DESIGN AND IMPLEMENTATION OF BIOMETRICS IN NETWORKS
S. Venkatesan¹, Sasikumar Gurumurthy²

HOW TO CITE THIS ARTICLE:

ABSTRACT: The traditional user verification technique does not provide proper security. But BIOMETRICS makes it possible to authenticate an individual’s identity based on one’s unique personal characteristics. So implementing biometric in computer networks is a challenging technique. In this paper, we have given a brief introduction to biometrics, their working and their role in computer networks. Traditionally, access to these networks involves the use of a network login ID associated with a password or personal identification number (PIN). Biometrics will change all of this. In this paper, we have a new semantic that uses existing password based systems, while eliminating user’s knowledge of their passwords for network security along with its function, working and setup. This semantic was later developed as a BioconX software in which the server uses one or more biometric database to map users’ physical characteristics and a SQL database as a repository for user and application information. Any SQL that supports an ODBC interface can be used for this purpose. Passwords stored in the database are encrypted. These techniques will span the entire information globe irrespective of the increased costs when compared to the level of security they offer.

KEYWORDS: Biometrics, pin, SQL, ODBC, BioconX.

INTRODUCTION: The biometric login process just described offers a significant improvement over the security of simple passwords and actually makes the user’s life easier, rather than imposing a new burden. Instead of manually typing user names and passwords, all users need to do is click a button and lay their thumb or finger over the scan window on the keyboard or mouse. The BIOCONX software uses one or more databases to compare our fingerprints or other characteristics. Since the fingerprint of everyone in this world is unique these can be used for strong authentication.[1]

The software processes fingerprint images by locating the minutiae points; that is, the points where fingerprint ridges terminate or bisect. With increasing in network vulnerability, the need for checking the users entering the networks is a major problem. These biometric technologies provide us a strong base solution for this problem. The method can be used in both government and private organization. We will show you the implementation of fingerprint authentication in electronic voting.[1] We have developed the application using C++. We are using the file system to store values which can be stored in a secure database in future. These applications with proper modification will definitely help the election commission of India to conduct elections in an honest manner. Currently we are working at implementing this software 100% practical, at least in a LAN. If all the hurdles are cleared, this technology is going to be a great boon in the field of security.

PREAMBLE TO BIOMETRICS: Authentication and security have been major issues right from the beginning of the computer age. The emerging and efficient technique for implementing security is BIOMETRICS. Biometrics makes it possible to authenticate an individual’s identity based on his or her
unique personal characteristics. Identification and authentication (I&A) is basic to security.\cite{8} In I & A, identification tells the system who the user is, while authentication provides some evidence that the user is really who he claim to be.

**Authentication is generally based on one or more of three factors:**

- What you know.
- What you have.
- What you are.

Traditional passwords are the obvious example of something ‘What you know’, and various kinds of hardware tokens implement an approach requiring something ‘What you have’. Biometric systems, such as a fingerprint or iris recognition, employ ‘What you are’.\cite{3}

**DRAWBACKS OF TRADITIONAL SYSTEMS:**

**Password Systems:**

- The passwords can be guessed, stolen, or cracked.
- In some environments, users deliberately share passwords for their own convenience. So passwords may not be secured in such cases.
- A system that uses only passwords to control access cannot authenticate whether the user identified with a password is really the authorized user.
- Passwords are also costly to administer. Password hassles account for a significant portion of help-desk costs.

**Hardware token Systems:** Hardware tokens implement a methodology based on something you have for identification. Requiring passwords or Pins to gain access to tokens often supplements this approach.

- Tokens depend on one or another cryptographic technique.
- Portability is both a strength and weakness of hardware tokens.
- Though tokens are of compact size and easily pocketed and carried from one system to another they may leave them behind or miss it.
- Hardware tokens are generally at greater risk of physical damage than is typical for most computer equipment.

