Global Information Assurance Certification Paper

Usefulness and Shortcomings of the Pre-configured Security Policy Templates that are Included with Windows 2000

Yong Seong Choe
March 6, 2001

I. Introduction

This paper analyzes the security policy template files provided by Windows 2000 to identify their uses and possible short-comings. After a brief introduction of the security template concept and associated tools in section II and III, Section IV presents a detailed analysis of each security policy template.

Windows2000 security policy templates are text-based configuration files that can be used to analyze and configure Windows 2000 based system security. These templates can be manipulated by The Security Configuration Tool Set supplied with the operating system, and it serves as a single point of managing multiple security attributes. The tool set includes secedit, Security Template, Security Configuration and Analysis add-ins, and Security Settings extensions to Group Policy.

The discussion involves the following pre-defind security templates are found in %SystemDir%\Security\Templates directory:

- Default Windows 2000 Workstation (Basicwk.inf)
- Default Windows 2000 Server (Basicsv.inf)
- Default Windows 2000 Domain Controller (basicdc.inf)
- Secure Windows 2000 Workstation/Server Securews.inf
- Windows 2000 Domain Controller (Securedc.inf)
- Highly Secure Windows 2000 Workstation/Server (Hisecws.inf)
- Highly Secure Windows 2000 Domain Controller (Hisecdc.inf)
- Compatible Windows 2000 Workstation/Server (Compatws.inf)
- Optional Components Workstation (Ocfilesw.inf)
- Optional Components Server (Ocfiless.inf)

The predefined templates listed above are helpful in configuring an environment for varying degree of security and interoperability. This paper examines how each template configures the system, identify their purpose, and identify any trade-off for using one set of templates vs. another.

II. Overview of Security Configuration

2.1 Account Policies

The account policies define security settings for the user and system accounts. They include password, account lockout and Kerberos policies. The password policy defines password aging, length and complexity rules. Account lockout policy governs how and when a user account can be locked out, and how and when the locked account can be unlocked.

A Windows 2000 system can be configured to lock accounts when there are more than a certain number of failed attempts to log-on within specified time interval. The locked accounts can be unlocked by either the administrator, or by expiration of lock period. Kerberos Policy only applies to the domain controllers because local logons does not use Kerberos for authentication. The entries include the lifetimes for service ticket, user ticket and user ticket renewal, logon restrictions, and the tolerance for computer clock synchronization.

2.2 Local Policies

Local Policies define the security settings for the local machine including the Audit Policy, User Rights Assignment, and the Security Option.

Audit policy determines what kind of events should be logged. Depending on the settings, the system will log various events such as account log-on, object access, directory services access, etc. Refer to Table 4.2 for a list of audit policy attributes.

User Rights define what of a group or a user are able to do in the system. For example, the Internet Information Server account need the right to log-on locally to function properly. The detailed list is defined in Table 4.3.

Many of the attributes under the Security Option had to be set using the registry editor. The examples are the removal of the last username from the logon prompt, displaying a text message during the log-on process, the use of password filter to define the complexity, etc.

2.3 Event Logs

Event Logs section defines how log files are managed. The log file size limit, the retention period, rules for overwriting recorded events, and how to handle the situation when an attempt to log an even fails for any reason.

2.4 Security Services

The configuration under Security Services determines how Windows services should whether to start automatically at reboot, and how they should run.

2.5 Restricted Groups

Restricted Group became available in Windows 2000. As a part of security policy, group membership can be pre-configured. This feature may be useful in making sure that only authorized users belong to privileged groups.

2.6 File System Security

The file system permissions and auditing can be defined though the use of a security policy template. The administrator can add filesystem objects and define the permissions, and the auditing status.

2.7 Registry Security

The registry key security settings, similarly to the file system settings, can be configured using the security policy template. The use of security template is less likely to introduce errors than the use of a registry editor (e. g. regedt32.exe).

III. Security Configuration Tool Set

A security policy template can be used to define organizes security parameters and attributes described in the previous section. The following tools are available with Windows 2000. They can be used to create security policy templates and apply them:

- Security Template snap-in: A stand-alone Microsoft Management Console (MMC) snap-in used to create a text based template file (.inf) that contains security settings.

- Security Configuration and Analysis snap-in: A stand-alone MMC snap-in that can configure or analyze a Windows 2000 system based on the security settings in a template available by default installation of Windows 2000 or created by using Security Templates snap-in. This tool can also export the current system security settings, so that they can be applied in other systems.

- Secedit.exe: A command line version of the security configuration and analysis snap-in. Because this tool is command-line based, it can be used to script security analysis and configuration for many machines.

- Security Settings extension to Group Policy: An extension snap-in to the group policy editor to configure local security policies as well as security policies for domain or organizational units. The Security Configuration and Analysis snap-in does not have the capability to configure or analyze security configuration of a domain or organizational unit (OU). This tool only allows the configuration of security for domains and OU, and the configuration, still, cannot be analyzed and exported.

"Step-by-Step Guide to using the Security Configuration Tool Set" provides an example of how these tools can be utilized to view, configure and analyze local security settings. This document can be found in Microsoft official Windows 2000 Web site.

IV. Pre-defined Security Policy Templates

4.1 Overview of Security Policy Templates

The predefined security templates can be divided into five categories according to their purposes. The basic security templates represent the default security settings from a clean Windows 2000 installation with minimal – but improved from Windows NT 4.0 in terms of filesystem access control – security measues. The secure templates can be applied in increment to the basic security setting to adopt more stringent account protection, auditing and other aspects of system security. The high security templates are applied in increment to the default installation (basic security) to achieve the highest level of security, but at the cost of additional processing time for auditing, and loss of interoperability with older version of Windows systems. The compatibility template is provided solely for the purpose of enabling the "Users" group to run legacy Windows applications. The optional component filesystem security template are provided to secure the compont that may or may not have been installed.

