

The purpose of this paper is to introduce the features of Windows 2000 (SE) and explain how they address various current security issues.

Implemented as part of an approved company or departmental security policy, can help achieve BS7799/ISO17799 certification.

Registered Office
Amen Corner Business Park,
Cain Road,
Bracknell,
Berkshire,
RG12 1HN.

© 2004 Hewlett Packard Information Technologies Group, L.P. Product names mentioned herein may be trademarks or registered trademarks of their respective companies. All information contained in this brochure is subject to change without notice. Calls may be monitored or recorded for quality control purposes.
INTRODUCTION

HP and Microsoft’s Security Enhancements for Microsoft Windows 2000 - Windows 2000 (SE) - provides enhancements to Windows 2000 primarily in the areas of authentication, access control, Multiple Desktops and removable media auditing. These enhancements were designed originally to meet UK Government requirements, but apply equally in a commercial environment.

Implemented as part of an approved company or departmental security policy, Windows 2000 (SE) can help achieve BS7799 certification.

Windows 2000 (SE) fits with the highly desirable HP COTS (Commercial Off the Shelf) products philosophy, which is to provide off the shelf enhancements to standard Microsoft products.
FEATURES

Windows 2000 (SE) offers several features not available in a standard Windows 2000 environment. These include:

Ø Choice of Password Hashing Algorithms
Ø Password Generation
Ø Choice of Password Length
Ø Last Logon Information
Ø Multiple Logon Denial
Ø Dynamic Device Access Control
Ø CD Auditing
Ø Floppy Auditing
Ø Multiple Desktops

System managers can choose to install either the entire set of functions or any combination of them, depending on their specific requirements. They may, for example, choose to install Password Hashing but not Generation; alternatively other systems may require only CD and Floppy Device Access Control installed.

These enhancements are available as a commodity priced, Commercial Off The Shelf (COTS) product layered on, and enhancing, Microsoft Windows 2000 security. The enhancements were developed because CESG were concerned that Windows 2000 was not sufficiently secure for their needs. CESG are faced with a great demand for Windows 2000 in UK Government but extra security facilities are required to meet their stringent requirements.
PASSWORD HASHING

In Windows 2000, the Domain Controller stores passwords in encoded form, and as a logon takes place the password is hashed before it is passed over the network.

The problem with standard Windows 2000 is that the password hashing may be compromised, if the algorithm becomes known. There are various tools freely available on the Internet which could allow users to break into NT and Windows 2000 systems using:

Ø Password dumping
Ø Password sniffing
Ø Dictionary attacks
Ø Brute-force attacks

Password dumping involves copying all the user account details with password hashes from the machine under attack to a disk or tape. This requires physical, privileged access to the machine under attack and is a limited risk.

However, password sniffing is more of a risk. Sniffing a network involves reading the network packets as they pass along the wire and collecting the usernames and hashed passwords as they appear. Software is freely available which, when run on an ordinary PC with a network card, will capture network packets.

Once the usernames and hashed passwords have been collected by dumping or sniffing they can be “cracked” using dictionary or brute-force attacks off-line.

Hashing algorithms are by nature irreversible: the password is encoded into the hash but the hash cannot be decoded to the password. However, if there is sufficient computing power available and the hash algorithm is known it is possible to encode all possible passwords and check the hash result against the hash recovered until the correct password is found. This is a brute-force attack. A more subtle attack involves hashing dictionary words until the correct hash is found. Many passwords in common use can be found in a dictionary.

Windows 2000 (SE) provides replacement password hashing algorithms which are tightly integrated with the Windows 2000 operating system modifying both the NTLM and Kerberos security models. These algorithms are not published or widely known so there is a certain amount of "security by obscurity". The algorithms may also be seeded with up to 64 bits of information, allowing installations for different customers or projects to be unique.

Windows 2000 (SE) can optionally be configured to use password “Salting” whereby password hashing may also include a unique user salt value (the Windows 2000 username). The inclusion of this salt value will ensure that two users with the same passwords will have unique password hashes.

Algorithms are available which are approved by both UK Government and NATO, and recommended by SECAN. An equally strong commercial algorithm is also available for non-government organisations.

---

1To hash is to map the password to a numerical value by means of a process known as a hashing function; this function uses a mathematical algorithm.
**PASSWORD GENERATION**

Denying users the use of passwords that may appear in a dictionary and are therefore vulnerable to a “dictionary attack” provides additional protection against unauthorised access. Windows 2000 (SE) provides this protection through generated passwords.

