STUDY ON BIOMETRICS AND NETWORK SECURITY

Maindro John Britto,
Lecturer,
Department of Computer Science,
National Institute of Public Administration University,
Zambia, Africa.

M. Devaraj,
Assistant Professor,
Department of Master of Computer Application,
The Kavery Engineering College,
Mecheri, Tamilnadu,India.

Abstract: Biometrics authenticates an individual's identity based on one's unique personal characteristics because the traditional user verification technique does not provide proper security. So that implementing biometric in computer networks is a challenging technique. In this paper, a brief introduction to biometrics, their working and their role in computer networks. In this paper, provide an overview of biometrics and discuss some of the salient research issues, modules, characteristics of that need to be addressed for making biometric technology an effective tool for providing information security.

Keywords: Network security, biometrics, authentication, fingerprint system, passwords

I. INTRODUCTION

Biometrics is a pattern recognition system that refers to the use of different physiological (face, fingerprints, etc.) and behavioral (voice, gait etc.) traits for identification and verification purposes. A biometrics-based personal authentication system has numerous advantages over traditional systems such as token-based (e.g., ID cards) or knowledge-based (e.g., password) but they are at the risk of attacks [1]. Biometrics, described as the science of recognizing an individual based on his or her physical or behavioral traits, is beginning to gain acceptance as a legitimate method for determining an individual's identity. The biometric login process provides 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. Biometrics method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons: the person to be identified is required to be physically present at the point-identification; these biometric technologies provide us a strong base solution for this problem. The method can be used in both government and private organization. Biometrics has several advantages compared with traditional recognition. Network security becomes a more important to personal computer users and the organizations [2]. With the advent of the internet, security becomes a major concern. Security is crucial to networks and applications. Network security [3] involves all activities that organizations, enterprises and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them. In this paper, the overview of biometric and network security discussed about the biometric system, BioconX architecture, network security aspects of biometric system, issues in biometric system and characteristics of biometric system.

II. BIOMETRIC SYSTEM

Biometric systems perform an automated pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic. Depending on the application context, a biometric system typically operates in one of two modes: verification or identification. **Verification mode:** The system validates a person's identity by comparing the captured biometric characteristic with the individual's biometric template, which is pre-stored in the system database. **Identification Mode:** The system recognizes an individual by searching the entire template database for a match. The system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database).

Operation of Biometric system

A biometric system may be viewed as a signal detection system with a pattern recognition architecture that senses a raw biometric signal, processes this signal to extract a salient set of features, compares these features against the feature sets residing in the database, and either validates a claimed identity or determines the identity associated with the signal. Biometric systems attempt to elicit repeatable and distinctive human presentations, and consist (in theory, if not in actual practice) of user-friendly, intuitive interfaces for guiding the user in presenting the necessary traits. In the context of biometric systems, sensing consists of a biometric sensor (e.g., fingerprint sensor or charge-coupled device (CCD), which scans the biometric characteristic of an individual to produce a digital representation of the characteristic. A quality check is generally performed to ensure that the acquired sample can be reliably processed by successive stages.

All the biometric systems have four basic modules which are sensor module, feature extractor module, matcher module and decision module [2]. These four modules are necessary in any biometric system to acquire and process raw biometric data and convert it into some useful information.

Sensor Module

In this type of module raw biometric data is captured by the sensor and it scans the biometric trait to convert it into digital form. After converting it to digital form, this module transmits the data to feature extraction module.

Feature Extraction Module:
It processes the raw data captured by sensor and generate a biometric template. It extracts the necessary features from the raw data which needs much attention because essential features must be extracted in an optimal way. It basically removes noise from the input sample and transmits the sample to input sample to the succeeding module known as matcher module.

Matcher Module
The resulting match score is transmitted to the decision module, which decides whether to accept the individual or not. This module compares the input sample with the templates being stored in the database using matching algorithm and produces match score.

Decision Module
After accepting the match score from matcher module, it compares the matching score against the predefined security threshold. This module accepts or rejects the individual on the basis of predefined security threshold. If match score is greater than predefined security threshold it will accept the individual otherwise reject it.