4.1.1 Basic Security Template

Files: basicdc.inf, basicsv.inf, and basicwk.inf

Basicdc.inf file is used for Windows 2000 domain controllers; basicsv.inf is used for standalone servers; and basicwk.inf is used to apply the settings to workstations.

Basic Security Policy Templates are provided to restore the default security settings that are configured when clean installation is performed. The template files in basic category will apply the *default* security settings in a clean Windows 2000 installation except user rights and group membership.

4.1.2 Secure Security Policy Tempate

Files: securedc.inf, securews.inf

Securedc.inf is used for domain controllers, and securews.inf is used for a workstation or a server.

This template is to be incrementally applied to the Windows 2000 Default configuration or the basic security policy to enhance security in the areas of account password and lockout policy, auditing, and various other aspects of security. It removes all members from Power Users group. Secure Security Policy does not modify access control lists (ACLs) for the filesystem and the registry.

Securedc.inf file is applied to the domain controller; securews.inf is applied to either the workstation or the server.

4.1.3 Highly Secure Security Policy Templates

Files: Hisecws.inf, hisecdc.inf

Highly secure settings must be used in a native mode Windows 2000 network. The policy requires digitally signed and encrypted communication between servers and clients. Auditing is most extensive, and account password and lockout policies are most stringent. This template is to be applied to Secure Security Policy Template to augment the level of security. The enhanced security comes at the cost of interoperability, system availability, and the cost.

4.1.4 Compatible Security Policy Template

Files: Compatws.inf

Compatible Security Policy Template enables the users that belongs to "Users" group to run non-Windows 2000 compliant systems. When a Windows NT system is upgraded, "Authenticated Users Group" members automatically assigned to Power Users so that the users have sufficient permissions to run legacy windows applications that may write temporary files or some subkeys under HKEY_LOCAL_MACHINE. This template grants bare minimum rights to enable users to run the legacy applications without these users belonging to the Power Users group.

4.1.5 Optional Component Filesystem Security Policy Template

Files: ocfilesw.inf, ocfiless.inf

These template files are used to set filesystem and registry access control list settings for the selected optional components.

4.2 Close-up Analysis Security Policy Comparison

This section shows how each security template is set to configure different categories of security attributes.

4.2.1 Account Policies

The security templates provided by Windows 2000 defines password policy and account lockout policy. The kerberos policy is not preconfigured in any of the listed predefined template because Kerberos is not the only secure protocol that provides authentication service in Windows 2000.

	Basic*	Secure*	High*
Password			
Enforce password history	0	24	24
Maximum password age	42	42	42
Minimum password age	0	2	2
Minimum password length	0	8	8
Passwords must meet complexity requirement	Disabled	Enabled	Enabled
Store password using reversible encryption for all users	Disabled	Disabled	Disabled
Account Lockout			
Lockout duration	Not Defined	30 min	0
Lockout threshhold	None	5	5
Reset account lockout counter after	Not Defined	30 min	30 min

Table 4.1 Account Policies Comparison

Basic template merely prompts the user to change its password every 42 days, but the user may cleverly get away with it by changing the password to his/her old password. Basic template does not check the length of the password, and the password does not have to meet the complexity requirement. A secure password tends to be a combination of upper and lower case letters, numbers and other legal symbols.

Basic template also does not need an account lockout policy because accounts are never locked when basic template is applied.

In secure and highly secure settings, the user account would be locked out after five failed attempts to log on. While permitting the maximum availability to the users. The secure and highly secure template provides similar level of password security. The only difference is that the highly secure settings require an Administrator intervention to unlock an account when secure settings makes the user wait 30 minutes each time account is locked out.

4.2.2 Local Policies

Local policies consist of Audit Policy, User Rights and Security Options. Audit Policy and Security Options are defined in basic*.inf, secure*.inf, and hisec*.inf templates.

4.2.2.1 Audit Policy

NA – No audit
ND – Not defined
F – Failure
S – Success

	basicwk	Basicsv	securews	securedc	highws	highdc
Account log on	NA	NA	SF	F	SF	SF
Account management	NA	ND	SF	SF	SF	SF
Directory Service Access	ND	ND	ND	F	ND	SF
Logon event	NA	NA	F	F	SF	SF
Object access	NA	NA	NA	NA	SF	SF
Policy Change	NA	NA	SF	SF	SF	SF
Privilege Use	NA	NA	F	F	SF	SF
Audit process tracking	NA	NA	NA	NA	ND	NA
System event	NA	NA	NA	NA	SF	SF

Table 4.2 Audit Policy Comparison

4.2.2.2 User Rights

User rights are not defined in any of the security settings provided by Windows 2000. Table 4.3 lists the default settings of clean Windows 2000 servers and workstations.

User Right	Default Workstation	Default Server
Replace a Process-Level Token		
Generate Security Audits		
Logon as a Batch Job		
Backup Files and Directories	Administrators, Backup Ops	Administrators, Backup Ops
Bypass Traverse Checking	Administrators, Backup Ops, Power Users, Users, Everyone	Administrators, Backup Ops, Power Users, Users, Everyone
Create a Pagefile	Administrators	Administrators
Create Permanent Shared Objects		

Create a Token Object		
Debug Programs	Administrators	Administrators
Increase Scheduling Priority	Administrators	Administrators
Increase Quotas	Administrators	Administrators
Logon Interactively	Administrators, Backup Ops, Power Users, Users, Guest[1]	Administrators, Backup Ops, Power Users, Users, Guest
Load and Unload Device Drivers	Administrators	Administrators
Lock Pages in Memory		
Add workstations to the domain		
Access this computer from the network	Administrators, Backup Ops, Power Users, Users, Everyone	Administrators, Backup Ops, Power Users, Users, Everyone
Profile a single process	Administrators, Power Users	Administrators, Power Users
Force shutdown from a remote system	Administrators	Administrators
Restore files and directories	Administrators, Backup Ops	Administrators, Backup Ops
Manage audit and security logs	Administrators	Administrators
Log on as a service		
Shutdown the system	**Administrators, Backup Ops, Power Users, Users**	**Administrators, Backup Ops, Power Users**
Modify firmware environment variables	Administrators	Administrators
Profile system performance	Administrators	Administrators
Change system time	Administrators, Power Users	Administrators, Power Users
Take ownership of files or other objects	Administrators	Administrators
Act as part of the OS		
Deny Interactive Logon		
Deny Batch Logon		
Deny Service Logon		

[1] The Guest account must be enabled before it is allowed to log on interactively.

