



Biometric Authentication Comes of Age

Data Breaches Raise Awareness	1
The Case for Biometric Authentication	2
Why Passwords and Tokens Aren't Adequate	2
The Details of Fingerprint Matching	3
Factors Affecting Performance and Accuracy	3
How a Trusted Platform Module Strengthens Biometric Authentication	4
Big Benefits to Businesses	5
The Outlook	6
About Wave Systems	6

Data Breaches Raise Awareness

When a laptop belonging to an employee of the Veteran's Administration was stolen from his home, the private data of 26.5 million veterans was suddenly compromised. While the computer was subsequently recovered less than two months later, the incident had numerous negative repercussions, including an expensive investigation that ensued and a negative impact to the agency's reputation. Similar embarrassing data breaches have occurred recently at Citibank, H&R Block and Ameriprise Financial, among others. In fact, according to the Privacy Rights Clearinghouse, which has been tracking these incidents since early 2005, over 93 million data records of U.S. residents have been exposed as a result of data security breaches.

Such high-profile cases within corporate America and the U.S. government have exposed a glaring vulnerability within organizations: the difficulty keeping sensitive data secure on personal computers. This vulnerability has forced an increased demand for stronger user authentication—in other words, methods of verifying that a user is who he or she purports to be.

Most security-conscious organizations are implementing or investigating new authentication technologies. Many are demanding multi-factor authentication—where a password combined with something else, a token such as a smart card or USB device, is required for access to a network or PC. For portability and ease-of-use concerns, enterprises are also evaluating biometrics, the science of measuring and statistically analyzing a person's biological data as a means for user authentication.

November 2006
www.wave.com

The Case for Biometric Authentication

There are multiple types of biometric verification including fingerprint matching, iris scanning, retinal recognition, facial recognition, voice recognition and handwriting matches. Fingerprint-based identification is the oldest and most familiar of all biometric techniques, dating as far back as the ancient Assyrians and Chinese who used fingerprints to sign legal documents. Fingerprints have been used in law enforcement to identify criminals since the late 19th century.

Today, the science of fingerprint biometrics has evolved significantly. The cost of

The cost of reliable silicon sensors has dropped substantially and they are now available on a significant number of business-class laptops and PCs.

reliable silicon sensors has dropped substantially and they are now available on a significant number of business-class laptops and PCs. The number of Dell PCs equipped with fingerprint sensors slated for shipment in 2007 alone is projected to be in the millions. Robust, low-cost software is also now commercially available. This off-the-shelf software is capable of matching fingerprints with unparalleled accuracy.

This white paper focuses on the emergence of fingerprint biometrics as an economical and feasible form of strong authentication for businesses—large and small alike.

Why Passwords and Tokens Aren't Adequate

While usually effective as a first line of authentication, the primary drawback of both passwords and tokens (such as smart cards) is that each relies on either *something you know* or *something you have*. There is no way of verifying that the person presenting the token or typing the password is the one authorized to access a laptop or network. Using passwords and smart cards together provides a higher confidence level, but it is still not impervious to a hacker determined to acquire or spoof

both. Additionally, complex password rules and smart card maintenance dramatically increase the difficulty of use and cost of support.

On the other hand, a fingerprint serves to identify that the person authenticating is who he/she claims to be. Barring extreme measures, a biometric cannot be transferred from one person to another. It is easy to use and is the only form of authentication that verifies identity based on *something you are*.

The Details of Fingerprint Matching

Before an individual can be verified via his or her fingerprints, it is necessary to capture fingerprint samples using a process that is often referred to as enrollment. A chip called a sensor, either integrated into the PC itself or as a separate device, is used to capture the entire fingerprint image. Information from the image is stored by creating what is called a template. The template is not actually the image, but can be thought of as an “information extract” of the fingerprint image.

Biometric authentication is easy to use and is the only form of authentication that verifies identity based on something you are.

To create the template, the fingerprint image is processed by a special algorithm and the resulting data is entered into a database. The algorithm creates a digital representation of the fingerprint image. Each subsequent attempt to access the system requires the fingerprint of the user to be captured again and processed into a digital template. That template is then compared to those existing on the database to determine if there is a match. If a match is made, the user is granted access.

Factors Affecting Performance and Accuracy

Fingerprint readings can be affected by the nature of the finger itself: density, thickness of the print’s ridges, the skin’s wetness, the age and sex of the person, as well as the size of the fingers. Users can affect a system’s accuracy simply by how they pass their finger over the sensor. Too much rotation forces the system to compensate by closely evaluating the reference information. If the user rolls or moves his finger, it may not present the system with enough area of overlap with the enrolled templates. A lack of overlap

decreases the confidence of the attempted match.

Today, the technology behind capturing fingerprints has advanced significantly and these problems are minimized. Integrated sensor adjustments control image sharpness, brightness/contrast and are designed to offer excellent performance, security and accuracy. To further counteract problems that may occur, users typically enroll multiple fingerprints in case of difficulty with reading any individual finger.

