Biometrics and Information Security

Deepthi Bala
Kennesaw GA USA
678.361.6623
dbala@students.kennesaw.edu

ABSTRACT

Today, everyone from fans of baseball games having their faces scanned and matched against a database of criminals to little kids at school using their thumbs to purchase their daily lunches, biometric technology is rapidly becoming a part of our everyday lives. With the advance in Information technology there has been an increase in threats to the system and its assets and therefore there has been a need to improve the security measures. The need for more and more reliable user authentication techniques has increased concerns about security and rapid advancements in networking, communication, and mobility in these days. Biometrics is one such authentication method which helps verify the users of the system. Biometric technologies are becoming the foundation of a highly secure identification and personal verification solutions. To ensure the integrity and confidentiality of its system it is necessary for every organization to have a good Security Policy. Security policy is an important factor to help secure the system, but by itself it will not help secure an information system [8].

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General-security and protection; K3.2 [**Computers and Education**]: Computer and Information Science Education

General Terms

Security

Keywords

Information Security, Biometrics

1. INTRODUCTION

Some of the key factors to ensure the security of the Information Systems of an organization are to have a good security Policy, proper Access Control Policy, a good SETA programs [10]. A good security Policy should define how the system should operate, who has access to it, moreover, what should be done in case of problems etc. [10].

Security, Education, Training and Awareness program (SETA) plays an important role for the proper functioning of the organization. It helps create awareness among the employees about the different type of threats, what should be done in case of an attack and how to reduce the vulnerabilities to the system.

Access Control Policy defines the access control or defining who can access, what type of resource and when. Access Control can be divided into 4 main groups Identification, Authorization, Authentication and Accountability.

There are three types of authentication: [10]

1) An authentication can be performed using memorized knowledge, like a pin or a password this is known as "something you know".
2) It can be done using some tangible and visible identification like a passport, driver's license, ID card, key or ATM card this is known as "something you have".
3) It can also be done comparing a persons features like fingerprints, signature, voice, iris, retina, DNA, hand geometry this is known as "something you are".

The last authentication method "something you are" is also known as Biometrics.

Biometrics is currently being used by banks, shops, corporate organizations, homeland security to identify criminals, airports etc.

This paper illustrates a brief understanding of the Origin of Biometrics, the different methods of Biometrics, how biometrics can be evaluated, Biometric Standards, the use of biometrics, and some of the Advantages and Disadvantages of using Biometrics.

2. BACKGROUND

In the case of Information security biometrics is used as a method of authentication to verify you are who you say you are before you can access the system. Biometrics is often used together with other user authentication methods rather than as a single, exclusive method to ensure the security of the information system. [10].

The use of biometrics could be traced back to as far as 31000 years ago when handprints were used by the prehistoric men as a signature for their paintings. Joao de Barros a 14th century Spanish explorer and writer described that the Chinese merchants used fingerprints for business transactions. In 1890, Alphonse Bertillion described a new system called 'Bertillonage', to identify convicted criminals and turned biometrics into a distinct field of study. He used different body measurement such as the size of the skull or the length of their fingers to identify individuals, this system faced some problems when it was discovered that some people shared the same measurements and therefore were convicted by mistake. By the late 1800s a new system was developed known as fingerprinting, this used fingerprint patterns and ridges to identify individuals, this characteristic was found to be unique for each individual and therefore more reliable in identification [2].

InfoSecCD Conference'08, September 26-27, 2008, Kennesaw, GA, USA. Copyright 2008 ACM 978-1-60558-333-4/00/0006…$5.00.

3. BIOMETRICS TODAY

Today, biometric systems are being widely developed and deployed to provide greater security to users and there is an increased awareness of the value of biometric systems. Biometrics has advanced a lot in the past few years. Some of the features that are used at present include face recognition, voice recognition, speech recognition, Retina scan, iris scan, signature identification, fingerprint etc.

Most users and develops of this have also recognized the need for a biometric standard. The standard establishes an appropriate biometric model and the associated security requirements that will allow different biometric solutions to co-exist in the marketplace. The standard views biometric systems within a global user community and it assures that the security of any one biometric system will be unaffected by the security of any other biometric system.

There are two ways Biometrics can be differentiated according to their functionality [9]:

1) Identification system

2) Verification system.

An Identification system identifies an individual by searching all the users in the database for a match. It tries to identify the person by asking “Who is this person?”

Verification tries to affirm or deny a person's claimed identity by asking, "Is this person whom he claims to be?" Verification is a one-to-one comparison of the biometric sample with the record held for the particular user.

Biometrics can be used for identification in two ways it can be identified based on unique physiological characteristics or behavioral characteristics. A physiological characteristic refers to inherited traits, namely traits that are formed in the embryonic stages of human development. Some of the physiological features measured include an individual's fingerprints, face, retina, iris and hand [1]. A Behavioral characteristic on the other hand refers to those characteristics that are based on the behavior of a person. Typical behavioral features that are currently used in the field of biometrics include voice patterns, handwriting and keystroke dynamics.

4. BIOMETRICS EMERGING TECHNOLOGIES

Like many security technologies, biometric devices today consist of a wide applicability. Several factors should be considered when implementing a biometrics system. We should consider the location, the number of users that will use the system; the value of the data that should be secured etc.Biometric devices may be adopted for use in a variety of settings in order to perform a wide variety of functions by different types of several different entities.