Deny Network Logon		
Remove Computer from a Docking Station	Administrators, Power Users, Users	Administrators, Power Users, Users
Synchronize Directory Service Data		
Enable computer and user accounts to be trusted for delegation		

Table 4.3. Windows 2000 Default User Rights (From Microsoft, 2000, "Default Access Control Settings in Windows 2000")

4.2.2.3 Security Options

Table 4.4 shows the security options that are defined at the three levels of security. From the basic level to the high security level, various attributes increase in the strength of the security.

- **Log-on Process Suspension**

In basic level for workstation, crt+alt+delete requirement for log-on is also not enforced. Lack of crt+alt+delete requirement adds to the convenience, saving an extra step, but this combination of keys suspends all programs, and possibly a Trojan that records the user's key-stroke.

- **Virtual Memory Flush**

The virtual memory may store sensitive information including but not limited to passwords and other sensitive information. When the system is shut down, it is generally good security practice to flush the virtual memory so that the information stored in the virtual memory is not available in case the page file is compromised. In high security policy template, the virtual memory pages will be wipe out before the system shut down.

- **Built-in Accounts**

It is recommended that the guest account be disabled, and the administrator account to be renamed in most of today's recommended security settings. The security templates provided by Windows 2000 does not (can not) perform this task for the administrator. Therefore, rename administrator and guest account setting is not defined in any OS supplied policy template.

- **Network Authentication and Communication**

In basic security setting, anonymous connection (null session) can be established without any restrictions. In secure setting, the enumeration is disabled, and in high security settings, any anonymous access is disallowed unless an explicit permission is set.

LAN Manager authentication level varies among the three security levels. On this attribute, increasing security creates a tradeoff of interoperability between Windows 2000 and older operating systems. LM authentication enables the use of Windows 95/98 workstation to be able to log onto Windows 2000, and NTLM authentication allows the user to log on from Windows NT4 workstation. NTLMv2 is the most secure, and high security level settings only allows the authentication of clients or servers with NTLMv2.

The interoperability trade-off also comes due to the varying security setting for the secure channel. While basic and secure settings use digital encryption and signature only when available, high security settings only allow digitally signed and encrypted communication. Because of these requirements, a system configured with high security level settings will only be able to interoperate with Windows 2000 systems (for now).

- **Smart Card Behavior**

The basic security setting would only require smart card only at the time the OS authenticates the user, and its removal does not affect the operation. This may add to the vulnerability by having a user loggin onto a system with a smart card, and leaving the system without logging off. Unless the user is logged off, an unauthorized user may take over the session, and use the system with that user's privilege. Gaining of non-privileged user rights is a significant step towards the gaining of privileged access. Secure and high security settings will either lock the workstation, or force the user to log off.
Driver and Non-driver Installation

- **Software and Driver Installation**

Software and driver installation is another area that may introduce rogue programs to the system. In this setting, the decision involves the trade-off between the availability (or cost) of the hardware or software, and security. Windows 2000 does not guarantee compatibility with all types of hardware, and the user may be forced to use a third party driver or software. When a software or driver is not signed by a trusted authority (Code signing CA), the user must assume the risk of installing a rogue software. Basic security level setting does change the settings to warn or disallow the installation of the unsigned code. Both secure and high security setting will allow the installation of non-driver software without warning. Because of HAL (Hardware Abstraction Layer) and other windows architecture, non-driver software are allowed to run in more limited sand-box than drivers are. However, drivers have direct access to the hardware, and
In secure settings, a workstation or server will allow the installation with a warning, but a domain controller would not allow the installation if the software were a driver. In high security settings, the installation of unsigned drivers is not allowed.

	Basic(wk/sv/dc)	Secure (ws/dc)	HiSec (ws/dc)
Additional restrictions for anonymous connections	None	Do not allow enumeration of shares & SAM accounts	No Access w/o explicit permissions
Allow server operators to schedule tasks (DC only)	ND	ND/Disabled	Disabled
Allow system to be shut down without having to log on	En/Disabled/Disabled	ND/Disabled	ND/Disabled
Allowed to eject removable NTFS media	Administrators	Administrators	Administrators
Amount of idle time required before disconnecting session	15 minutes	15 min	15 min
Audit the access of global system objects	Disabled	Disabled	disabled
Audit use of backup and resotre previlege	Disabled	Disabled	disabled
Automatically log off users when logon time expires	ND	ND/Enabled	Enabled
Automatically log off users when logon time expires(local)	ND/Enabled	Enabled	ND/Enabled
Clear virtual memory pagefile when system shuts down	Disabled	Disabled	Enabled
Digitally sign client communication (always)	Disabled	Disabled	Enabled
Digitally sign client communication (when possible)	Enabled	Enabled	Enabled
Digitally sign server communication (always)	Disabled	Disabled	Enabled
Digitally sign server communication (when possible)	Disabled	Enabled	Enabled
Disable ctrl+alt+del requirement for logon	ND/Disabled/ Disabled	Disabled	Disabled
Do not display last user name in logon screen	Disabled	Disabled	Enabled
LAN Manager Authentication Lebel	Send LM & NTLM responses	Send NTLM response only	Send NTLM v2 response only/refuse LM & NTLM
Message text for users attempting to log on			
Message title for users attempting to log on			
Number of previous logons to cache (in case domain controller is not available)	10	10	10 logons
Prevent system maintenance of computer account password	Disable	Disabled	Disabled
Prevent users from installing printer drivers	Disabled/Enabled/Enabled	Enabled	Enabled
Prompt user to change password before expiration	14 days	14 days	14 days
Recovery Console: Allow automatic administrative login	Disabled	Disabled	Disabled
Recovery Console: Allow floppy copy and access to all drives	Disabled	Disabled	Disabled
Rename administrator account	ND	ND	ND
Rename guest account	ND	ND	ND
Restrict CD-ROM access to locally logged-on user only	Disabled	Disabled	Disabled/Enabled
Restrict floppy access to locally logged-on user only	Disabled	Disabled	Disabled/Enabled
Secure channel: digitally encrypt or sign secure channel data (always)	Disabled	Disabled	Enabled
Secure channel: digitally encrypt secure channel	Enabled	Enabled	Enabled