The UK Government and NATO approved algorithms used to generate passwords in Windows 2000 (SE) produce variable 8 to 15 character passwords of the form CVCCVCCVCNN. This format is designed to produce pronounceable passwords which are generally more easily remembered than simple random letter combinations.

For commercial use, the FIPS-181 compliant Automated Password Generator (APG) can be used to generate random character, letter or word passwords.

The password change mechanism available at logon or through the Secure Attention Sequence (SAS) Dialog has been modified and integrated as a replacement GINA (Graphical Identification and Authentication DLL). A utility is supplied to allow administrators to generate passwords as required for setting up new accounts, resetting user passwords, etc.

**PASSWORD PREPROCESSING**

In a standard Windows 2000 environment, a user can access files and services anywhere on the domain simply by using the “connect as” option, and a username and password with the required access privileges.

In Windows 2000 (SE), the password entered at logon or when changing their password, is passed through an obfuscation process by the GINA. This modified form of the password is then hashed and used in the authentication process. The password known to the user is therefore different from the one stored by the system. The users password is only valid when used through the GINA and, if used elsewhere, will not be recognised.

**LAST LOGON INFORMATION**

Last Logon Information is the first line of detection of unauthorised access attempts. The system presents the user with the date, time and workstation of the last successful logon and unsuccessful attempt along with the number of failed logons, since last logon. If the user notices that this information does not match what they expect, they can alert the system administrator to a potential security breach. This is a feature common to most multi-user operating systems.

The user interface for the last logon information is integrated with the GINA and uses the “Discoverer Service”. The Discoverer Service is a central repository for the last logon data and also provides a central audit trail for successful and failed logon attempts. The Discoverer Service is installed on one or more servers throughout the domain. Each Windows 2000 (SE) workstation or server uses an entry in the Windows 2000 Active Directory to determine which Discoverer Service each user should record logon information to.

**MULTIPLE LOGON DENIAL**

If a user walks away from a logged on system and attempts to logon on again elsewhere in the domain, a warning is given that they are already logged on in the domain. Depending on whether multiple logons have been disabled, they will then be allowed or denied access.

---

2 C is a consonant and V is a vowel.
Workstations left unattended can be vulnerable to unauthorised access. An Autologout Meta Screensaver can be enforced to automatically log the user out after a predetermined duration of inactivity.

**Dynamic Device Access Control**

CD, Floppy and other devices can introduce viruses, Trojans, and other illicit software into an organisation presenting a potential security issue and enabling users to install and use unauthorised software, perhaps deviating from the “standard” desktop used within a department or organisation and thereby increasing support and maintenance costs.

In addition to this, a single Floppy or other removable device can carry or transmit huge amounts of sensitive or valuable information out of an organisation. To overcome this issue some customers have ordered PCs without these devices or even removed them from existing machines. This can cause major problems with PC maintenance as all software needs to be installed over the network and support staff are required to carry Floppy and CD drives around with them.

Windows 2000 (SE) controls access to devices by applying Access Control Lists (ACLs) on the devices. ACLs may be set on a device-by-device, user-by-user or group basis.

Devices that can be controlled include USB, PCMCIA, Infrared, Bluetooth, Modems, COM/LPT ports, IEEE 1394 Bus host controllers and other removable disk drives. Windows 2000 (SE) can be configured to allow or deny connection to unlisted devices.

By referencing domain groups in the ACLs, the administrators have centralised control over device access. All users who need access to each device can be added to the domain group of that device using the standard user-administration tools. The normal support staff and trusted users would be permanent members of these groups but individual users may be added to, or removed from, the group on a temporary basis.

The ACLs are applied to the devices and monitored by a service process installed on the Windows 2000 (SE) system.

**File Type Access Control**

In addition to controlling which devices can be used to transfer data to and from a workstation, Windows 2000 (SE) can restrict which file types can be transferred. Lists of permitted file types, identified by their extension, can be controlled for each user or group.

**CD Auditing**

It is increasingly common for users to need access to CDs for directories, manuals, etc. In these situations locking the device is not appropriate, instead an audit trail is required.

Windows 2000 (SE) allows auditing of CDs inserted into, and removed from, the CD drive. This feature uses the Windows 2000 Event log and records the CD label, user, date/time and whether the CD is being inserted into, or being removed from, the drive. Users can therefore be trusted to use the CD drive for legitimate purposes and an audit trail is available should the origin of programs or files need to be traced.

