Concern - *Security*

Is the security in Windows for Workgroups adequate for security critical situations? Some of our employees work with very sensitive data and if that data was accidentally made freely available from their hard disk over the network it would be a serious security breach. Also, how will Windows for Workgroups interact with the security features we already have in place on our servers?

Response

Windows for Workgroups is as secure as **any** other LAN client available. It complements, rather than replaces, your existing LAN security.

Windows for Workgroups respects all server-based security schemes just as the Windows operating system version 3.1 does today. As a result, sensitive, mission-critical data can continue to reside on a server and be protected on a user-by-user basis while less sensitive, more routine information, can be shared directly between the people that need to interact. This type of security architecture can actually free up both server space and the LAN administrator's time. For peer-to-peer sharing Windows for Workgroups provides an additional security model. When Windows for Workgroups users decide to share their resources (files, printers, etc.) on the network, they have the option of declaring the information to be *read-only* or *full access*, and can also decide whether or not to require a password for such access. Adding a password when users share information will help guard their data from unauthorized use.

Windows for Workgroups also makes security easy to use for the network users by automatically remembering the passwords to resources the user had previously connected to. The appropriate passwords for the resources are saved in encrypted files on the user's hard disk and are provided to the servers as needed. In this way, users don't have to type passwords every time they reconnect to shared resources. For example, suppose that each morning a user wants her PC to connect to five shared directories on five different LAN Manager and Windows for Workgroups servers and one network printer. In Windows for Workgroups, she does not have to type in the passwords for the shared resources every day to set up these connections. Windows for Workgroups automatically gives her access to all of the resources she had previously provided the passwords for after she has logged onto her Windows for Workgroups desktop. And because the passwords for these connections are stored in an encrypted file using the RC4 algorithm, there is little chance that someone could wrongfully obtain the password for a certain resource. In fact, there is usually a greater risk when passwords are not stored and encrypted on disk for the user. Why? Because when users have to reenter a password every time they try to connect to a shared resource, they often resort to writing down the password somewhere in their office space or saving it on their hard drives, unencrypted!

If needed, an individual Windows for Workgroups workstation can be quickly and easily prevented from sharing some or all resources by using one of several methods:

- Go to the Networks section of the Windows Control Panel and untoggle the "Enable Sharing" box. This will prevent the user from sharing anything on the Windows for Workgroups network but leaves sharing software on the hard drive.
- Edit the **system.ini** file and restart Windows for Workgroups. This prevents the user from sharing anything on the Windows for Workgroups network and will not allow toggling of the "Enable Sharing" box. The sharing software is left on the hard drive.
- Modify the **setup.src** file so that the **vserver.386** file is not installed on the machine This prevents the user from sharing anything on the Windows for Workgroups network and leaves no sharing software on the hard drive.
- Edit **winfile.ini** to just prevent file sharing while permitting printer sharing. This will remove all file sharing capability (buttons and drop down menus) in the File Manager.
- Edit **win.ini** to prevent printer sharing while permitting file sharing. This will remove all printer sharing capability (buttons and drop down menus) in the Print Manager.

You can of course modify the master copies of these files and have them installed on individual PCs in the organization automatically through the Windows for Workgroups **SETUP /N** command (explained later in more detail) or from a floppy-disk based installation.

This gives the network administrator control over his network and at the same time lets the users retain all of the other Windows for Workgroups features including access to shared resources on other machines, built-in electronic mail and scheduling, and

network DDE capability.