data (When possible)			
Secure channel: Digitally sign secure channel data (when possible)	Enabled	Enabled	Enabled
Secure Channel: Require strong (windows 2000 or later) session key	Disabled	Disabled	Enabled
Secure system partition (for RISC only)	ND	ND	Not defined
Send unencrypted password to connect to third-party SMB servers	Disabled	Disabled	Disabled
Shutdown system immediately if unable to log security audits	Disabled	Disabled	Disabled
Smart card removal behavior	No Action	Lock WK/Force logoff	Lock WK/Force logoff
Strengthen default permissions of global system objects (Symbolic links)	Enabled	Enabled	Enabled
Unsigned driver installation behavior	ND	Warn but allow /Do not allow	Do not allow installation
Unsigned non-driver installation behavior	ND	Silently succeed	Silently succeed

Table 4.4. Security Options Comparison

4.2.3 Event Logs

The event log settings are characterized by the size of the log file, access of a guest account to the log file, number of days of retention, retention method, and shutting down the computer when the audit log is full.

Basic security setting sets limited logging capability that could easily be destroyed. The logs are kept for 7 days, and guest user is not restricted to view the event log.

Event log has two main purposes: trouble shooting and evidence gathering for unauthorized use. Basic security template is only useful for troubleshooting. An end-user (non-privileged) that may want to see why Windows Office program would not save his/her file will benefit from inspecting the log. In terms of gathering traces of unauthorized access, it is much easier to flood the event log to overwrite any entries that the offender wants to hide. For example, if a guest user have gained an unauthorized resource, then the guest can view the event log to check if his/her activity was logged. If it was logged, then the guest user can cause other events repeatedly using a script or other automated means to cause the log files to overwrite the true offense that the guest user committed. Logging event can be expensive in terms of CPU cycles and storage spaces, and this policy is suitable when processing power is important.

The events are retained for seven days, and seven days' worth of event log may be used to set-up a baseline use of the system for log analysis tools to identify abnormal usage pattern.

In secure and high security settings, the log files are 10x and 20x larger respectively than the basic settings because more information is being logged. The sizes of the log have to

be adjusted appropriately according to the auditing policy. These settings do not allow guest users to view the log file, and the logs will not be overwritten unless the limit is reached.