III. NETWORK SECURITY ASPECTS OF A BIOMETRIC SYSTEM

Two samples of the same biometric characteristic from the same person, For instance, two impressions of your right index finger—are not exactly the same due to imperfect imaging conditions (such as sensor noise and dry fingers), changes in the user's physiological or behavioral characteristics (such as cuts and bruises on the finger), ambient conditions (such as temperature and humidity), and the user's interaction with the sensor (such as finger placement). Therefore, a biometric matching system's response is typically a matching score s (usually a single number) that quantifies the similarity between the input and the database template representations.

BioconX Architecture:
BioconX provides biometrically authenticated login service, regardless of when an application is launched. To set up and manage user accounts, as well as configure applications for biometric login. BioconX constantly monitors the system for process initiation and window creation. The BioconX server maintains a database of users, applications, biometric data and comparison templates, and logon information.
The BioconX server utilizes one or more biometric database to map users' physical characteristics and a SQL database as a repository for user and application information. 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.
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.

Biometric System Issues

- The finger print of those people working in Chemical industries is often affected. Therefore these companies should not use the finger print mode of authentication. It is found that with age, the voice of a person differs. Also when the person has flu or throat infection the voice changes or if there is too much noise in the environment this method may not authenticate correctly. Therefore this method of verification is not workable all the time
- For people affected with diabetes, the eyes get affected resulting in differences.
- Biometrics is an expensive security solution.

IV. CHARACTERISTICS OF BIOMETRICS

The physical characteristics of a person like Fingerprint recognition, Hand geometry, face recognition, voice recognition, signature recognition and iris are called as biometrics. Each biometric trait has its strengths and weaknesses. The suitable biometric can be selected depending upon the application in various computer based security systems. The important features of the various biometrics are discussed briefly in this section.

1) Fingerprint recognition
Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. The finger prints of the identical twins are different. The fingerprint is scanned electronically and a reference template created accordingly. This template may be derived from either minutiae element, the pattern of the fingerprint, or simply the image of the fingerprint [5]. The inside surfaces of the hands and feet of all primates contain minute ridges of skin, with furrows between each ridge. This fingerprint recognition system is becoming affordable in a large number of applications like banking, Passport etc The purpose of this skin structure is to facilitate exudation of perspiration, enhance sense of touch, and provide a gripping surface. Fingerprints are part of an individual's phenotype and hence are only weakly determined by genetics. Fingerprints are distinctive to a person. This method is traditional and it gives accuracy for currently available Fingerprint Recognition Systems for authentication [6]. Facial recognition is very attractive from the user perspective and they may eventually become a primary biometric methodology.

2) Signature recognition
Signature recognition is a method of analyzing font, stroke order, stroke speed and pressure features to acquire identity authentication. At present, signature recognition is mainly applied to the credit card for transaction signature [7].

Because of serious disadvantages of much easy to be imitated, signature recognition is difficult to get the extensive application.

3) Hand Geometry

Hand geometry is concerned with measuring the physical characteristics of the users hand and fingers, from a three-dimensional perspective. One of the most established methodologies; it offers a good balance of performance characteristics and is relatively easy to use. Hand geometry readers are deployed in a wide range of scenarios, including time and attendance recording where they have proved extremely popular. Ease of integration into other systems and processes, coupled to ease of use makes hand geometry an obvious first step for many biometric projects [8].

4) Face recognition

Face recognition is a nonintrusive method, and facial images are probably the most common biometric characteristic used by humans to make personal recognition. An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints in a database Large volumes of fingerprints are collected and stored everyday in a wide range of applications including forensics, access control, and driver license registration. To reduce the search time and computational complexity, it is desirable to classify these fingerprints in an accurate and consistent manner so that the input fingerprint is required to be matched only with a subset of the fingerprints in the database. The applications of facial recognition range from a static, controlled "mugshot" authentication to a dynamic, uncontrolled face identification in a cluttered background. As this technique involves many facial elements; these systems have difficulty in matching face images [9]. The face recognition systems which are used currently impose a number of restrictions on how facial images are obtained. This face recognition system automatically detects the correct face image and is able to recognize the person. 1) The global analysis of the face image represents a weighted combination of a number of canonical faces or 2). The location and shape of facial attributes, like nose, eyes, eyebrows, lips, and chin and their spatial relationships.

