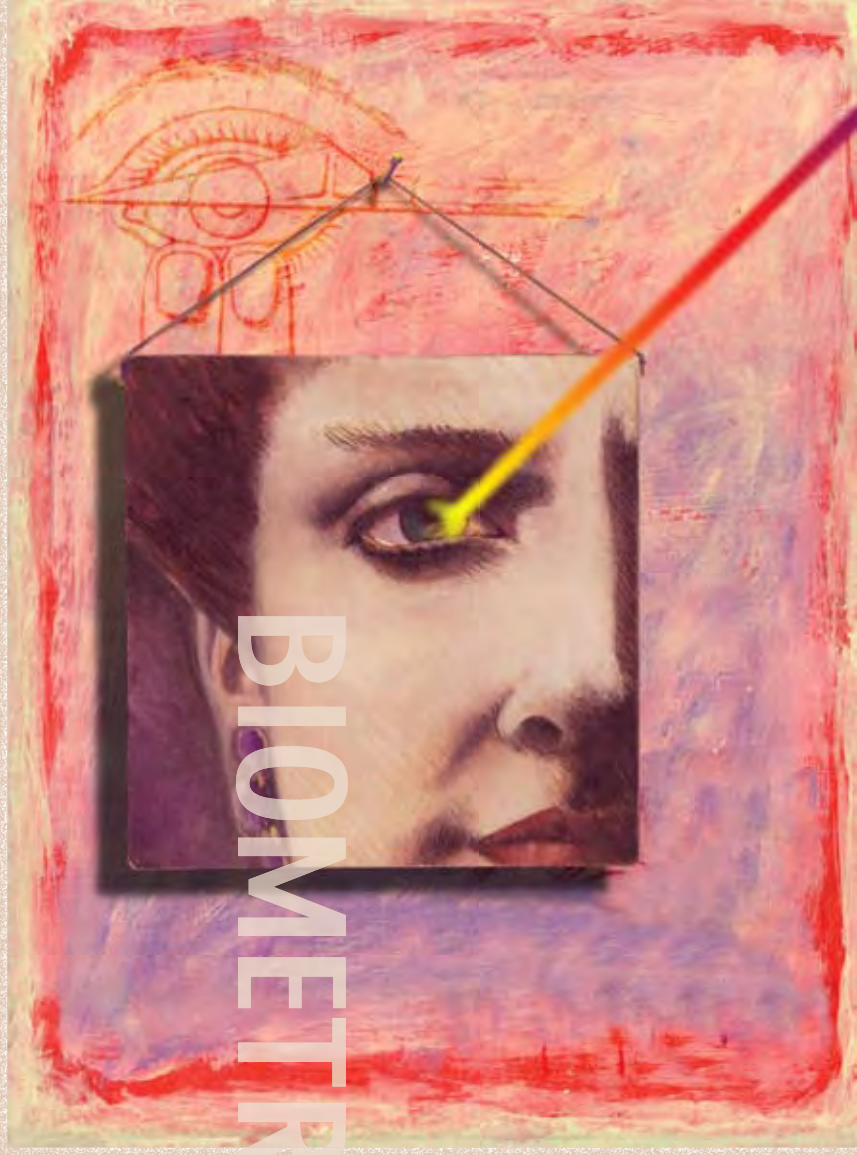
Biometrics security through middleware



By Shoieb Yunus

In today's world, businesses realize the equal importance of digital and physical security. Digital data and physical assets are lost – accidentally or deliberately. Biometrics can increase a company's ability to protect its data by implementing a more secure mechanism than a password. In this article, the author discusses device security needs and presents middleware tools to add fingerprint-based security.

A common problem with a password is that it can be compromised easily. Passwords are stolen, forgotten, and shared. Biometrics provides ways to protect data. Sales forecasts, business plans, new product ideas, customer lists, and other critical data can be protected using biometrics.

Biometrics is the only form of security that positively identifies and verifies an individual. Fingerprint, face, iris, and voice recognition technologies are used to determine an individual's identity and their corresponding access privileges. An unauthorized user can fraudulently swipe someone's card or use their password to gain entry into a building or computer, but cannot use their fingerprint or face.

For example, fingerprint readers for door access allow an authorized person's entry into the building. A standalone fingerprint reader enrolls and verifies an individual, but it does not address the issue completely. In a corporate environment, it is imperative to connect this device to the network server. A centralized system can monitor, manage, and verify entry and exit of employees, contractors, vendors, and visitors, even tracking employees' time, attendance, and desktop and network usage as well. In corporate environments, physical security must be tied to network security to be completely effective.