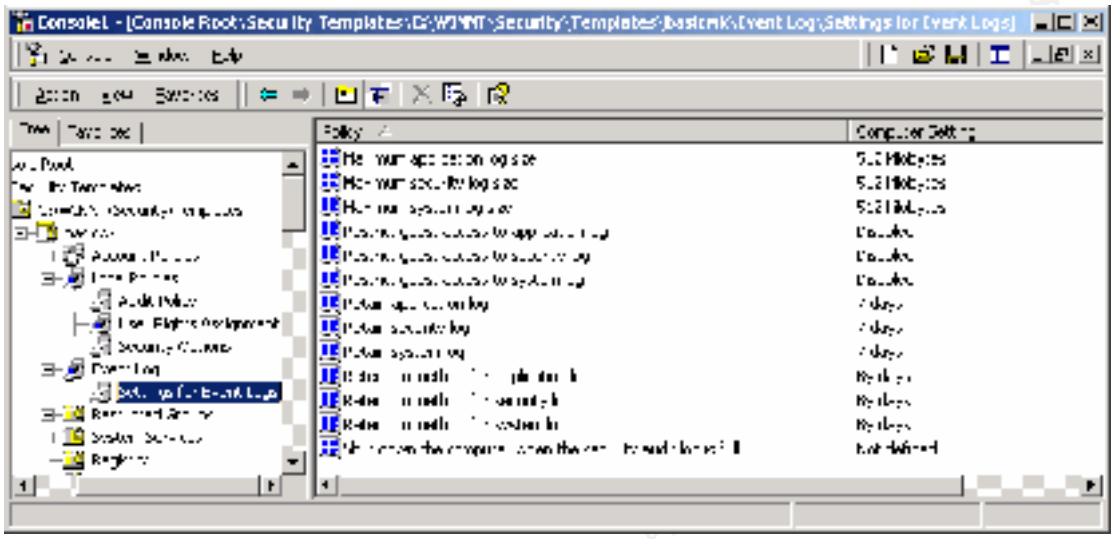

Figure 4.1. Basic Level Event Log Security Settings

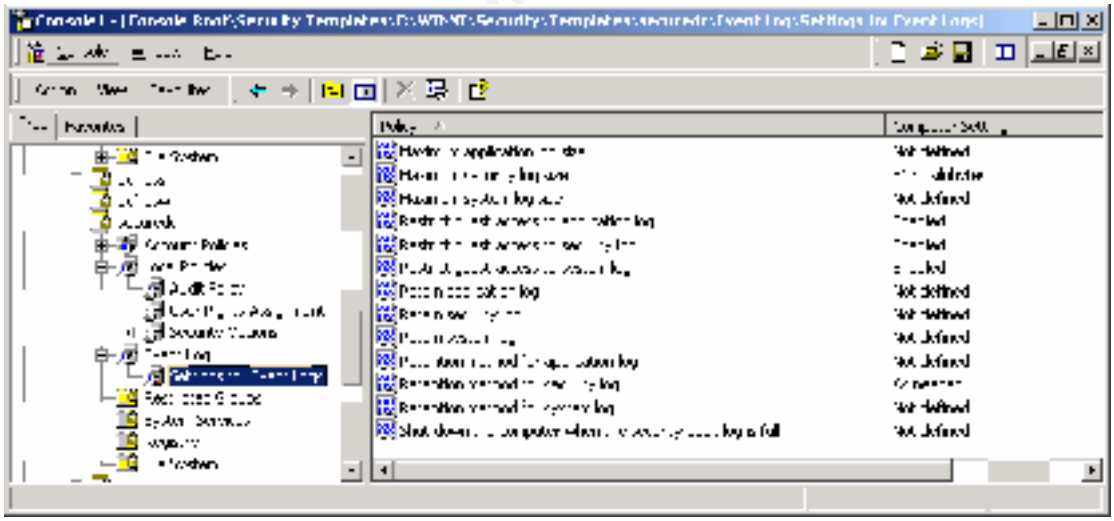

Figure 4.2. Secure Security Level Event Log Security Settings

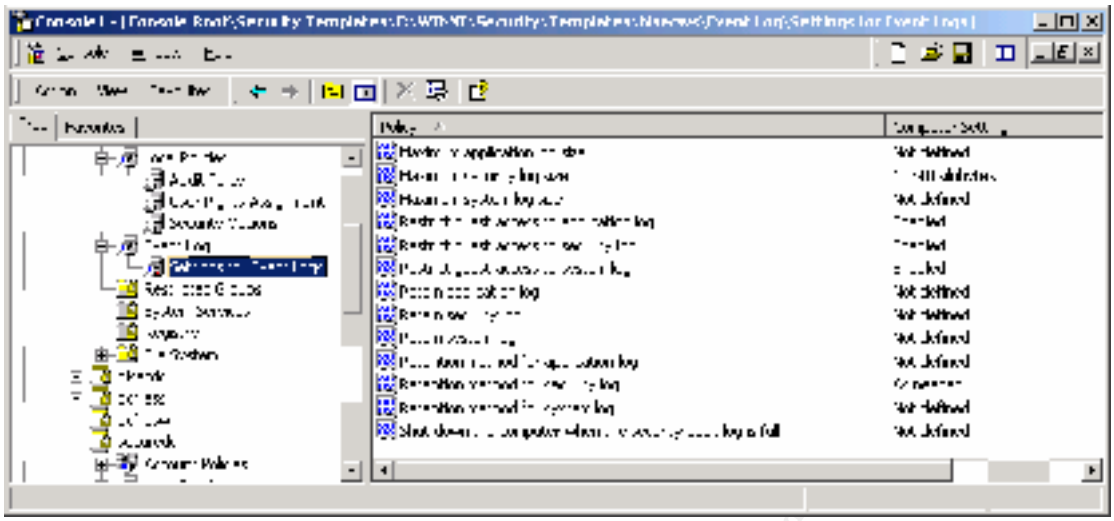

Figure 4.3. High Security Level Event Log Security Settings

4.2.4 Restricted Group

Secure template removes all the members of Power Users group to make the system more secure. Compatible template does the same to enhance the security, but after making the granting more access permissions to the "Users" group.

4.2.5 System Services

System Services defines which how various services are started and behaved. Secure template and high security template does not configure this category. However, since there are some services that could be safely disabled depending on the configuration, it is advised that the customized template would disable extra services that can be safely disabled. Figure 4.4 shows a snapshot of how basic template configures the security services.

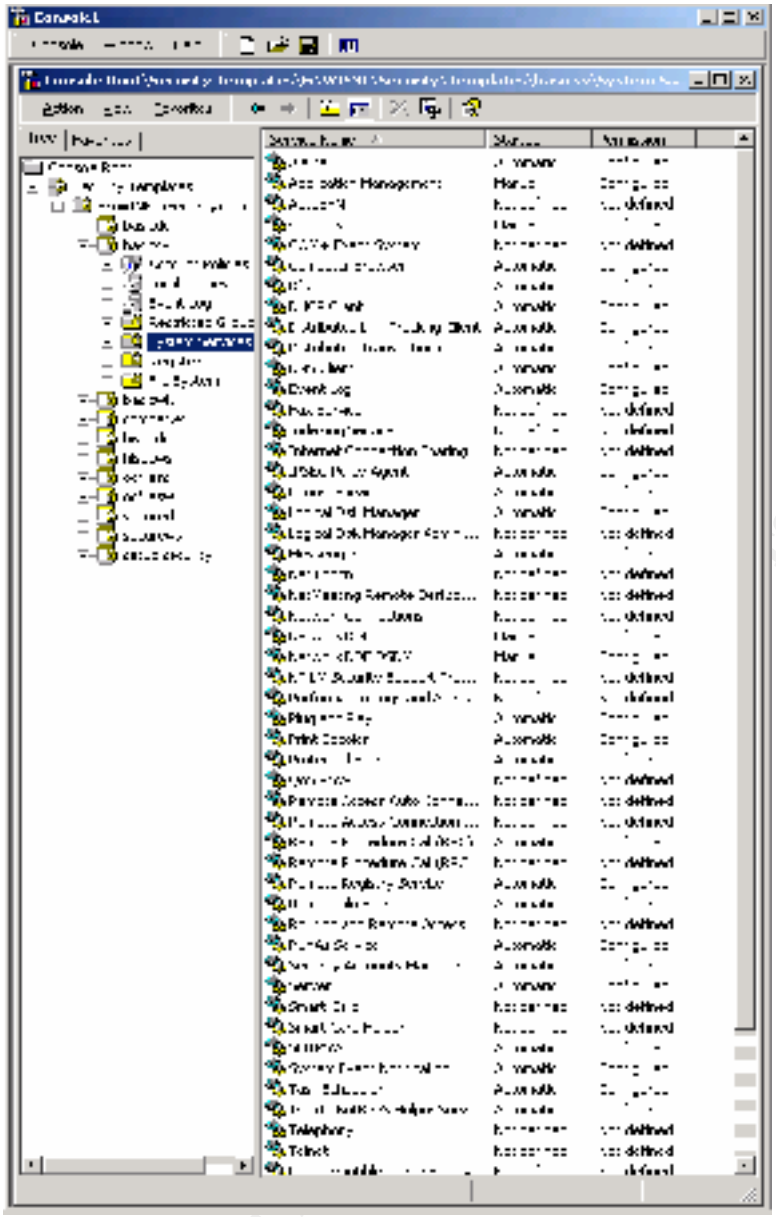

Figure 4.4. Snapshot View of Security Services from MMC Security Template snap-in