---

3 Supported devices include DVD/CD-ROM drives, floppy disk drives, IEEE 1394 Bus host controllers, infrared devices, modems, PCMCIA adapters, COM and LPT ports, tape drives, USB controllers and Windows CE USB devices.

4 Trojan horse programs are harmful programs disguised as games, utilities, or applications. They appear to do something useful while being simultaneously destructive.
Floppy Auditing
Some users will still need access to Floppy disks to import or export files. Again, simply locking the device is not appropriate, an audit trail is required.

Windows 2000 (SE) allows auditing of files copied to and from the Floppy drive. This feature uses the File Explorer (FEXPLORER) component of Windows 2000 (SE) and the Windows 2000 Event log to record the file names, destination directories, user and date/time. Users can therefore be trusted to use the Floppy drive for legitimate purposes with an audit trail available should it become necessary to trace an individual program or file.

An additional feature of FEXPLORER is that any user for which Floppy auditing is enabled is prevented from running programs directly from the Floppy disk – files can only be copied to, or from, the device.

Multiple Desktops
Windows 2000 (SE) combines the existing Windows Terminal Server facilities of Windows 2000 with a multi-role management tool, providing multiple role logons from a single workstation. Each logon has an associated desktop with facilities to switch desktops. This enables users to have concurrent multiple logons to domains, supporting multiple user roles and multiple security levels.

Multiple role security allows the security of a system to be much more tightly controlled. Multiple role accounts can be used by a single user and each of these role accounts could be granted different privileges, for example, administrative rights, access to a database, email access, etc. The users work can be compartmented onto different desktops, separating everyday work from administrative and privileged tasks.

Use of the clipboard can be restricted by controlling access to “cut and paste” operations. Windows 2000 (SE) allows separate permissions to be granted for pasting up and down through security layers.

This functionality is integrated into the replacement GINA and the option to switch desktops is available through a client management tool.

Additional administration facilities are provided to enable the system administrator to manage access by defining policies based on username and workstation, such that the same user may only be granted access to a restricted role from a workstation in a restricted area and not from a workstation in an unrestricted office.
IMPLEMENTATION AND USE
Minimum user impact has been achieved by making only minimal changes to the standard user interface. These changes have been tightly integrated with the Windows 2000 Operating System. The enhancements are made through the replacement of operating system files on both the server and workstation.

USER INTERFACE
Windows 2000 (SE) is designed to have a very low impact on end users; changes to the Windows 2000 Operating System and GUI are limited to:

Ø A revised logon screen, showing Windows 2000 (SE) version information
Ø A revised logon failure message, which gives no indication of whether the username or password is incorrect
Ø The optional display of last logon information
Ø A revised change password screen, with optional password generation
Ø The addition of a File Explorer component (FEXPLORER) to allow and audit access of Floppy drives by authorised users

CONFIGURATION
Each Windows 2000 (SE) implementation is unique; this is achieved using seed values for the password hashing algorithms when the installation is built.

The system administrator builds the installation kit once, tailoring it to suit the organisation’s specific security requirements. The installation kit generated by this process is then distributed and installed on all servers and workstations within the domain, thus ensuring that the same seed values have been used for each installation. If last login information is to be displayed the system administrator must also install the Discoverer Service on one or more servers in the domain.

The installation can optionally be configured to:

Ø Use generated passwords – Where password generation is selected, three forms are available and users are given the choice of three generated passwords when changing their password.
Ø Record login attempts and display last login information – If this option is selected the administrator must also install the Discoverer Service on at least one server in the domain.
Ø Restrict access to devices – The system administrator must provide the name of a user group. Only members of the named group will be allowed access to specified devices, such as CD and Floppy drives.
Ø Audit CD drive usage – If enabled, all CD drive access made by authorised CD users will be audited. (The audit log shows user, date and time, CD serial number and label).
Ø Audit Floppy drive usage – The system administrator must provide the name of a user group, all members of the group will only have access to the Floppy drive through the FEXPLORER utility, and all access will be audited. (The audit log shows username, date, time and names of files copied)
EXISTING NT(SE) AND WINDOWS 2000 (SE) ENVIRONMENTS

HP and Microsoft recognise the investment already made by customers in NT(SE). To protect this investment and to make the migration from a secure NT to a secure Windows 2000 environment less painful, the NT(SE) Windows 2000 (SE) Compatibility Update Kit is available.

Windows 2000 (SE) can participate in a Windows 2000 (SE) domain without the need for any modification or updates.

