SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings"
            VALUENAME "WarnonBadCertRecving"
            VALUEON NUMERIC 1 VALUEOFF NUMERIC 0
            PART
               "Advice: This should be enabled." TEXT
            END PART
         END POLICY
         POLICY "Warn if changing between secure and not secure mode"
            KEYNAME "SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings"
            VALUENAME "WarnonZoneCrossing"
            VALUEON NUMERIC 1 VALUEOFF NUMERIC 0
            PART
               "Advice: This should be enabled." TEXT
            END PART
         END POLICY
         POLICY "Warn if forms submittal is being redirceted."
            KEYNAME "SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings"
            VALUENAME "WarnonPostRedirect"
            VALUEON NUMERIC 1 VALUEOFF NUMERIC 0
            PART
               "Advice: This should be enabled." TEXT
            END PART
         END POLICY
         POLICY "Disable password caching"
            KEYNAME "SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings"
            VALUENAME "DisablePasswordCaching"
            VALUEON NUMERIC 1 VALUEOFF NUMERIC 0
            PART
               "Advice: This should be enabled." TEXT
            END PART
         END POLICY
         POLICY "Enable Browser Extensions IE6"
            KEYNAME "Software\Microsoft\Internet Explorer\Main"
```

```
      VALUENAME "Enable Browser Extensions"
      VALUEON NUMERIC 1 VALUEOFF NUMERIC 0
      PART
         "Advice: This should be disabled." TEXT
      END PART
   END POLICY
   POLICY "Check for Signatures on Downloaded Programs IE6"
      KEYNAME "Software\Microsoft\Internet Explorer\Download"
      VALUENAME "CheckEXESignatures"
      VALUEON NUMERIC 1 VALUEOFF NUMERIC 0
      PART
         "Advice: This depends on group decision D" TEXT
      END PART
   END POLICY
END CATEGORY
END CATEGORY
END CATEGORY
```

Appendix D: Internet Explorer and Group Policy References

http://www.microsoft.com/windows/ie/default.asp
Microsoft's Internet Explorer Home Page

http://www.secadministrator.com/Articles/Index.cfm?ArticleID=20468
This is a 6-part article by Randy Franklin Smith explaining security features of Internet Explorer 5.0.

http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp
This white paper contains an explanation of Group Policy settings, including sections for Internet Explorer settings.

http://www.microsoft.com/windows/ie/techinfo/overview/default.asp
Microsoft Internet Explorer 6 Technical Overview – explains changes new in version 6.0.

http://www.microsoft.com/windows2000/techinfo/howitworks/management/rbppaper.asp
An explanation of Registry-Based Policy; also contains the ADM Language Reference.

http://www.guninski.com/
Georgi Guninski Security Research explains and demonstrates vulnerabilities in Internet Explorer.

Appendix E: Configuration Summary Worksheets

Options Chosen
A 1 2 B 1 2 3 C 1 2 3 D 1 2 3

Worksheet 1: Group Policy Settings Provided By Microsoft

Setting Location	Setting Name	Recommended Value(s)	Your Value
Computer Configuration:Administrative Templates:Windows Components:Internet Explorer	Security Zones: Use only machine settings.	Disabled	
	Security Zones: Do not allow users to change policies.	Enabled	
	Security Zones: Do not allow users to add/delete sites.	Enabled	
	Make proxy settings per-machine (rather than per-user)	Disabled / Enabled	
	Disable Automatic Install of Internet Explorer components	Enabled	
User Configuration:Windows Settings:Internet Explorer Maintainance:Connection	Connection Settings	Set (D1) *make notes on these settings elsewhere* Left Blank (D2 D3)	
User Configuration:Windows Settings:Internet Explorer Maintainance:Security:Security Zones and Content Ratings	See Worksheet 2: Security Settings By Zone		
User Configuration:Administrative Templates:Windows Components:Internet Explorer:Internet Control Panel	Disable the Securtiy Page, Disable the Advanced Page	Enabled	
User Configuration:Administrative Templates:Windows Components:Internet Explorer:Internet Control Panel	Disable the Connections Page	Enabled (D1 or D2) Disabled (D3)	

Options Chosen
A 1 2 B 1 2 3 C 1 2 3 D 1 2 3

Worksheet 1 Continued

Setting Location	Setting Name	Recommended Value(s)	Your Value
User Configuration:Administrative Templates:Windows Components:Internet Explorer	Disable Changing Advanced Page Settings, Disable Changing Certificate Settings, Disable Changing Automatic Configuration Settings	Enabled	
	Disable Internet Connection Wizard[4], Disable Changing Connection Settings, Disable Changing Proxy Settings	Enabled (D1 or D2), Disabled (D3)	
	Do not allow AutoComplete to save passwords	Enabled	
User Configuration:Administrative Templates:Windows Components:Internet Explorer:Offline Pages	Disable adding channels Disable removing channels Disable adding schedules for offline pages Disable editing schedules for offline pages Disable removing schedules for offline pages Disable offline page hit logging Disable all schedule offline pages Disable channel user interface completely Disable downloading of site subscription content Disable editing and creating of schedule groups	Enabled	
User Configuration:Administrative Templates:Windows Components:Internet Explorer:Browser Menus	Disable Save this program to disk option	Enabled (C1 or C2) Disabled (C3)	

[4] This setting has an associated warning.