5) Voice recognition

The voice recognition systems have been currently used in various applications. Voice is a combination of physical and behavioral biometrics with regard to everyday business transactions is considered. The features of person voice are based on the vocal tracts, mouth, nasal activities and lips movement that are used synthesis of sound. These physical characteristics of human speech are invariant for individuals. The behavioral part of the speech of person changes over time due to age, medical conditions, and emotional state. The speaker dependent voice recognition systems are text dependent; and the speaker independent systems are what he or she speaks [10]. Whilst there have been a number of voice verification products introduced to the market, many of them have suffered in practice due to the variability of both transducers and local acoustics. The speaker dependent voice recognition system is more difficult to design but provides more protection. The error rate for this type of technology ranges between two and five percent, however it lends itself well for voice verification over the public telephone system and is more secure than PINs [11].

6) Iris recognition

Iris scanning is the less intrusive of the eye related biometrics. It utilizes a conventional camera element and requires no intimate contact between user and reader. An iris recognition algorithm first has to identify the approximately concentric circular outer boundaries of the iris and the pupil in a photo of an eye. In also has the potential for higher than average template matching performance. The iris information can be collected by iris image. The accuracy of iris based recognition system is promising. Each iris is believed to be distinctive and even the irises of identical twins are also different [12]. The set of pixels covering only the iris is then transformed into a bit pattern that preserves the information that is essential for a statistically meaningful comparison between two iris images [13].

However, ease of use and system integration has not traditionally been strong points with the iris scanning devices. The iris is biological feature of a human. The iris is the annular region of the eye. The left and right irises of an individual can be treated as separate unique identifier. It is a unique structure of human which remains stable over a person lifetime. The iris recognition system has become more users friendly and cost effective. The iris have a very low false accept rate as compared to other biometrics like finger print, face, hand geometry and voice.

Drawbacks of 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 the authorized user.
- Passwords are also costly to administer. Password hassles account for a significant portion of help-desk costs.

V. CONCLUSION

Biometrics offers a strong authentication alternative to traditional passwords, and can do so without imposing the burden and cost of application source- code modification. Biometrics offers greater security and convenience than traditional methods of personal recognition. In some applications, biometrics can replace or supplement the existing technology. Where security requirements mandate even stronger authentication, biometrics can be used in combination with a token, or with a token and a password. Biometric systems are commonly used to control access to physical assets (laboratories, buildings, cash from ATMs, etc.) and logical information (personal computer accounts, secure electronic documents, etc.). In this paper, mainly concentrates on biometric and network security in an efficient way.

VI. REFERENCES

[1]. Tiwalade O. Majekodunmi, Francis E. Idachaba, "A Review of the Fingerprint, Speaker Recognition, Face Recognition and Iris Recognition Based Biometric Identification Technologies", proc. *World Congress On Engineering* 2011.

[2]. Prof. Dr. Tarik ZeyadIsmaeel,and Ahmed Saad Names, "Data Encryption Algorithm using Asymmetric Key Derived from Fingerprint Biometric Features",International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015.

[3]. Kaufman, C., Perlman, R., &Speciner, M. (2002). Network security: private communication in a public world. Prentice Hall Press.

[4]. Jain Anil K., Ross Arun and Salil Prabhakar, "An Introduction to Biometric Recognition", proc. *IEEE Transactions on circuits and systems for video technology*, 2004.

[5]. [5] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York: Springer Verlag, Jun. 2003.

[6]. A.K. Jain, L. Hong, R. Bolle, "On-line Fingerprint verification" , IEEE Trans. Pattern Anal. Mach. Intel. 1997.

[7]. X.L. Du, "An analysis of the characteristics and the future development direction of biological recognition technology", Technology & Application, 2014, 6, pp.75-79.

[8]. Hand and Finger Geometry System retrieved on 1 March 2014 from http://science.howstuffworks.com/biometrics.htm.

[9]. Mathew Kabatoff John Dougman, BioSocieties, "Pattern Recognition: Biometrics, Identity and State – An Interview with John Dougman", (2008), 3, 81, 86, © London School of Economics and Political Science, London UK.

[10]. Bill Swartz, Neeraj Magotra, "Feature Extraction for Automatic Speech Recognition ", 1997 IEEE Transaction.

[11]. Voice Verification System retrieved on 25 Feb 2014 from <http://www.emory.edu/BUSINESS/et/biometric/Voice.htm>

[12]. John Daugman, "How Iris Recognition Works", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004

[13]. Iris Recognition – Wikipedia, the free encyclopaedia [Online]. Available: http://en.wikipedia.org/wiki/Iris_recognition, (2010, August 10).

