White Paper

SECURED BioPass™

for Biometric Authentication

Contents

Introduction

In today's fast growing enterprises, protecting against information theft has become a major concern. The loss of valuable information can lead to a number of business and legal issues. In many cases, they lose their customers confidence due to lack of security policies and measures.

As a result, today's enterprises are increasingly concerned about securing access to enterprise IT resources. Apart from securing the network from unauthorized users and unauthorized network devices, more attention is being paid towards stringent identity enforcement mechanism to provide guaranteed privacy and confidentiality of information access.

The Password Problem

The most common way of controlling access to systems has always been using passwords. Each authorized user is allocated a user-id and an initial password. The users are expected to change their initial passwords the first time they login to the system.

As long as the user has one or two accounts or applications to manage, this approach is simple and easy to implement. But when the number of accounts become large, problems beings to surface. Users find it very difficult to remember all the user-ids and associated passwords of their various application accounts.

When burdened with remembering so many user-ids and passwords, some users make a list of their user-id's and passwords and store them into the system or some of them make sticky notes and paste them in and around their working area.

In addition, some users also share their account information with their family, friends and co-workers.

Some users use same passwords for different applications, some of them use names of their dear ones as their passwords thus making them easily vulnerable to hackers.

As a result, security of the system and hence the enterprise have to be compromised.

Need for Better Access Controls

Access control is the first and foremost security measure an enterprise must implement - it is the very first hurdle an intruder will face. Weak access control means that anyone with limited knowledge and experience can also gain access to valuable information.

The most common (user-id and password) way of implementing access control is easy to implement, but requires the user to take extreme care to safeguard this information. It also becomes cumbersome to manage on a large scale across many applications with many different user-ids and passwords.

In an effort to implement more strict rules on password-based access controls, most enterprises insist their users to keep changing their passwords at regular intervals of time. They also require passwords to be strong (combination of numbers, letters, and characters). These passwords end up being complicated. Users trying to adhere to such policies have a difficult time memorizing the passwords and typing them as well.

It is very common for the support teams in the enterprise to be extremely busy supporting their users with password resets and implementing stricter password policies.

Another approach to implementing access control has been the use of hardware tokens for authentication. Some problems with this approach are that people end up with many tokens, one for each account, so they are difficult to carry and manage. In addition, it is easy to lose hardware tokens and they can be expensive to manage.

The use of biometrics for access control can lessen many problems including the vulnerabilities, cost and inconveniences associated with the traditional password only or token based solutions.

The Biometrics Advantage

Biometrics enable the identification of a person based on his or her physical characteristics and/or behaviour. Common biometrics include fingerprint, voice pattern, retinal pattern and facial features. Among this large variety of biometric possibilities, the use of fingerprint for identification and verification dominates the market. There are many reasons for this including the low cost, high-reliability and fast-response of the fingerprint technology and systems.

The use of fingerprints for user authentication has been on the rise as people have discovered many problems with password and hardware token-based systems.

Fingerprint-based authentication provides a rather elegant solution to all of the problems associated with passwords and hardware tokens. Since fingerprint technology has become affordable and is reliable, its use in user authentication is rapidly increasing. It is much easier and faster for users to provide their fingerprint than to remember and type in their passwords or to carry tokens around.

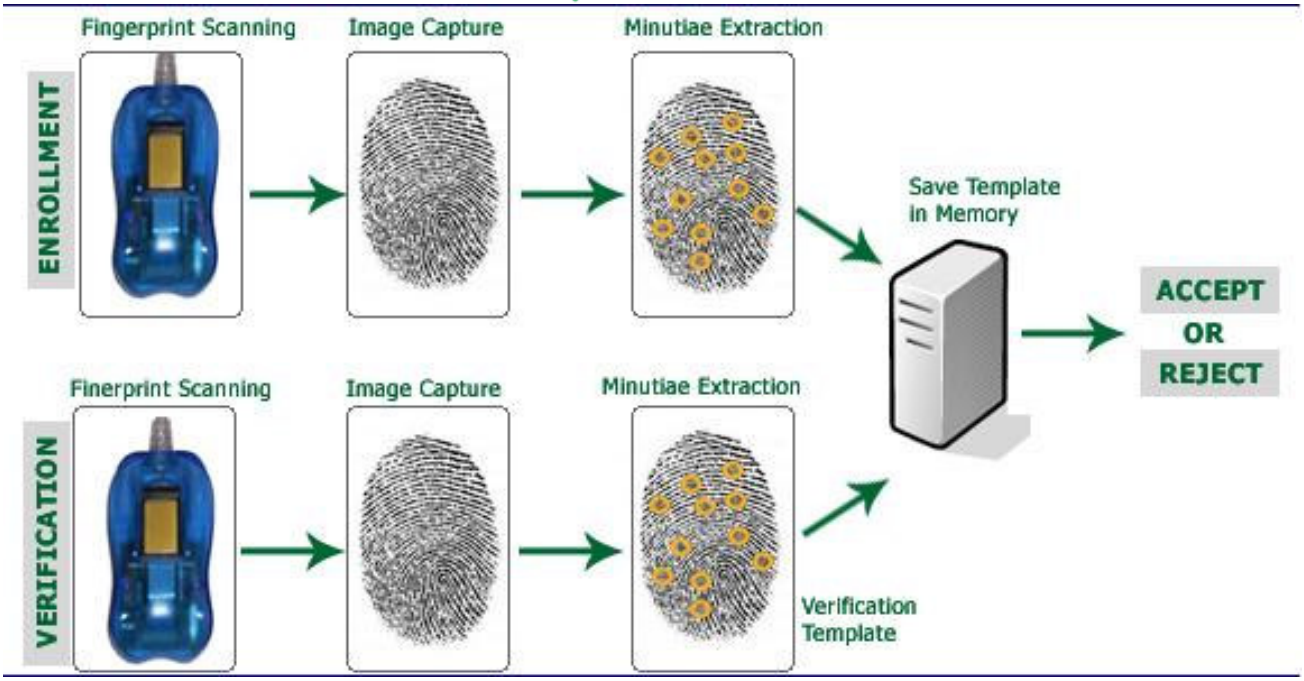
SECURED BioPass™ from SutiSoft does an elegant job of using fingerprints for logical access control.

