Windows 2000 Security Features

Windows 2000 introduces a number of new security technologies to the Windows platform, and provides a usable front-end for many that previously required extensive configuration, thus making them much easier to use.

By Justin Kapp
Risk Management Consultant

Windows 2000 has seen the introduction of many new technologies to the Windows platform, some in the area of security. Support has been added for better enterprise security as well as better security support for the standalone user.

Authentication

Windows 2000 sees the introduction of a new protocol for authentication between Windows 2000 machines on a Windows 2000-based network. This authentication protocol is the open standard protocol known as Kerberos (version 5).

Microsoft, however, has made an extension to the original Kerberos protocol to allow the initial authentication of users using public key certificates instead of the standard shared secret keys normally used by Kerberos version 5. The extensions in this manner now allow interactive logons to Windows 2000 using smart cards.

As well as Kerberos, Windows 2000 contains support for four other authentication systems: Windows NT LAN Manager (NTLM), Distributed Password Authentication (DPA), Extensible Authentication Protocol (EAP) and Secure Channel (SChannel). Windows 2000 uses NTLM to authenticate in Windows NT 4.0-based environments, whereas DPA, EAP and SChannel are all used to authenticate over dial-up networks or networks such as the Internet. By default, Windows 2000 will use Kerberos to authenticate with other Windows 2000-based servers, or when using resources within a Windows 2000-based networking environment. Windows 2000 will use NTLM when communicating with Windows NT 4.0-based servers or when operating within a Windows NT 4.0-based domain environment or machines which are running a previous Windows platform.

Windows 2000 will use DPA to authenticate on the Internet to allow the Windows 2000 user to use the same password with Internet-based resources that are part of the same membership organisation as the Windows 2000 user. DPA, however, is not supplied “out of the box”; with Windows 2000 it is an add-on product.

Finally, SChannel is designed to provide authentication, data integrity and secure communication over the Internet. SChannel includes four protocols:

- Secure Sockets Layer (SSL) version 2.
- Secure Sockets Layer (SSL) version 3.
- Private Communication Technology (PCT) version 1.
- Transport Layer Security (TLS) version 1.

Using these protocols, SChannel provides authentication using digital certificates.

Windows 2000 has seen the movement from proprietary mechanisms to more open standard mechanisms for authentication. This allows Windows 2000 to support a wider range of clients or access a wider range of environments. It also moves away from the proprietary mechanisms that in the past have proven to be a security weakness in the Windows platform.

Distributed Security

Windows 2000 has brought a new order to security services within the Windows platform in the guise of Windows 2000 Distributed Security Services. And Win-

dows 2000's support for multiple security protocols has seen a movement away from proprietary protocols, not only to Kerberos, but also to the new Active Directory service, which is based on the Lightweight Directory Access Protocol (LDAP), making it compatible with other directory services such as Novell's NDS.

Let's look at these security services that are distributed throughout the network and examine how they work together.

Active Directory Security

This includes the new concept of transitive trusts, which allows user account authentication to be distributed across an organisation. This also provides the granular assignment of access rights and the ability to delegate administration below the domain level.

Multiple Security Protocols

This includes the implementation of the security protocol Kerberos, the support of Public Key Infrastructure (PKI), and the use of NTLM for backwards compatibility with Windows NT 4.0-based networks.

Security Support Provider Interface (SSPI)

This component of the security subsystem provides an application with access to a wider range of security protocols using a generic interface for the authentication systems.

Secure Sockets Layer (SSL)

This standard protocol is used for secure communication between the user and Internet-based services.

Microsoft Certificate Services

This service was originally included as part of IIS 4.0 within the Windows NT 4.0 Option Pack. Certificate Services have been upgraded and made part of Windows 2000. It is used to issue and manage public key certificates for applications, and for secure communication over the Internet as well as within a organisation's intranet.

CryptoAPI (CAPI)

CryptoAPI is Microsoft's application programming interface, which allows the developer to access encryption services within the operating system. It also allows developers to provide their own encryption provider services with modules known as cryptographic service providers (CSPs).

Single Sign-On (SSO)

This is a key feature to Windows 2000 authentication. It allows the Windows 2000 user to log on just once to the domain using a single password and then authenticate to any computer within the domain.

Security Configuration Tool Set

Windows NT 4.0 saw, with the release of Service Pack 4, a new tool called the Security Configuration Manager. This tool is now part of the operating system and is accessed via the Microsoft Management Console (MMC). The Security Configuration Tool Set has four components: the Security Configuration And Analysis snap-in, the Security Settings Extension to Group Policy, the command-line tool secedit.exe, and the Security Templates snap-in.

The Security Configuration And Analysis snap-in is the tool used to create, test and apply machine security configurations. This tool creates a text file that contains settings that can be applied to a system to secure it. You can also use it to import templates and other security configurations to create scenarios and test them against the machines' current settings. It is then possible to apply the settings to the machine using the tool.

The Security Settings Extension to Group Policy is a tool that allows the administrator to export a security scenario into a format that can be imported into the Group Policy for an organisational unit of domain. The Group Policy editor and Local Policy editor are both shown in Figure 1.

Windows 2000 Security Templates

Features of the different template security levels are as follows:

Default

These are the basic*.inf templates. Use these to correct configuration. These default templates allow the administrator to roll back security to the original installation defaults.

Compatible

These are the compat*.inf templates. By default, all users are "power users" on Windows 2000 Professional. If you do not want your users to have power user rights, the compatible configuration alters the default permissions for the Users group so that legacy applications can run properly. Many applications required that a user had an elevated level of permissions in order to run properly. Note that this is not a secure environment.

Secure

These are the secure*.inf templates. The secure templates will increase the level of security for account policy, certain registry keys and auditing. Permissions for file system objects are not affected with this configuration.

continued...