Mobile applications proliferating

Mobile phones are available with much more functionality than the ability to make a simple phone call. More Application Programming Interfaces (APIs) are available for imaging, multimedia, games, and enterprise access. In 2003, more than 84 million units of digital camera phones were sold. A myriad of mobile applications are in development, including video, imaging, document sharing, ERP, CRM, field service, e-mail, SMS, and other applications with access to potentially sensitive data. Some of the applications include secure logon to the device and network, secure access to voicemail, trusted mobile commerce, and many more. There is a stronger need than ever to make these applications secure via a single touch or swipe of a finger.

Various companies including AuthenTec, Fujitsu, and others manufacture high-performance, low-cost fingerprint swipe sensors, such as the AuthenTec EntrePad fingerprint scanner shown in Figure 1, for computers, mobile phones, PDAs, and other devices. However, gaps exist between sensors and mobile devices. A middleware solution could bridge the gap by providing *mobile-aware* software tools for application developers and service providers.

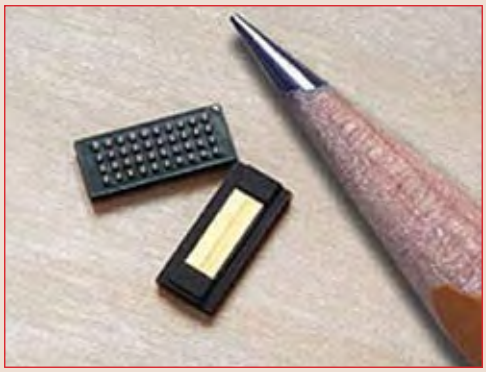


Figure 1

Goals for device security

A good device security system, including biometrics, should provide these functions:

- **Secure logon to devices** – Allow only an authorized user access to a personal computer or other device using biometric or non-biometric (such as smart card) authentication, and record and report on access attempts.
- **Protect application launch** – Allow only an authorized user to start productivity applications (such as accounting, financial, contact management, word processing, CAD, EDA software, databases, and Web browser), and secure those applications against unauthorized access.
- **Encrypt files and folders** – Secure sensitive data via *right clicking* on files/folders or using commands from the application console, and prevent unauthorized users from accessing critical data.
- **Manage password bank** – Securely store passwords for single sign-on to productivity applications and websites, replacing user names and passwords with a convenient, unique authentication.
- **Lock unattended screens** – Screen access (deactivation of *screen saver*) is secured by biometric or non-biometric authentication, protecting the device and data while a registered user is away.
- **Support multiple user authentication methods** – Various combinations of user name, password, biometric, and non-biometric authentication should be supported.
- **Simplify user interface** – Consumers should be able to use security through simple and attractive interfaces, reducing fear and making the technology easy to use without requiring technical knowledge.

EzPassport middleware toolkit

Almost all biometric sensor manufacturers provide a high-level interface or Software Development Kit (SDK), but there is no standard for the high-level functions provided for different sensors, so SDKs from different vendors force system changes if a sensor or data store changes. Also, these SDKs from sensor manufacturers usually cannot be customized easily, so integrators must often deal with a variety of programming tools and interfaces.

The EzPassport family of products is an open application framework, so system integrators or software developers can quickly and easily integrate biometric security features into any Microsoft Windows application. Since the EzPassport middleware is biometric-layer agnostic, it can be integrated with fingerprint, face recognition, iris, retina, voice, signature, and smart cards. It can also be married easily with biometric-enabled fingerprint readers for door entry and other applications.

EzPassport Toolkit, designed in C++, includes API, DLL, header files, and sample code for including EzPassport Plus functionality within any Windows-based software products.

EzPassport Plug-in is COM-based and supports a variety of applications without rebuilding when a new or changed component is used, and can be used very easily with .NET platform and a variety of programming languages such as Visual Basic (VB), C# as well as scripting languages such as JScripting, Java Scripting, or VB Scripting. Because the EzPassport Plug-in is built in Microsoft Visual C, it can also be used by C++ applications.

By using products from the EzPassport family, developers can implement a uniform set of high-level functions from lower-level primitives that understand specific components. For example, if only the functionality of the authentication engine or database engine is required, that component can be accessed by a low-level interface. Developers write applications to a high-level API, minimizing the application changes required when new biometric authentication devices are introduced. ECD

Shoieb Yunus *is founder and CEO of EzValidation, Inc., which provides secure, practical, and affordable solutions to the problem of proving positive identity on personal computers, mobile phones, and handheld devices. Prior to founding EzValidation, Shoieb was a marketing consultant at Veridicom, a leading fingerprint technology company, and business development and product marketing manager at Dazzle Multimedia (a subsidiary of SCM Microsystems). He has a BS in Computer Science from the University of Kentucky.*

To learn more, contact Shoieb at:

EzValidation, Inc.
830 Stewart Drive • Sunnyvale, CA 94086
Tel: 408-329-4360 • E-mail: shoieb@ezvalidation.com
Website: www.ezvalidation.com