4.2.6 File System

Basic security template configures HKEY_LOCAL_MACHINE key with the permissions listed in Table 4.7. The high security template strips reduces the rights of the Power Users to "Read Only" from "Modify" in key areas.

File System Object	Default Power User Permissions	Default User Permissions
c:\boot.ini	RX	None

c:\ntdetect.com	RX	None
c:\ntldr	RX	None
c:\ntbootdd.sys	RX	None
c:\autoexec.bat	Modify	RX
c:\config.sys	Modify	RX
\ProgramFiles	Modify	RX
%windir%	Modify	RX
%windir%*.*	RX	RX
%windir%\config*.*	RX	RX
%windir%\cursors*.*	RX	RX
%windir%\Temp	Modify	Synchronize, Traverse, Add File, Add Subdir
%windir%\repair	Modify	List
%windir%\addins	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\Connection Wizard	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\fonts*.*	RX	RX
%windir%\help*.*	RX	RX
%windir%\inf*.*	RX	RX
%windir%\java	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\media*.*	RX	RX
%windir%\msagent	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\security	RX	RX
%windir%\speech	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\system*.*	Read, Execute	RX
%windir%\twain_32	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\Web	Modify (Dir\Subdirs) RX (Files)	RX
%systemdir%	Modify	RX
%systemdir%*.*	RX	RX
%systemdir%\config	List	List
%systemdir%\dhcp	RX	RX
%systemdir%\dllcache	None	None
%systemdir%\drivers	RX	RX

%systemdir%\CatRoot	Modify (Dir\Subdirs) RX (Files)	RX
%systemdir%\ias	Modify (Dir\Subdirs) RX (Files)	RX
%systemdir%\mui	Modify (Dir\Subdirs) RX (Files)	RX
%systemdir%\OS2*.*	RX	RX
%systemdir%\OS2\DLL*.*	RX	RX
%systemdir%\RAS*.*	RX	RX
%systemdir%\ShellExt	Modify (Dir\Subdirs) RX (Files)	RX
%systemdir%\Viewers*.*	RX	RX
%systemdir%\wbem	Modify (Dir\Subdirs) RX (Files)	RX
%systemdir%\wbem\mof	Modify	RX
%UserProfile%	Full Control	Full Control
All Users	Modify	Read
All Users\Documents	Modify	Read, Create File
All Users\Application Data	Modify	Read

Table 4.7. Default Access Control Settings for File System Objects (From Microsoft, 2000, "Default Access Control Settings in Windows 2000")

4.2.7 Registry Security

Basic security template configures HKEY_LOCAL_MACHINE key with the permissions listed in Table 4.7. The high security template reduces the permissions of the Power Users to "Read Only" from "Modify" in key areas.

Registry Object	Default Power User Permissions	Default User Permissions
HKEY_LOCAL_MACHINE		
HKLM\Software	**Modify**	**Read**
HKLM\SW\Classes\helpfile	Read	Read
HKLM\SW\Classes\.hlp	Read	Read
HKLM\SW\MS\Command Processor	Read	Read

HKLM\SW\MS\Cryptography	Read	Read
HKLM\SW\MS\Driver Signing	Read	Read
HKLM\SW\MS\EnterpriseCertificates	Read	Read
HKLM\SW\MS\Non-Driver Signing	Read	Read
HKLM\SW\MS\NetDDE	None	None
HKLM\SW\MS\Ole	Read	Read
HKLM\SW\MS\Rpc	Read	Read
HKLM\SW\MS\Secure	Read	Read
HKLM\SW\MS\SystemCertificates	Read	Read
HKLM\SW\MS\Windows\CV\RunOnce	Read	Read
HKLM\SW\MS\W NT\CV\DiskQuota	Read	Read
HKLM\SW\MS\W NT\CV\Drivers32	Read	Read
HKLM\SW\MS\W NT\CV\Font Drivers	Read	Read
HKLM\SW\MS\W NT\CV\FontMapper	Read	Read
HKLM\SW\MS\W NT\CV\Image File Execution Options	Read	Read
HKLM\SW\MS\W NT\CV\IniFileMapping	Read	Read
HKLM\SW\MS\W NT\CV\Perflib	Read (via Interactive)	Read (via Interactive)
HKLM\SW\MS\W NT\CV\SecEdit	Read	Read
HKLM\SW\MS\W NT\CV\Time Zones	Read	Read
HKLM\SW\MS\W NT\CV\Windows	Read	Read
HKLM\SW\MS\W NT\CV\AsrCommands	Read	Read
HKLM\SW\MS\W NT\CV\Winlogon	Read	Read
HKLM\SW\MS\W NT\CV\Classes	Read	Read
HKLM\SW\MS\W NT\CV\Console	Read	Read
HKLM\SW\MS\W NT\CV\ProfileList	Read	Read
HKLM\SW\MS\W NT\CV\Svchost	Read	Read
HKLM\SW\Policies	Read	Read
HKLM\System	**Read**	**Read**
HKLM\SYSTEM\CCS\Control\SecurePipeServers\winreg	None	None
HKLM\SYSTEM\CCS\Control\Session Manager\Executive	Modify	Read
HKLM\SYSTEM\CCS\Control\TimeZoneInformation	Modify	Read
HKLM\SYSTEM\CCS\Control\WMI\Security	None	None
HKLM\Hardware	**Read (via Everyone)**	**Read (via Everyone)**
HKLM\SAM	**Read (via Everyone)**	**Read (via Everyone)**
HKLM\Security	**None**	**None**
HKEY_USERS		