SECURED BioPass™: Fingerprint based access control For the Enterprise

SECURED BioPass™ provides effective access control for individual systems by requiring registered users to authenticate themselves with their fingerprints rather than by passwords. By doing so, it addresses the vulnerabilities associated with password-based authentication by combining the biometric identity verification technologies and the best-in-class extraction/matching techniques. SECURED BioPass™ provides a rock solid access control mechanism for the enterprise IT infrastructure.

SECURED BioPass™ is a client-server solution for fingerprint-based authentication. Credentials of the users are stored in the SECURED BioPass™ Server.

In a SECURED BioPass™ enabled enterprise, when users want to login to their computers, they need to provide their user-id and fingerprints.



Each user's fingerprint is matched by the SECURED BioPass™ Server against his registered fingerprints stored in the SECURED BioPass™ Client. In case of a mismatch, the user is denied access to the system.

In case of a successful match, user login is permitted. From this point onwards, user experience is identical to their everyday experience with their normal application system.

SECURED BioPass™ provides local authentication i.e. user is authenticated for local access to the system. It prevents other users in the LAN to gain access to the system. It allows registration of fingerprint templates and their update to be done at the time of windows login.

The various features and benefits of SECURED BioPass™ include:

Robust Security

By using fingerprint-based access control, it eliminates the vulnerabilities associated with simple user-id/password type access controls. SECURED BioPass™ provides rock solid security access control to the enterprise IT infrastructure.

Best in class fingerprint algorithms

SECURED BioPass™ uses the best-in-class fingerprint algorithms developed by NEC. NIST (National Institute of Standards and Technology), in their evaluation of many fingerprint technologies, has clearly placed NEC as the leader (ELFT, 2009). As the fingerprint algorithms form the heart of any fingerprint-based authentication system, the quality of the algorithms is the most important factor.

Sensor Agnostic

SECURED BioPass™ is sensor agnostic and can work with a variety of fingerprint sensors available in the market. Within a single installation of SECURED BioPass™, several different types of sensors can be used. Fingerprint registration of a user can be done by one type of sensor and verification can be done by another.

AD Support

SECURED BioPass™ is designed to work in a plug and play manner. It can populate the database by extracting user information from the Active Directory and synchronize back when new users register or existing ones update their details / fingerprint templates.

Easy Migration to Fingerprint-based Authentication

SECURED BioPass™ allows the system administrator to manage the process of introducing fingerprint based access control easily and at pace that the enterprise can handle.

During the migration period, SECURED BioPass™ allows both fingerprint and password authentication to co-exist in the same network. It allows for a staged migration which enables the enterprise to continue its operations without disruption while existing users are being moved to the fingerprint system.

Your fingerprints are secure

SECURED BioPass™ does not store or transmit the image of the user fingerprints. It extracts salient points from the image, called minutiae points, and uses them for authentication purpose. While the minutiae can be extracted from a fingerprint image, one cannot take the minutiae and develop the original fingerprint image. This eliminates the chance of fingerprint image being lost, stolen or misused.

Fail Safe

SECURED BioPass™ provides secondary server support for authentication in case of primary server failure. Whenever there is a hardware failure in the primary server, authentication is automatically done from the secondary server in a completely seamless manner. The secondary server is a near full replica of the primary server.

