PASSFACES FOR WINDOWS APPLICATION NOTE #2

Passface for Windows – Components and Function

Real User's Passfaces™ for Windows (PfW) provides a strong authentication solution for users accessing Windows network domains from a desktop or laptop computer running many versions of Windows OS. This document describes the components that make up the system and outline how they work together to perform the required functions.

Components

The Passfaces for Windows system is made up of three major components:

Passfaces for Windows Client – this module resides on each individual desktop and laptop PC, and, in conjunction with the standard Microsoft Windows Graphical Identification and Authentication (GINA) module, provides the user interface for the entry of required information for authentication such as username, password, and Passfaces identification. It combines the password and Passface information into a composite passcode and submits it for validation to the standard Windows GINA module.

Like the standard Microsoft GINA module, it responds to, and is activated by, the secure attention signal (usually ctrl-alt-delete), and prompts the user for input. It is also the module that performs the Passface training and familiarization when users first begin to use Passfaces, or when users change Passfaces.

Passfaces for Windows Configuration Service – This Windows Service allows the Passfaces for Windows Client to access and update users' Passface configuration data stored within Active Directory. It need only be installed on domain controllers running Windows 2000 Server or Windows 2003 Server. (It is not required for domain controllers running Windows NT 4.0).

Passfaces for Windows Administration Tool – This tool allows the System Administrator, or designated individuals, to perform many of those functions necessary to administer the authentication tasks of the system. Specifically, it provides for the following common administrative tasks:

- Reviewing all user accounts and their current authentication settings
- Configuring an account to use Passfaces in addition to a password
- Determining how many Passfaces each user will use
- Resetting a user's password

The Administration Tool allows the administrator to configure users' Passface authentication settings on the Windows domain controller. Although the Administration tool can be run on any networked computer that the administrator might normally use to manage user accounts, it prompts the administrator to select the domain controller where the user accounts to be viewed/modified are located. In the case where no networked domain controller is in use, the Administration Tool can also be used to configure accounts on the local machine thereby enabling Passfaces for Windows to be demonstrated and tested on standalone computers, without a domain controller.

The Administration Tool only needs to be installed on networked computers used by the administrator to manage user accounts. It is expected that this tool will be used in conjunction with Windows' existing tools for managing users and groups.

Use of Domain Controller Data Store

The Passfaces for Windows software uses information about each network user stored in Active Directory on Windows 2000 domain controllers. By using an existing user attribute in Active Directory, and one that is present across all of the Microsoft "enterprise" operating systems, Passfaces for Windows takes advantage of the existing database and maintenance procedures, and avoids the need for any additional server software or user databases. The major advantage of this approach is that the users' Passface configuration data will be automatically maintained, managed, and replicated across domain controllers and backed up and restored with Windows' existing user database (or Active Directory).

Passfaces for Windows stores configuration information about each user (e.g., whether or not the user is using Passfaces, which Passfaces to present, etc) in a standard Windows attribute associated with each user account. The attribute used is the "user comment" field (LDAP name "comment"). This rarely used field is present as part of NT4.0's user account information and is an attribute of the Active Directory "User" object on Windows 2000 domain controllers (and later).

Similarly, no additional user secret data storage is required in the existing user database. Passfaces for Windows combines password data and Passfaces data into a character sequence that is stored using Windows' existing password storage and authentication mechanisms.

Function

The components described above work together as described below. A number of different scenarios will be described to help fully explain how all the components function.

Normal Use

The Passfaces for Windows login screen appears in place of the standard Microsoft GINA module, at the point of user logon. This could be at boot time, or in response to the secure attention signal. As with the GINA, the user is prompted to enter a username and password, and can select a domain to which to authenticate, or the user can authenticate to the local machine.

The Passface Configuration information then must be retrieved, either using the original WinNT method of getting the configuration (which will work if accessing a Win NT Server domain controller or a local machine NT/2000/XP account). If that fails an attempt to access the Passfaces for Windows Configuration Service on the domain is made. If that fails its own local cache stored in the local machine's registry is checked. The cached value is used only as a last resort because it might be out of date.

Once the configuration information is available, the user is presented with the Passfaces Identification screens, from which they will select their Passfaces. When all the faces have been selected, the numeric identifier of each face selected is mapped into a 4-bit value, and each 4-bit value is, in turn, appended to the password previously entered. This combination of password and Passface values is passed to the standard Microsoft GINA module for validation. The MS GINA will pass it through a one-way hash function and then request a challenge from the domain controller. It will then use the composite passcode hash value to encrypt the challenge and send the result back to the domain controller (so the actual composite passcode or its hash result never crosses the network.

Disconnected Use

In the case where the user has used this machine to authenticate to the network previously, and the network is not now available, as would be the case when the user packs up their laptop, unplugs the network cable and goes home, the authentication process can proceed as above, except in this case, the authentication is made against the encrypted composite passcode previously generated and cached on the machine (assuming this Windows feature has not been disabled). This allows the user to have the appearance of authenticating to the network domain controller, even though the domain controller is not accessible.

User Training

The user training is carried out by the Passfaces for Windows Client (GINA module) when the user executes the change password process. It first prompts for current password and/or Passfaces to verify the identity of the user. It then prompts for a new password, and then by accessing the Passfaces for Windows Configuration Service, the users' current alphabet (Passfaces plus decoys) of faces is determined (if one exists) and then the required number of faces, next in line, are assigned to the user. From those, the Passfaces are assigned at random and displayed to the user. The process of familiarization and training then take place until the user has successfully selected their Passfaces at least four times. The new encrypted composite passcode (combined password and Passfaces) is stored by the domain controller.

Administration Tool

As described previously, the Passfaces for Windows software, utilizes the data store of the domain controller for maintenance of all information about the users. When activated by the System Administrator, the Passfaces for Windows Administration Tool accesses the data store of the selected network domain and presents information about the users. Information such as User Name and Group are standard attributes. Information such as whether the user is using Passfaces, and how many, are retrieved from the Passface Configuration information stored in the user comment field (as described above).

An individual user, or groups of users, can be selected, and the detailed properties about those users will be displayed and available for maintenance. The standard features such as using the "Ctrl" and "Shift" keys to select multiple users work as expected in the tool. Any changes made will trigger updates to the domain controller's data store. [NOTE: The Passfaces for Windows Administration Tool is designed to maintain only that information directly related to the user's use of Passfaces. As such, it is not designed as a replacement for standard Microsoft tools that maintain other information, such as group membership, for domain users].

Conclusion

This document has attempted to explain in some level of detail how the Passfaces for Windows software performs the functions of user training, administration, and authentication. The three components that make up the system work in concert to deliver an easy to install, easy to manage strong authentication solution.

For more information about Passfaces for Windows please visit our web site at www.realuser.com. To speak with someone regarding your particular requirements, please contact Real User at (202) 331-2200.