**Biometric Involves:**

A person’s live biometric data is being matched against a bio print in the database, such as on a smart card. If it matches, it means that the person is who or she claims to be and access is granted. This process is called verification. Whereas in identification using Passwords the system only cares if the password is valid one and not cared about whether the user using the password is authorized to use it.\cite{3}
Biometrics for Network Security: One of the most obvious applications for biometrics is network security. Authentication is an essential component of network security.\cite{6} Authentication is inherently coupled with Identification and these two processes comprise the entire purpose of biometrics technology. Therefore, any network requiring users to identify and authenticate themselves is a prime candidate for biometrics. The prevalence and use of such networks in current society were already high and growing at an exponential rate. As growth continues, security concerns escalate along with it. Proponents of biometrics see this technology as the solution to these rising concerns about network vulnerability.\cite{3}

Governments and corporations maintain the majority of secure networks worldwide. Traditionally, access to these networks involves the use of a network login ID associated with a password or personal identification number (PIN). Biometrics will change all of this. Today there are commercial applications for computer access control, access to web site servers, access through firewalls, and physical access control to protect sensitive information.\cite{5} Governments are using biometric technology to provide robust authentication for access to computer systems containing sensitive information used by the military services, intelligence agencies, and other security-critical Federal organizations. As the technology advances and becomes more cost-effective, biometrics will eventually control identification and authentication for all internal networks.\cite{8}

There are also significant applications for biometrics in other commercial networks accessed by the general public.\cite{7} Some of the biggest potential applications include the use of biometrics for access to Automated Teller Machines (ATMs) or for use with credit or debit cards. Many types of financial transactions are also potential applications; e.g., banking by phone, banking by Internet, and buying and selling securities by telephone or by Internet. Fraud on cellular telephone systems has increased dramatically and is estimated by some sources at over $1 billion per year. Biometrics are being considered to reduce this fraud. Telephone credit card fraud is also a significant problem that may benefit from the use of biometrics.

Working of Biometric System:
Users whose biometric match one of the biometric templates of authorized users are automatically authenticated and logged on to the network. For a new user his biometric information's are enrolled and stored in the server.\textsuperscript{[2]}

Physical biometric and behavioral characteristics are the two classifications of biometrics. The physical biometric includes chemical composition of body odor, fingerprints, and features of eye, skin pores, and hand veins.

The behavioral characteristics include:

- Handwritten signature, Keystrokes(typing patterns), Voiceprint.

**An ideal biometric technology would generally include a system based on:**

- A unique biometric characteristic, Non-intrusive data collection, No or minimal contact between the person being scanned and the equipment doing the scanning, an automated system, i.e., no human decision maker in the decision loop, Very high accuracy, High speed.

**A good biometric system is fast, accurate, user-friendly and low-cost. In terms of operability, desirable biometric characteristics generally include:**

- Precision of the measurement(s), Speed (Throughput Rate), Public acceptability, Reliability, Resistance to counterfeiting, Acceptable storage requirements, Fast enrolment time.

**The potential benefits of an integrated biometric-based identification system include improvements in:** The cost of administration, the integrity of identification and information, access to information held by organizations, the speed of delivery and accuracy of services and Benefits, the level of technical security of communications.

**Conversion Challenge of Access Control:** An annual survey conducted by the Computer Security Institute and the FBI's Computer Intrusion Squad states that 85% of surveyed corporations and government agencies detected computer security breaches in 2004. The important thing is that this figure doesn't include even virus attacks. Thus the IT security must meet the challenge of strengthening user I&A to improve network security.\textsuperscript{[6]} However migrating an organization's passwords based application to an I&A scheme based on biometric is a tough challenge for developers because the applications has to be recorded to use an authentication API.\textsuperscript{[2]} This process is impossible in environments that are heterogeneous to begin with and that employs applications from third party vendors because it may not offer suitable hooks for implementing effective I&A.\textsuperscript{[7]}

**A New Semantic for User Verification in Networks:** This new semantic tackled the issue of conversion challenge by developing a biometric I & A system that does not require organizations to change a single line of source code. This technique accomplishes this by using existing password-based systems, while eliminating network users' knowledge of their passwords.