SECURED BioPass™

The complete SECURED BioPass™ system consists of the following components:

- Login Client
- Admin Utility
- SECURED BioPass Server, and
- A number of value added tools

SECURED BioPass™ is installed on the user PC and is used by the user at the time of logging-in to the system. It captures the user-id, fingerprint and sends them to the SECURED BioPass™ Server for authentication. The same are verified against the registered templates.

Upon successful authentication, it passes the system control to the MS domain server for authorizations and further processing.

The main function of the SECURED BioPass™ Admin utility is to enable the system administrator to configure and manage the SECURED BioPass™ Server. New users are registered into the Server by using this utility. The system administrator can view the status of user registrations and all of the activity taking place on the Server.

The SECURED BioPass™ Server is the heart of the system. It stores user-id's and fingerprints of all the legitimate users. When new users are registered, their data is stored in the Server. The Server also maintains a log of all of the activity that takes place on it including user registration, deletion, and user authentications. For each transaction, it keeps track of the associated user-id, date and time of the transaction.

SECURED BioPass™ Client software replaces the existing Microsoft graphical user interface for login and puts its own interface in place of MS-GINA (a Microsoft Windows DLL that does the authentication function). It does the communication with the MS Domain server just as MS-GINA would do and does the required authentication.

SECURED BioPass™ is designed to support the most stringent reliability requirements of enterprises. To cover against any unforeseen failures with systems (hardware failure or software failure, SECURED BioPass™ provides secondary servers.

SECURED BioPass™ will automatically switch to a secondary sever whenever the system detects any problem with the primary server. The secondary server is a near-full replica of the primary server both in terms of data as well as functionality.

When a new user is registered, the details are automatically copied in the secondary server. In addition, both servers can provide full authentication services. This failover design ensures that the system can provide uninterrupted service even if one of the servers is temporarily out of action.

SECURED BioPass™ provides a number of useful utilities which enable the enterprise users to extract more value from their investment in fingerprint sensors and systems. The most useful utilities Simple Sign-On™ (SSO) and File/Folder Encryption/Decryption.

Simple Sign-On™ Utility

SSO enables users to register their user-id's and passwords used to access web-based services. Once these are registered, the user can logon to these services using their fingerprint, thus eliminating the need to remember user-ids and passwords.

In this scenario, when the web page or application pops up on the screen, SECURED BioPass™ client displays the fingerprint authentication screen.

Upon successful verification of the user-id and fingerprint with the server, it automatically populates the user-id and password fields of the web page or application. Then all the user has to do is to press enter to accept the user-id and password and continue with the log-in process.

Encryption / Decryption Utility

Encryption/Decryption utility, as the name suggests, enables the user to encrypt and decrypt files and folders by using their fingerprint as the key. This eliminates need for the user to remember long keys or passwords for encrypting files and folders.

Value Proposition

There are a number of convincing reasons for using SECURED BioPass™ in the enterprise which include cost savings, security, and time saving.

Security

Most importantly, SECURED BioPass ™ provides a rather robust level of security access to the enterprise IT resources. It helps enterprises meet the most stringent security compliance requirements which are becoming increasingly common due to regulations such as HIPPA and Sarbanes Oxley.

Fingerprint-based authentication insures that the user is who he/she claims to be as users cannot lend or share their fingerprints with anyone.

Time Saving

It is considerably faster to provide fingerprint for authentication than to type in passwords.

Generally passwords are required to be long and cryptic strings of alpha, numeric and special characters. For such passwords, not only is the time to type in long but users often have to retype them as errors are easily made in typing such passwords.

Sometimes, after a user attempts to log in 3 or more times unsuccessfully, the system rejects the user. The user in this case has to reset his account. This leads to wasted time and frustration for the users.

SECURED BioPass™ provides a much faster and convenient way to provide secure authentication information.

Summary

SECURED BioPass™ provides fingerprint based access control for the enterprise IT infrastructure. It addresses the vulnerabilities associated with password based authentication.

The architecture of SECURED BioPass™ makes it easy for the system administrators to introduce fingerprint-based access control in the enterprise without having to revamp the existing system. The migration to fingerprint based access control can be done over a period of time and at a pace which is convenient for the users.

SECURED BioPass™ uses the best-in class algorithm for fingerprint matching, resulting in unmatched performance and accuracy.

In addition, SECURED BioPass™ is fingerprint sensor agnostic. This enables users to use sensors that best match their needs. It allows a mix of different types of sensors to co-exist in the enterprise as well as users to switch sensors anytime they like.

References

ELFT (2009). An Evaluation of Automated Latent Fingerprint Identification

U.S. Office Address:
SutiSoft
4984 El Camino Real
Suite 200
Los Altos, CA 94022
(650) 969-SUTI (7884)
Fax: (650) 969-2783
info@sutisoft.com

Japan Office Address:
SutiSoft, Inc
Minato Bldg 4F
1-1-12 Minato, Chuo-ku
Tokyo 104-0043 Japan