The Security Templates are a series of pre-designed templates that can be used to secure a machine. These are split into two categories, Default and Incremental. The default templates are applied by the operating system when a clean installation has been performed. The incremental templates should be applied after a default template has been performed. The default templates are not applied if an upgrade installation is performed. There are four types of incremental template: Compatible, Secure, Highly Secure and Domain Controller (see box).

The Command Line tool is a Win32 console-based tool that allows the user to perform many of the tasks that can be achieved in the MMC snap-in. The reporting capabilities of this command line are a little limited. Although you can perform a security analysis you cannot view the results with this tool - instead you view them within the MMC snap-in.

Encrypting File System

Windows 2000 provided within the latest version of NTFS support for file and directory encryption built into the Windows 2000 environment. This feature is known as EFS, and employs both symmetric and asymmetric cryptography in an architecture that allows fast encryption using a DES variant known as DESX, in 40-bit, 56-bit and 128-bit modes of operation. International users of Windows 2000 will get 40-bit EFS and US customers will get 56-bit and 128-bit EFS.

A randomly-generated file encryption key (FEK) is used to encrypt data stored within the file system (eg, local NTFS files) using DESX. Then, using an asymmetric cryptosystem, the FEK is encrypted using the user's public key component. The user's private key component is used to decrypt the FEK so that it can be unlocked to decrypt the data. NTFS stores a list of encrypted FEKs with the encrypted file in special EFS attributes known as Data Decryption Fields (DDFs) and Data Recovery Fields (DRFs).

During the installation of a Windows 2000 domain controller a default recovery policy is implemented. This allows the recovery of encrypted files held within EFS by an administrator. This data recovery is made possible by the information stored in the DRFs stored with the FEK.

Public Key Infrastructure

Windows 2000 has seen the integration of infrastructure to provide PKI services to an organisation. This has been achieved by the integration of the Microsoft Certificate server. Microsoft Certificate Server has been around since Windows NT 4.0, and has provided the basic functionality of a Certificate Authority for requesting, issuing, publishing and managing certificates. Certificate Server offered Authenticode authentication and Secure MIME (S/MIME) integration for Exchange Server, but Microsoft geared Certificate Server mostly for public key-based client authentication for Microsoft Internet Information Server (IIS).

In Windows 2000, Certificate Server's name changes slightly to Certificate Services. Certificate Services is more powerful and better integrated into the rest of the operating system. The MMC snap-ins provides GUI tools for both the client side and the server side. Although Certificate Services can maintain its standalone data store, for full enterprise functionality Certificate Services uses Active Directory (AD) to store and publish certificates. Using AD, you can easily map certificates to users and leverage the management features of Group Policy Editor (GPE) to control for whom, by whom, and for what purposes Certificate Services issues certificates.

Smart Card Support

Smart card support has been added to Windows 2000 to provide support for Client Authentication and Smart Card Logon.

Client Authentication

Client authentication is the process of verifying a user's identity. Within Windows 2000 this is used for verification of secure communications channels such as Secure Socket Layer (SSL) and Transport Layer Security (TLS). The smart card is used to enhance the public key authentication and session key exchange process

Windows 2000 Security Templates (continued)

Highly Secure

These include the hisec*.inf templates. Highly Secure configurations add security to network communications. IPSec will be configured for these machines and will be required for communications. Down-level clients will not be able to communicate.

Domain Controller

These are the dedica*.inf templates. These templates optimise the security for users on a domain controller that do not run other applications.

for establishing the secure session. The user's private key is stored on the smart card and is only accessible to the holder of the card and the PIN. If the smart card is a "smart" smart card (known as an ICC Smart Card) the actual key exchange process can be carried out on the smart card.

Public-Key Interactive Logon

In the past, interactive logon with Windows has meant the user would enter credentials into a logon screen in the form of a username and password. With the public key interactive logon the process has changed significantly. With Windows 2000 the user has an x.509v3 certificate on the smart card along with their private key. Instead of entering a username and password, the user would put their smart card into a smart card reader then enter a user PIN; the user is then authenticated to the card.

Windows 2000 Certificate Services has support built in to perform smart card enrolment with the certificate template that is stored in the Active Directory. This will allow the user's smart card to be used for interactive logon and other services.

Network Security

Windows 2000 now contains support for the IPSec security architecture. IPSec allows you to secure TCP/IP packets at a network layer in a manner that is transparent to the user and also to the protocols that lie above the transport layer. The core of Windows 2000 IPSec implementation is Windows 2000's IP security policy, which consists mainly of a rule that controls how IPSec works in Windows 2000. This rule is a collection that consists of an IP filter list, filter action, authentication methods, tunnel setting, and a connection type. The following policy attributes are available:

Creating An IP Security Policy

Windows 2000 IPSec provides several pre-configured security policies. For example, the secure server policy always requests security and doesn't allow unsecured communication between clients that don't trust each other.

Deploying IP Security Policies

After you define IP security policies for your Windows 2000 network, you can set up the policies in AD, or you can use Windows 2000's IP Security Policy Management, an MMC snap-in, to set up policies in individual computers. To use a specific security policy that you define on a local computer you can manually configure the computer's IPSec option in the TCP/IP property.

Conclusion

Windows 2000 builds on Windows NT security in a number of ways. It provides a usable front-end for many technologies that before would require extensive configuration, thus making them better-placed to provide security services within an organisation. Some of these features come with a price: Windows 2000 does require more muscle to run, and initially the volume of features could lead to some weaknesses introduced by mis-configuration, so the rollout of Windows 2000 security should be performed with care.

Figure 1 - The Group Policy editor and Local Policy editor.

PCNA

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.