USERS\.DEFAULT	Read	Read
USERS\.DEFAULT\SW\MS\NetDDE	None	None
HKEY_CURRENT_CONFIG	= HKLM\System\CCS\HardwareProfiles\Current	
HKEY_CURRENT_USER	Full Control	Full Control
HKEY_CLASSES_ROOT	= HKLM\SW\Classes	

- HKLM = HKEY_LOCAL_MACHINE
- SW = Software
- MS = Microsoft
- CV = CurrentVersion
- CCS = CurrentControlSet
- W NT = Windows NT

Table 4.7. Default Access Control Settings for Registry (From Microsoft, 2000, "Default Access Control Settings in Windows 2000")

4.3 Compatibility Security Policy Template (compatws.inf)

The default security setting in Windows 2000 is much more secure than Windows NT 4.0, especially in terms of file and registry access permissions. Sometimes, but not always, additional security means a less than favorable trade-off of functionality. Windows File Protection System even stops administrators from installing system files. One may notice that when a system file is replaced, within a few minutes, the system is smart enough to detect the change, and restores the original file reversing the changes.

Windows NT, by default, grants Change permissions to most directories to Everyone group, and a large part of registry. Even though non-administrator was prohibited from performing some system and configuration tasks, it was able to install and run most applications.

In Windows 2000, by default, users only have full control to HKEY_CURRENT_USER registry key, and the %userprofile% directory. All other parts of the system is read-only to the non-privileged users.

Such restriction causes non-Windows 2000 compliant applications to fail. For example, when an application attempts to create temporary files in any other parts of the system, or needs to write to HKEY_LOCAL_MACHINE to store configuration changes.

On the other hand, when a Windows NT system is upgraded to Windows 2000, all the users in "Authorized Users" group are automatically assigned to "Power Users" group so that older windows NT application will function properly in the upgraded environment.

Power users are capable of performing many tasks that ordinary users are not required to do, and this violates the rule of least privilege.

Microsoft provided compatws.inf security template to address this problem. The security changes that this template makes is limited to granting additional access for "Users" group to make changes to certain registry keys and system directories. Figure 4.6 and 4.7 shows the rights assigned to the Users group by compatws.inf template. At the same time, through the Restricted Group settings, the application of this policy will empty the "Power Users" group to remove the extra rights that ordinary users may not need.

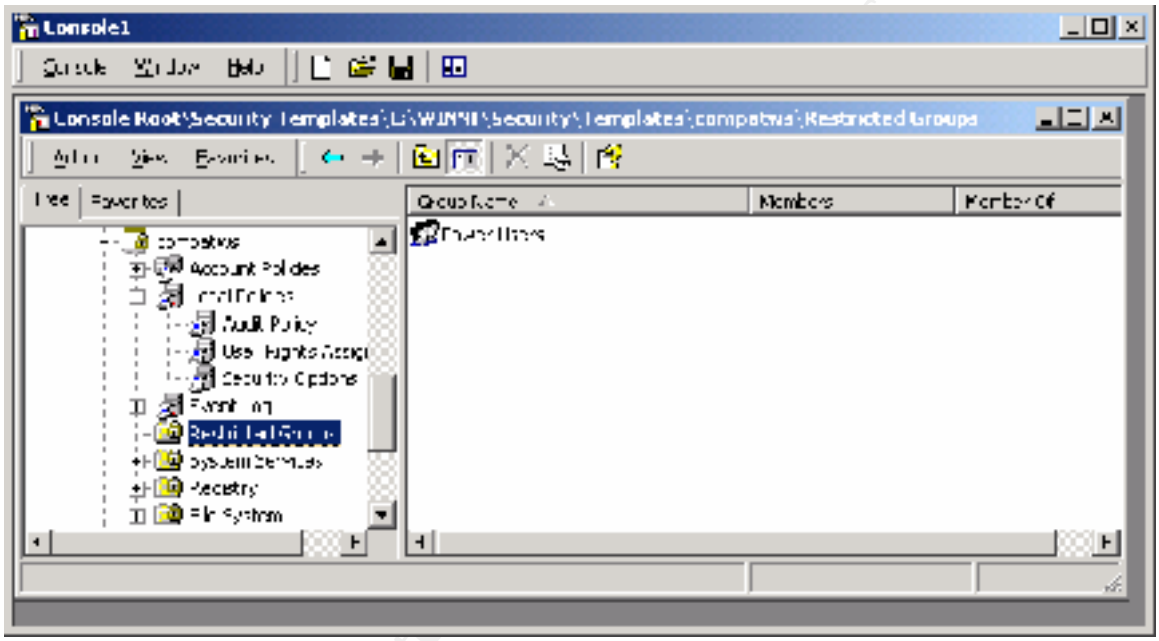

Figure 4.5. Restricted Group in Compatible Security Template

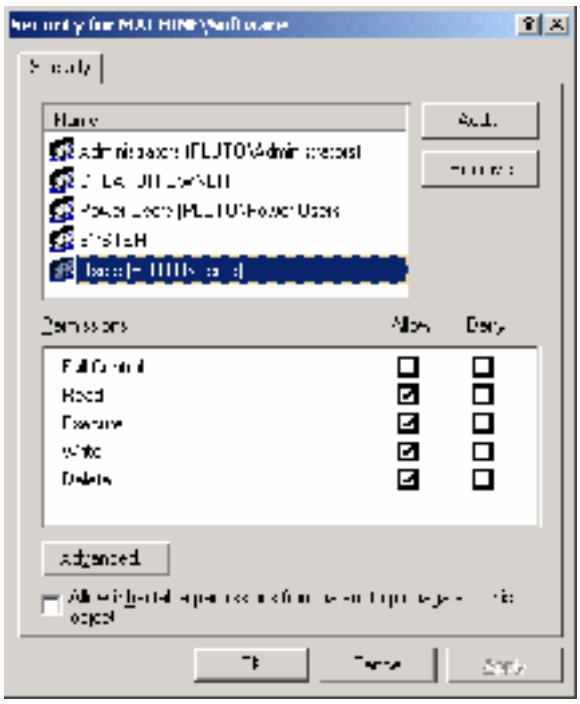

Figure 4.6. HKEY_LOCAL_MACHINE\SOFTWARE Permissions for “Users” group in compatws*.inf