NT(SE) WINDOWS 2000 (SE) COMPATIBILITY UPDATE KIT

Windows 2000 (SE) and Windows 2000 (SE) use a different mechanism to communicate password information from that used in NT (SE).

The Compatibility Kit for NT (SE) enables the NT(SE) domain to recognise both the NT(SE) and Windows 2000 (SE) forms of these passwords.

The NT (SE) Windows 2000 (SE) Compatibility Update Kit is installed on all Domain Controllers in the existing NT(SE) domain, allowing Windows 2000 (SE) systems using the same algorithm and seed values to participate in the domain.
**Configuration Example**

The following example uses a fictitious scenario to illustrate how Windows 2000 (SE) can be used to meet different security requirements.

**ACME LTD**

The fictitious company, ACME Ltd has offices in several UK cities, each connected via WAN to the company network on a single domain. The company also has a large mobile workforce of consultants using laptops to dial-in to the Remote Access Service (RAS) on the company network from their homes, customer sites and hotels. All users, both office-based and mobile, run Windows 2000 and have access to both central and local services. In order to control maintenance and support costs the IT department had previously implemented several standard configurations which restricted the applications and resources available to specific groups of users. However, since implementation many users have installed non-standard software on their systems, requiring many to be re-installed with a standard configuration when the new software proved to be incompatible. There has also been an increase in downtime caused by the introduction of viruses onto the network from the unauthorised loading of Floppy Disks and CDs from unapproved sources.

The management of ACME Ltd are becoming increasingly concerned by the loss of productivity caused by unscheduled downtime and the IT departments rising support and maintenance costs; and following the loss and theft of several laptops, they are also concerned by the threat to the business should someone gain unauthorised access to the network. If confidential company material got into the hands of the press or a competitor, the company’s ability to compete could be severely affected. With this in mind, the management ask the IT department to recommend a solution which addresses these issues whilst having minimal impact on the users.

The IT department propose implementing Windows 2000 (SE) throughout the company. The increased security offered by the secure password hashing and the use of generated passwords will prevent a stolen laptop from being used to gain access to the network, and the ability to audit device access or deny it completely for groups of users will reduce the instances of unauthorised software and viruses being introduced onto the company network. They also recommend new procedures to allow those users with a genuine need for temporary access to a CD, Floppy disk or other device to request it providing they have appropriate authorisation and requiring all users to report any suspected unauthorised access.

Following management approval of the proposals, the IT department run the Windows 2000 (SE) installation, enabling password generation, last login information, device locking and auditing. The resulting site-specific Windows 2000 (SE) installation kit is then made available on a network share and copied to CD for distribution to mobile workers.

New user groups of CD user, Floppy user and Audit Floppy user are created with the few super-users who require unlimited access at these levels added to the relevant groups. Two further groups of Temp CD users and Temp Floppy users are also created and these groups are added to the CD users and Audit Floppy users groups respectively.

In order to roll out the Windows 2000 (SE) installation, all administrative and user passwords are changed to 6 lower case characters and password change is disabled, ensuring that users will still be able to login while the upgrades – which may take several days to roll out – are completed.

The site-specific Windows 2000 (SE) installation kit is then installed on each of the servers within the domain, followed by a rollout to each user, installing from the network share or CD. Once a user’s system has been upgraded, their account is again changed to enforce password change at next logon, forcing the user to choose a generated password from the list provided.
Any user needing temporary access to a removable disk logs a call with the IT Help Desk and provides the relevant approval from their manager. The IT Help Desk add the user to either Temp CD users or Temp Floppy users as required, and after logging on again they now have temporary access. Each evening, a housekeeping routine automatically removes all users from these two groups, removing the need to revoke temporary access for each user individually.

Once implemented, the incidence of viruses and the number of calls requiring re-installation of standard configurations reduced dramatically, with the CD and Floppy audit logs enabling the IT department to quickly trace the source of infected files and unauthorised software.
**FURTHER INFORMATION**

For further information please access the HP Secure Solutions Web site:

http://www.hp.com/hps/security/products/

**CONTACTS**

<table>
<thead>
<tr>
<th>Region</th>
<th>Name</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>Sarah Brennan</td>
<td>+44 (0)1925 841881</td>
</tr>
<tr>
<td>USA</td>
<td>Tom Norton</td>
<td>+1 (612) 326 2043</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>Simon Roller</td>
<td>+61 (3) 927 53400</td>
</tr>
</tbody>
</table>

or Email security.enhancements@hp.com