Instead of user's manually entering logon information, this software identifies the user based on a biometric scan. It uses either fingerprint or optical recognition as the biometric device. Our paper deals mainly with the fingerprint biometric technique which is the most commonly used. The biometric device automatically authenticates the user identity, then instantly provides the necessary logon information.
Users do not need to know the password for signing on to a network or application. Rather than serving as a mechanism for identification via something you know, the password becomes a secret shared only between the server and the network and applications.[2]

The syntax of the logon remains unchanged, but the semantics is completely different. A traditional password based method means: "User X has provided password Y." The new semantic means: "The software has scanned the fingerprint of the individual seated at the computer and has determined the person to be user X. User X's password for this specific network or applications for which he is authorized is Y/." This semantic was later developed as "BIOCONX" software.[1]

Internally, the software processes fingerprint images by locating the minutiae points; that is, the points where fingerprint ridges terminate or bisect. These ridges form regular designs, which are classified into pattern types. As shown in the figure the fingerprint pattern resembling a bulls-eye is called a whorl, while a triangular pattern is classified as an arch and the third type of pattern is called a loop. All fingerprints fall within these pattern types.

**Examples of Fingerprint Pattern Types:** There are lots of minutiae points—typically from 50 to 100 on a fingerprint. The challenge is that there is no way to simply look at a set of minutiae points and come up with an index in the database to match against. Fingers are positioned differently from one scan to the next, they may be applied to the sensor with different pressure, they may be drier on one occasion than on another, and the processing is rarely perfect. On a small scale, missing a few minutiae points or adding a couple isn't a problem because the number of minutiae present on a fingerprint is an order of magnitude greater than the number required to be confident of a match.[1]

However in large scale there will be a problem. The raised lines on a human fingertip are called friction ridges, or simply ridges.

**WORKING OF BIOCONX:**
BioconX Architecture:
As the figure illustrates the software consists of:

- A client component that runs on the user's system and is responsible for obtaining biometric information about users from a fingerprint scanner, Interactions with other systems and their applications, Interactions with the BioconX server.
- The BioconX server that maintains a database of users, applications, biometric data and comparison templates, and logon information.
- The Administrator that is used by security administrators to set up and manage user accounts, as well as configure applications for biometric login.

The client component runs on end-user workstations. Client components administer the initial network login via a GINA on Windows NT/2000 systems, or via a network provider on Windows 9x. During logon, a biometric scan is obtained from users. Scan data are forwarded to the BioconX server where they are matched against template records in the database. If a match is found, the software retrieves the user's logon and application information from the database. Back on the user's system, the user is logged on to the network. Applications configured to launch at start-up are launched, and logon information (Typically, the username and password) is provided for each application as necessary in the background without any user action.

The BioconX server uses one or more biometric database to map users' physical characteristics and a SQL database as a repository for user and application information. Any SQL that supports an ODBC interface can be used for this purpose. Passwords stored in the database are encrypted. Coherency among multiple servers is maintained by Microsoft Cluster Server. Because of the sensitivity of logon information, organizations deploying BioconX software often house the servers in physically secure locations.

Applications do not need to be launched and logged into at startup. BioconX provides biometrically authenticated login service, regardless of when an application is launched. BioconX constantly monitors the system for process initiation and window creation. When a new login window appears in an application that BioconX recognizes, BioconX prompts for a fingerprint and forwards the information to the server. The server matches the scan against its database and responds to the client with the logon information required by the application. If users have logged out of an application and want to log back in again, BioconX login services are invoked by clicking a tray icon, and selecting re-login from a pull-down menu.

The BioconX Administrator software is used to setup users and configure applications for biometric login. Like the user tool, the administration tool communicates with the server using an encrypted network connection. Each BioconX user requires a user account, created and administered by the administration tool. To facilitate managing a large population of users, the BioconX Administrator lets users with similar access rights and application requirements be aggregated into user groups. User setup is carried out using the BioconX Administrator. Biometric data are collected for each device users need to use, and the users' network logins and applications are configured.

The administrator automatically synchronizes BioconX user accounts with network operating systems and with Microsoft Exchange. Users can be created, deleted, or modified from within BioconX Administrator, and those changes are automatically propagated to the NT SAM database, Windows 2000 Active Directory, Novell, and Microsoft Exchange. Passwords can be set manually by the administrator or generated randomly. In the case of randomly generated passwords, even the
administrator never knows the password assigned to a user account. Similarly, user group memberships can be assigned or modified.

The BioconX Administrator also configures applications for biometric login. This is accomplished by creating templates that define all the information the client requires to recognize, launch, and login to each application. Each template includes a login script that defines the keystrokes required to navigate the application's login screen. The Administrator software lets applications be configured in one of two ways, either by using the Application Wizard or by configuring the application manually. The Application Wizard captures the required information by monitoring a controlled launch and login of an application. The captured information includes the application's executable file name, command-line switches, window titles, and keystrokes required to generate the application's login script.