Options Chosen

A 1 2 B 1 2 3 C 1 2 3 D 1 2 3

Worksheet 2: Security Settings By Zone

	Restricted Zone		Internet Zone		Trusted Sites Zone	
Setting Name	**Recomm. Value**	**Your Value**	**Recomm. Value**	**Your Value**	**Recomm. Value**	**Your Value**
Download Signed ActiveX Controls	Disable		Disable (B1 or B2) or Enable (B3)		Disable (B1) or Enable (B2 or B3)	
Download Unsigned ActiveX Controls	Disable		Disable		Disable	
Initialize and Script ActiveX Controls Not Marked as Safe	Disable		Disable		Disable	
Run ActiveX Controls and Plug-ins	Disable		Disable (A1) or Enable (A2)		Enable	
Script ActiveX Controls Marked Safe for Scripting	Disable		Disable (A1) or Enable (A2)		Enable	
Allow Per Session Cookies (IE 5.5 Only)	Disable		Enable		Enable	
Allow Cookies That Are Stored on Your Computer (IE 5.5 Only)	Disable		Disable/Enable		Enable	
File Download	Disable		Disable (C1) or Enable (C2, C3)		Enable	
Font Downolad	Disable		Disable		Disable	
Java Permissions	Disable Java		Disable Java or High Safety		High Safety	
Access Data Sources Across Domains	Disable		Disable		Disable	
Don't Prompt for Client Certificate Selection When No Certificates or Only One Certificate Exists	Disable		Disable		Disable	
Drag and Drop or Copy and Paste Files	Disable		Disable		Disable	
Installation of Desktop Items	Disable		Disable		Disable	

Options Chosen

A 1 2 B 1 2 3 C 1 2 3 D 1 2 3

Worksheet 2 Continued

	Restricted Zone		**Internet Zone**		**Trusted Sites Zone**	
Setting Name	**Recomm. Value**	**Your Value**	**Recomm. Value**	**Your Value**	**Recomm. Value**	**Your Value**
Launching Application and Files in IFRAME	Disable		Disable		Disable	
Submit Non-Encrypted Form Data	Disable		Prompt		Prompt	
UserData Persistence	Disable		Disable		Disable	
Active Scripting	Disable		Disable (A1) or Enable (A2)		Enable	
Allow Paste Operations Via Script	Disable		Disable		Disable	
Scripting Java Applets	Disable		Disable or Prompt		Enable	
Logon	Anonymous Logon Only		Prompt for Username and Password		Prompt for Username and Password	
Meta Refresh (IE6 Only)	Disabled		Disabled		Enabled	
Display Mixed Content (IE6 Only)	Disabled		Prompt		Prompt	

Options Chosen

A 1 2 B 1 2 3 C 1 2 3 D 1 2 3

Worksheet 3: Group Policy Settings Provided by ADM Templates

Setting Location	Setting Name	Recommended Value(s)	Your Value
User Configuration:Administrative Templates:Windows Components:Internet Explorer:Advanced Internet Explorer Settings	Check Certificate Revocation: Publisher Certificates	Enabled and Numeric Value	
	Check Certificate Revocation: Server Certificates	Enabled	
	Do not save encrypted pages to disk	Enabled	
	Empty Temporary Internet Files folder when Browser is closed	Enabled/Disabled	
	User Fortezza	Enabled	
	Cryptographic Protocols	Enabled and Numeric Value	
	Warn About Invalid Certificates	Enabled	
	Warn if forms submittal is being redirected	Enabled	
	Disable Password Caching	Enabled	
	Enable 3rd Party Browser Extensions (IE6 only)	Disable	
	Check for Signatures on Downloaded Programs (IE6 Only)	Disabled (C1) or Enabled (C2 or C3)	
Computer Configuration:Administrative Templates:Windows Components:Internet Explorer:Advanced Internet Explorer Settings	Code Base	Enabled and Clear (B1) or Enabled and Text Value (B2 or B3)	