How a Trusted Platform Module Strengthens Biometric Authentication

The Trusted Platform Module (TPM) is a small semiconductor chip located on the motherboard of a computer. The TPM chip performs specialized security functions for protecting data and for accessing sensitive data and networks. By the end of 2006, more than 60 million PCs with TPM chips are projected to ship from the leading global PC manufacturers. Two branches of the military—the U.S. Army and Air Force—formally require TPM chips on all new PCs.

As the deployment of business-class PCs equipped with TPM chips has grown, their role in assisting and securing biometric authentication has emerged. Because the TPM chip is separate from the CPU, it provides what is called the platform root of

trust. This means that, since it can be trusted, it is able to extend its trust to other parts of the platform by building a chain of trust, where each link extends its trust to the next one. This offers a verifiable way to link the trust of any component or event back to the root of trust – the TPM chip. Furthermore, certain cryptographic functions are executed within the TPM chip itself where external hardware and software agents cannot gain access.

TPM chips are used to encrypt and protect biometric templates. They also provide a second factor of authentication to the fingerprint without requiring an external token.

There are two common ways that TPM chips can be combined with biometric authentication. First, TPM chips can be used to encrypt and protect biometric templates. Second, they provide a second factor of authentication to the fingerprint – *something you have* – without requiring an external token.

Big Benefits to Businesses

Fingerprints help businesses prevent data loss and theft because of how difficult they are to duplicate. Protecting an organization's sensitive data in the event a laptop is lost or stolen is invaluable, but implementing biometric authentication can lead to other, less obvious benefits, such as helping firms comply with a litany of government regulations for data security or combating hackers' exploitation of password weaknesses. Preliminary findings suggest employees prefer using their fingerprints to authenticate to their machines over other methods. Passwords can be difficult to remember and tokens are easily lost. Furthermore, most corporations have seen that acceptance by users can either make or break the adoption of a new technology.

Today, businesses are using biometric technology in a variety of ways. When a fingerprint is required up front before the operating system loads, this is called "pre-boot authentication." Proper authentication before booting the operating system or accessing the hard drive is one of the strongest ways to protect data if a laptop is lost or stolen. Using biometrics for pre-boot authentication adds security, but keeps the process easy and convenient. Fingerprints can also be combined with passwords and used as two-factor authentication when accessing Windows, a VPN or the corporate network. Another

common business application is to require fingerprint authentication, in order to access sensitive documents or to log into secure applications.

With respect to administration, fingerprint authentication systems have made huge headway in recent years and are easy to deploy and maintain. Passwords and their hassles may even be eliminated entirely when the biometric validation is done at a central server. A server-based biometric implementation benefits network administrators by allowing them to enroll a user's fingerprints at a remote station. When fingerprint enrollment is done at a central location and the fingerprints are automatically distributed to the user's account across the network, the system administrator can verify the user's identity when he or she enrolls his or her fingerprint. In this scenario, users are also free to "roam" or, in other words, to log into different computers, all with a single fingerprint enrollment. To alleviate the fears that users may get "locked out" of their computers, administrators are able to specify a backup method of authentication in case of sensor failure, which is uncommon. Compared to other authentication methods that require complex administration systems, external tokens or expensive hardware, biometrics is emerging as one of the more cost-effective technologies in terms of both deployment and administration.

Biometric authentication systems prevent data loss and comply with government regulations.

The Outlook

Forrester Research has identified biometric authentication as one of the top ten identity management trends to watch in 2006 and predicts that it will go mainstream – extending beyond the market of early adopters. This prediction is coming true as sales of laptops with embedded biometric sensors have exceeded the expectations of major PC manufacturers.

Biometric sensors' lower cost and inclusion in PCs has caused fingerprint authentication to suddenly become affordable and convenient. Many corporate users enjoy the convenience and novelty of using their fingerprint and trends indicate that biometric authentication will gain widespread adoption in the near future as a form of strong authentication in the corporate environment.

About Wave Systems

Wave Systems solves the most critical security problems for enterprises and government with solutions that are trustworthy, reliable, easy-to-use and offer a speedy return on investment. Wave's trusted computing solutions include strong authentication, data protection, advanced password management and enterprise-wide trust management services.

Wave's network management products include:

- **EMBASSY® Authentication Server** provides centralized management, provisioning and enforcement of multifactor domain access policies. With EMBASSY Authentication Server, authentication policies can be based on TPM credentials, smartcard credentials, user passwords or fingerprints.
- **EMBASSY® Network Access Control** allows network administrators to easily deploy strong authentication policies on a corporate network integrating with standard Windows functions.
- **EMBASSY® Key Transfer Manager** is a key archive system that ensures recovery of TPM keys in the event of hardware failure or system transfer to a new user.
- **EMBASSY® Remote Administration Server** allows network administrators to remotely manage the security settings and administration of TPM-enabled PCs.

Copyright © 2007 Wave Systems Corp. All rights reserved. Wave "Juggler" and EMBASSY logo are registered trademarks of Wave Systems Corp. All other brands are the property of their respective owners. Distributed by Wave Systems Corp. Specifications are subject to change without notice.