A020301

Security in Earlier Editions of IIS

Despite impressions to the contrary, IIS has always had a relatively high level of security infrastructure available, even if the way in which it has been installed with the base operating has left doors open that have later caused security breaches.

File/Folder Security

Since the introduction of Windows NT and the NTFS file system, the security of the files and folders that store information for your Web sites has been relatively high. The NTFS system provides extensive access control list (ACL) based security, enabling individual files and folders to be secured to a variety of levels to specific individuals and groups.

There have been few changes between the earlier versions of IIS and IIS 6 in this respect—NTFS is still the recommended file system for secure installations.

Authentication

Authentication is the system that protects files and folders by requiring a user to provide some form of identity to prove that he should have access to the file or folder in question.

IIS has always provided a number of different authentication systems that can validate a user against the local or domain-based databases.

The authentication systems provided by IIS are

- **Anonymous authentication**—Automatically logs a user in to the system using an anonymous or guest account. This is usually the default for an application-based site within the system—with the guest user having very low privileges on the system, thereby ensuring that the user cannot access other areas of the site or the machine unless the guest user account has been specifically granted the right.
- **Basic authentication**—Provides a simple login/password dialog box in which the user must enter his login information, which is then checked against the local or domain databases. The authentication is not encrypted unless you are using basic authentication in combination with an SSL enabled site—when obviously all data is encrypted.
- **Integrated Windows authentication**—Similar to basic authentication, this validates a user's credentials against the local or domain databases. But unlike basic authentication, it doesn't prompt the user for his information. Instead, it uses the credentials that were applied when the user logged in to his machine. This is particularly useful within an intranet, where you want users to gain access to specific areas of the site without having to enter their login/password combination again. The credentials are encrypted, irrespective of whether SSL is in use, but the system only works when the client is using Internet Explorer.
- **Digest authentication**—Provides a login/password dialog box, but unlike basic authentication, it encrypts the information as it is exchanged. The only requirement is that the IIS server must be a domain controller.

Host-based Security

Host-based security has been available since early versions of IIS and enables you to restrict access to a Web site or directory according to the IP address or domain name of the machine accessing that resource.

For example, within an intranet, you might want to restrict access so that only users from within your own network can access the Web site.

The system works in two ways—either all hosts are rejected apart from those listed, or all hosts are allowed except those listed.

Secure Sockets Layer (SSL)

SSL, a method for encrypting information between the client and the server when sending requests and responses, has existed since IIS 1. IIS 4 provided the next major functional update by supporting the 128-bit as well as the 40-bit standard for encryption keys.