BIOMETRIC USER AUTHENTICATION

Biometric user authentication techniques can be used to protect PCs and networks from unauthorized access by authenticating users based on a physical feature such as a fingerprint, retina, iris, hand, or face. Although voice and signature identification do not involve physical characteristics, they are usually included with biometric user authentication techniques.

For some of these biometric techniques, the cost of the equipment needed to identify a user is too high for widespread use. For example, the cameras and equipment needed for iris scanning can cost thousands of dollars. However, iris scanning is one of the most accurate biometric user authentication techniques, and it is expected to be used extensively in applications such as user identification for automatic teller machines (ATMs).

Some biometric techniques are unacceptable to many users. For example, some are uncomfortable with retinal scanning because it requires looking directly into an infrared light. Although retinal scanning has been used for some time in high-security employee verification applications, it is not likely to see widespread use for PC or network user authentication.

Voice and signature user authentication techniques are generally less secure and accurate than other biometric techniques; thus, they are not strong candidates for authenticating PC or network users. However, both techniques are attractive for specific applications. The main attraction for voice identification is telephone applications, where most of the necessary hardware is already in place. Signature authentication is used primarily for document authentication.

Hand, face, and fingerprint authentication techniques are all user-friendly and accurate enough for most PC user authentication purposes. Hand authentication is gaining some acceptance for physical access and attendance checking, but it requires bulky reader hardware, making it unsuitable for PC and network user authentication. Face identification requires camera equipment for user identification; thus, it is not likely to become popular until most PCs include cameras as standard equipment. This leaves fingerprint identification as the most viable and established biometric technique for verifying the identity of a PC or network user. And, in most cases, fingerprint authentication is the easiest and most economical biometric PC user authentication technique to implement.

Choosing a Biometric Authentication Solution

Before choosing a biometric user authentication solution, an organization should evaluate its needs carefully. The following list includes items that should be considered—the order of importance depends on the environment and level of security needed.

- Level of security required
- Accuracy
- Cost and implementation time
- User acceptance

Level of Security

Voice and signature recognition techniques are generally considered to be appropriate for many non-PC access authorization uses, but in most cases are not good candidates for PC and network user authentication. Biometric techniques that identify physical features are more accurate; therefore, they offer a higher level of security.


Accuracy

Retinal scanning and iris identification are both highly accurate ways of identifying individuals; however, they are both expensive to implement and most organizations do not need this level of accuracy. Hand, face, and fingerprint authentication techniques offer good accuracy for a smaller investment in scanning hardware.

Physical changes such as cuts, scars, and aging can affect the accuracy of certain types of biometric authentication techniques; however, user identification databases can be updated to overcome most of these problems.

Cost and Implementation Time

When implementing a biometric user authentication system, an organization should work with its PC vendor to evaluate the cost and time associated with the following factors:

- Researching, purchasing, and installing PC-compatible authentication hardware and software
  - Biometric capture hardware (readers, cameras, scanners, and so on) and associated software
  - Hardware and software to maintain the user information database
  - Time required to integrate the authentication hardware and software into the existing environment
- Training IT staff to manage the new system
- Training users in the new authentication protocol
- Collecting and maintaining a database of user identification data
- Updating the database as necessary

User Acceptance

Users generally find less intrusive biometric techniques, such as fingerprint, face, or hand identification, most acceptable. However, some users may be reluctant to have their fingerprints recorded in a database. An organization should provide its employees with information and training on the chosen biometric method, so they have a chance to become familiar with the requirements before the system is implemented.

Products

Vendors offer everything from basic biometric user authentication devices to complete systems, including a server to run the system. When planning an installation, an organization should work with its PC vendor to compare the products that best fit their criteria. Several vendor Web sites and articles that describe and/or evaluate various biometric user authentication products are listed at the end of this article.

The price of biometric user authentication systems varies from under $100 per PC, including all necessary hardware and software, to thousands of dollars for a complete, integrated solution for a large network of users. Most biometric products/systems surveyed for this article are designed for use with the Microsoft® Windows NT®, Windows® 2000, and Novell® NetWare® operating systems, and most support Windows 95 and Windows 98 clients. A few of the products surveyed are compatible with the UNIX® operating system, but they are generally a little more expensive than the Windows products. Some of the systems (for example, those that use the Identix Identicator technology) store fingerprint data directly in Windows NT’s Security Accounts Manager (SAM) database, making implementation relatively simple for IT managers.

Some of the simpler biometric systems offer a separate fingerprint scanner that connects to the parallel port on the PC and includes pass-through connections for the mouse and keyboard. Others integrate the fingerprint scanner into the keyboard, but still require connections to the parallel, keyboard, and mouse ports. USB provides a much simpler connection to the PC and frees the parallel port for other uses.
management scheme, especially the systems that store user identification data directly in the operating system’s security accounts database. Novell has given users a choice of authentication methods in its NetWare 5.0 and later releases by adding a menu of user authentication methods.

Some vendors offer more elaborate security solutions where many different authentication techniques can be implemented. As an example, BioNetrix Systems’ BioNetrix Authentication Suite for Windows NT supports a number of biometric user authentication techniques as well as voice identification, passwords, smart cards, and more. The BioNetrix product uses Microsoft’s Structured Query Language (SQL) server as the database back end to store user information.

**Conclusion**

For many organizations, implementing the right biometric user identification technique can improve data security and lead to significant cost savings by reducing help desk calls. Dell offers a number of user authentication solutions through Dellware™ and Gigabuys™. Contact your Dell™ sales representative for more information.

**For More Information**

The following Web sites provide more information on biometric user authentication:

- Dellware and Gigabuys: [www.dell.com](http://www.dell.com)
- The Biometric Consortium: [http://www.biometrics.org](http://www.biometrics.org)
- Voice ID Quarterly: [http://www.jmarkowitz.com/pubs.html#anchor_voice](http://www.jmarkowitz.com/pubs.html#anchor_voice)
- Biometric authentication products and systems:
  - [http://www.authentec.com](http://www.authentec.com)
  - [http://www.truetouch.com](http://www.truetouch.com)
  - [http://www.identix.com/itsecurity](http://www.identix.com/itsecurity)
  - [http://www.dba-sys.com](http://www.dba-sys.com)
  - [http://www.ultra-scan.com](http://www.ultra-scan.com)
  - [http://www.pito.org.uk/nafis/brochure/page3-i.html](http://www.pito.org.uk/nafis/brochure/page3-i.html)
  - [http://www.saflink.com/home.html](http://www.saflink.com/home.html)
  - [http://www.mytec.com](http://www.mytec.com)
  - [http://www.cadix.com](http://www.cadix.com)

Information in this document is subject to change without notice.

© 2000 Dell Computer Corporation. All rights reserved.

Trademarks used in this text: Dell and the Dell logo are trademarks and Dellware and Gigabuys are service marks of Dell Computer Corporation; Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation; Novell and NetWare are registered trademarks of Novell, Inc.; UNIX is a registered trademark of The Open Group in the United States and other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Computer Corporation disclaims any proprietary interest in trademarks and trade names other than its own.