The scripting language provides facilities for entering text, special characters, and control characters such as Tab, Delete, and Backspace. BioconX logs a user into an application by playing back the sequence of keystrokes defined in the script, while inserting logon information such as user name and password specific to individual users. The biometric login process just described offers a significant improvement over the security of simple passwords and actually makes the user's life easier, rather than imposing a new burden. Instead of manually typing user names and passwords, all users need do is click a button and lay their thumb or finger over the scan window on the keyboard or mouse.

For environments requiring even stronger user I&A, BioconX provides two-factor and three-factor authentication solutions. BioconX two-factor solutions marry something you have with something you are by supplementing the biometric authentication described earlier with challenge/response authentication using a cryptographic token. In challenge/response authentication, the cryptographic token is used to digitally sign a random challenge generated by the server. To authenticate users, the server verifies both the digital signature and biometric scan. BioconX three-factor authentication supplements two-factor authentication by adding a password to the mix.

SETTING UP: Setting up a BioconX-based security system is straightforward. For instance, the figure shows the main BioconX Administrator screen with the application configuration window for Outlook Express:

- Name specifies a unique name associated with the application.
- Description provides a brief explanation of the application.
- The five Path edit boxes specify possible paths from which the application can be launched. Multiple possibilities are permitted to support different hosts that use different paths to the same application.
- Caption identifies the caption associated with the login window. The BioconX client uses Caption and Path to identify the specific application being launched.
- Keys to Send specify the key sequence that the BioconX client sends to the application to login users. In this case, SH {TAB} {DELETE} tabs to the Outlook Express User Name edit box and clears its contents. UN, {TAB} inserts the user's application user name from the BioconX database at the current location, and tabs to the password edit box. PW, {TAB} inserts the password from the database and tabs to the Outlook Express logon OK button. The final {ENTER} sends a carriage return.
Pause After provides a way to insert a pause between launching an application and inserting logon information.

The BioconX client itself attaches no meaning to the keystrokes it sends to the application. In this example, {TAB} and SH, {TAB} are used to navigate around the window, but the interpretation of this virtual keyboard input is the responsibility of the application and may be different from one application to another. This gives the BioconX client the flexibility to login to mainframe and UNIX applications through terminal emulators, mainframe logins on a 3270 emulator, and standard Windows and web applications.[5]

BioconX Version 3.5 runs on Windows and is written primarily in Microsoft Visual C++, although some user-interface components are written in Visual Basic.

User and application profiles are typically kept in a Microsoft Access database co-hosted with the server, although any ODBC data source can be used. Because all database access takes place on the server, the usual performance issues associated with using an Access database in a network application are avoided. The server uses ODBC interfaces to access the database, so it doesn’t really know what database is actually being used. The scripting language is based on the Visual Basic Send Keys method with a couple of extensions. The script language uses a comma to separate individual Send Keys “chunks.” To send a comma, {,} is used. The strings UN and PW are used to specify the application user ID and password, respectively. The construct {OPL n} inserts a delay of n seconds.

IMPLEMENTATION OF BIOMETRICS IN E-VOTING: We implemented this biometrics concept in electronic voting system. We used C++ to develop our application. In that we have separate entry to enter voter list, candidate list and election commissioner. We used files to store all the biometrics value of the voters fingerprint, if want we can also use a secure database.[4] We will show you the live demonstration of our implementation and also how it works. During our presentation session the future works on this application will be explained clearly.

CONCLUSION: Biometrics offers a strong authentication alternative to traditional passwords and tokens, and can do so without imposing the burden and cost of application source-code modification. This is accomplished by converting existing password-based access control schemes to biometric I&A while maintaining the syntax of password-based logon. Where security requirements mandate even stronger authentication, biometrics can be used in combination with a token, or with a token and a password. Hence biometric techniques using BIOCONX will span the entire information globe irrespective of the increased costs when compared to the level of security they offer.[8]

REFERENCES:


8. L. Podio and Jeffrey S. Dunn, Biometric Authentication Technology: From the Movies to Your Desktop, National Institute of Standards and Technology (NIST), Information Technology Laboratory 2002.