Some of the new technologies that are being researched in Biometrics include vein scan, facial thermography, DNA matching, fingernail bed identification, body odor, ear shape, gait, skin luminescence, brain wave pattern, Gait recognition ,footprint recognition and foot dynamics [2]. In order to have an enhanced security system it is necessary to have two or more Biometric technologies in one application this is known as a multimodal biometric system.

5. APPLICATION OF BIOMETRICS

More and more organizations are implementing Biometrics to keep their system secure. From securing the software to the network and even the country biometrics is being actively considered. After the September 11 attacks, the government has been trying to secure the country by improving the security measures. One such task is the implementation of Biometrics in airports. It requires that passengers exiting the United States to take a 10 finger scan to verify their identities [3]. This system is expected to be implemented by the end of 2008 or the beginning of 2009.

Many banks have implemented biometric systems to improve the security and protect their critical systems. Hitachi has implemented a vein based access control system at the New York branch of Japan's Shinkin Central Bank and Dutch bank ING has implemented fingerprint biometrics in their system [7].

Britain, Singapore, Brunei are some of the countries are now using Biometric technology for their passports [5]. The passports will include an electronic chip which contains the photograph and the fingerprint of the individual.

6. STANDARDS OF BIOMETRIC SYSTEMS

The two committees that work to establish the standards for Biometrics in the United States is the International Committee for Information Technology Standards (INCITS) and the International Organization for Standards (ISO) [9].

The November 2001 the INCITS established Technical Committee M1 (Biometrics) to help in the development and approval of national and international biometric standards.

M1 serves as the U.S. Technical Advisory Group (U.S. TAG) for the international organization ISO/IEC JTC 1/SC 37 on Biometrics.

The tasks of M1 include improving biometric standards for data interchange formats, iris interchange format, Biometric application interfaces (BioApi), Face Recognition, Data Interchange Format etc [1].

7. DISADVANTAGES OF BIOMETRICS

As with any technology Biometrics also has its advantages and disadvantages. Most individuals are apprehensive of accepting new technologies. An individual might feel that scanning and other methods for biometrics is intruding on their privacy and might not be willing to use it, for e.g. fingerprinting was associated with criminal for a long time and therefore having their fingerprint taken might make some people uncomfortable.

Some people feel that some of the techniques (the iris scan and retina scan) might be harmful due to the exposure to the light.

The data stored of each individual is permanent, unless the person has to undergo an amputation or the feature that is used for authentication is damaged in an accident.

Most of the biometric technologies are patented, which makes it expensive for companies to license the use and implementation of these techniques.

Using biometric readers on every door leading into a building or every PC on a network can be expensive. Hardware and software costs may not be the only consideration there is also the cost of training the employees to use the new technology [4].

Voice recognition is one biometric that most people find non invasive but this system may not be able to identify you if you have a cold.

8. ADVANTAGES OF BIOMETRICS

After the initial implementation and setup of the database Biometrics is an easy and convenient method to authenticate a user. Passwords can be forgotten or stolen, keys can be misplaced, and PIN numbers can be difficult to remember. Biometrics on the other hand can not be stolen or misplaced it is unique to every individual.

9. CONCLUSION

Problems of identity fraud are becoming common in all countries and increasingly governments are expected to be taking action to address these problems. Biometric security is an emerging as the most foolproof method of automated personal identification in today's highly computer dependent world. Biometric systems are automated methods of verifying or recognizing the identity of a living person on the basis of some physiological characteristics or some behavioral aspects.Biometrics has advanced in the past few decades with new technologies being developed; Vein scanning, iris scanning, facial thermography, gait recognition are just some of the new technologies being researched. As we have read earlier Biometrics has many disadvantages but many companies have implemented biometrics in a variety of areas, from network access control, to analyze staff access time and attendance, authenticating the user, for passports etc. To secure the Information System we should have good security policy, create awareness among the employees about the different threats to information security and also have multiple authentication system [10].

10. REFERENCES

[1] Bowman, E. Everything You Need to Know About Biometrics. (2000, January).http://www.biometrie-online.net/dossiers/generalites/AboutBio.pdf

[2] Chadwick, K., Good, J., Kerr, G., McGee, F., O'Mahony, F., Biometric Authentication for Network Access and Network Applications.

[3] Chan, W. D Biometrics enter DHS exit system. Federal Computer Week, 21(13), 46. (2007, May).

[4] Down, M. P & Sands, R. J Biometrics: An Overview of the Technology, Challenges and Control Considerations (2004).

[5] Farrell, N .British biometric passport hacked (2006, August).

[6] Ratha, N. K, Connell, J.H, Bolle, R.M. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal (2001).

[7] Savvas, A. Bank installs vein pattern access control. Computer Weekly (2007, March).

[8] Whitman, M. E., & Mattord, H. J., Principles of Information Security. Canada: Course Technology (2003).

[9] Whitman, M.E., & Mattord H. J. Readings and Cases in the Management of Information Security. Canada: Course Technology (2006).

[10] Whitman, M.E., & Mattord H. J. Management of Information Security. Canada: Course Technology (2008).