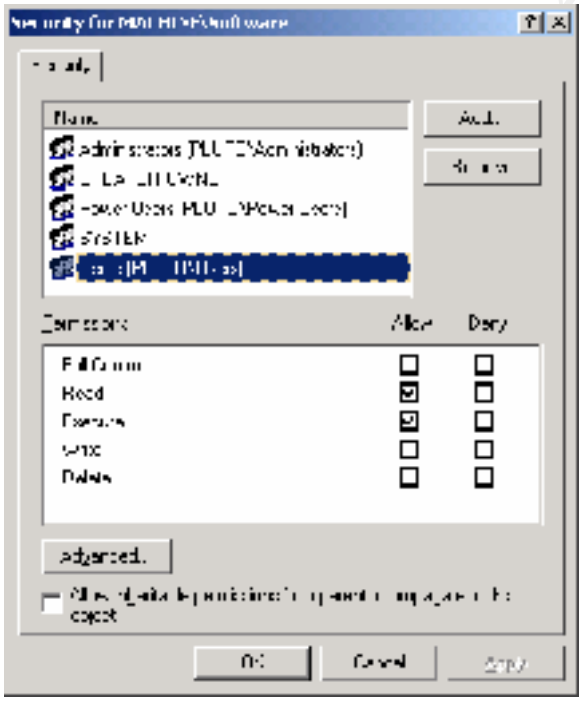

Figure 4.7. HKEY_LOCAL_MACHINE\SOFTWARE Permissions for “Users” group in compatws*.inf

V. Conclusion

The policy template are included with Windows 2000 installation to provide a good starting point, but rarely the administrators will be able to appropriately secure a system without customizing it. Basic level templates is recommended if security is not as critical as convenience, but account password policy may be configured more securely. Secure level template is recommended as a starting point if interoperability is essential as much as security is. When security is the foremost priority against the cost of upgrading to a native Windows 2000 environment with a processing power and storage, start from high security template.

There are some limitations to the use of security templates:

- The security template does not allow you to add new security attributes. Only modification of values for pre-defined attributes is possible.

- The use security template only applies to local policy, and it can be imported to more a group policy object that is defined for domains and organization units. When the security policy template is used to configure a windows 2000 system, the setting may not take effect because of the security policy at the domain and organizational unit level. However, the local security settings can be exported, and configured in Group Policy Object that can be applied to a domain or an OU.

Overall, the default security templates are provided as a starting point, but not a final solution. In most cases, they need to be customized and applied selectively depending on the goals of the use. There are several areas that require customization:

- Two main security categories not addressed, if not adequately, by the three levels of default templates are User Rights, System Services and Restricted Groups. Depending on the use situation, some user rights can be removed or added. Turning off some of the network services defined in basic configuration by defining and implementing System Services settings will increase the security and system performance at the same time. The system may not need all of the services to function properly, and the potential vulnerabilities decrease when services are disabled when they are not absolutely required for the system to function properly. Restricting the membership of some groups will prevent the organization from inadvertently adding a user to a privileged group by error.

- Finally, various customizable settings such as log-on messages are not even defined in highly secure template. Renaming of an Administrator account is also a security desirable practice that are not customized by default because of its nature.

VI. References

Jeffrey Brill, May, 2000, "Windows 2000 Template Security Implications."

Jason Fossen, 2000, SANS Security: Windows 2000 Course Books, Washington DC SANS Conference.

Robert Huie, December 2000, "Security Configuration Tool and Template Settings: Usefulness and Shortcomings of the Preconfigured Security Policy Templates that are included with Windows 2000."

Judi Kling, June 2000, "Using security templates to batten down the hatches", URL (http://www.elementkjournals.com/ewn/0006/ewn0061.htm).

Jon Loomes, "Default Security Settings in Windows 2000 May Cause Legacy Applications to Fail", URL (http://www.swynk.com/friends/loomes/win2kacl.asp).

Microsoft, 2000, "Default Access Control Settings in Windows 2000."

Microsoft Windows Knowledge Base Article Q234926 – "Windows 2000 Security Templates Are Incremental."

Thomas W Schinder, Debra Littlejohn Shinder, D. Lynn White, 2000, Configuring Windows 2000 Server Security (ISBN 1-928994-02-4).

Last Updated: February 24th, 2018

Upcoming Training

SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS Security West 2018	**San Diego, CA**	**May 11, 2018 - May 18, 2018**	**Live Event**
SANS Crystal City 2018	**Arlington, VA**	**Jun 18, 2018 - Jun 23, 2018**	**Live Event**
SANSFIRE 2018	**Washington, DC**	**Jul 14, 2018 - Jul 21, 2018**	**Live Event**
SANSFIRE 2018 - SEC505: Securing Windows and PowerShell Automation	**Washington, DC**	**Jul 16, 2018 - Jul 21, 2018**	**vLive**
SANS Boston Summer 2018	**Boston, MA**	**Aug 06, 2018 - Aug 11, 2018**	**Live Event**
SANS Amsterdam September 2018	**Amsterdam, Netherlands**	**Sep 03, 2018 - Sep 08, 2018**	**Live Event**
SANS Network Security 2018	**Las Vegas, NV**	**Sep 23, 2018 - Sep 28, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**