COMPARATIVE STUDY OF HUMAN IDENTIFICATION METHODS

Punita Arora*

Shalini Goel**

Sunil Kumar***

ABSTRACT

The purpose of this paper is to study about the various methods, which are mainly used in the authentication area. Information technology (IT) systems, their stored data and the processes are valuable resources, which need to be protected from outer world. First step toward securing an IT system is the ability to verify the identity of its users. The process of verifying a user's identity is typically referred to as user identification and authentication. Passwords are the methods that were used most often for authenticating computer users, but this approach has often proven inadequate in preventing unauthorized access to computer resources when used as the sole means of authentication. Because of above discussed problem, a new technique was emerged by researchers that can significantly improve the protection afforded by password-only authentication i.e. Biometrics Recognition.

Keywords: *Identification, Authentication, Biometric Recognition, Security, Passwords.*

*Faculty**,** Panipat Institute of Engineering & Technology, Panipat.

****Assistant Professor**,** Panipat Institute of Engineering & Technology, Panipat.

*****Assistant Professor, Panipat Institute of Engineering & Technology, Panipat.

1 INTRODUCTION

Determining if a user is authorized to use an IT system includes the distinct steps of identification and authentication [4]. Identification concerns the manner in which a user provides his unique identity to the IT system. The identity may be a name (e.g., first or last) or a number (e.g., account number). The identity must be unique so that the system can distinguish among different users. Depending on operational requirements, one "identity" may actually describe one individual, more than one individual, or one (or more) individual's only part of the time. For example, an identity could be "system security officer," which could denote any of several individuals, but only when those individuals are performing security officer duties and not using the system as an ordinary user. The identity should also be non-forgible so that one person cannot impersonate another. Additional characteristics, such as the role a user is assuming (for example, the role of database administrator), may also be specified along with an identity.

Authentication is the process of associating an individual with his unique identity, that is, the manner in which the individual establishes the validity of his claimed identity [6] [13]**.**

2 BASIC AUTHENTICATION METHODS

There are three basic authentication means by which an individual may authenticate his identity.

- Something an individual KNOWS (e.g., a password, Personal ID Number (PIN), the combination to a lock, a set of facts from a person's background).
- Something an individual POSSESSES (e.g., a token or card, a physical key to a lock).
- Something an individual IS (e.g., personal characteristics or "biometrics" such as a fingerprint or voice pattern).

These basic methods may be employed individually, but many user login systems employ various combinations of the basic authentication methods. An important distinction between identification and authentication is that identities are public whereas authentication information is kept secret and thus becomes the means by which an individual proves that he actually is who he claims to be. In addition, identification and authentication provides the basis for future access control.

.2.1 Passwords

The security of a password scheme is dependent upon the ability to keep passwords secret. Therefore, a discussion of increasing password security should begin with the task of choosing a password. A password should be chosen such that it is easy to remember, yet

difficult to guess. There are a few approaches to guessing passwords which we will discuss, along with methods of countering these attacks. Most operating systems, as well as large applications such as Database Management Systems, are shipped with administrative accounts that have preset passwords. Because these passwords are standard, outside attackers have used them to break into IT systems. It is a simple, but important, measure to change the passwords on administrative accounts as soon as an IT system is received.

A second approach to discovering passwords is to guess them, based on information about the individual who created the password. Using such information as the name of the individual, spouse, pet or street address or other information such as a birth date or birthplace can frequently yield an individual's password. Users should be cautioned against using information that is easily associated with them for a password.

There are several brute force attacks on passwords that involve either the use of an on-line dictionary or an exhaustive attempt at different character combinations.

2.2. Memory Card

There is a very wide variety of memory card systems with applications for user identification and authentication. Such systems authenticate a user's identity based on a unique card, i.e., something the user possesses, sometimes in conjunction with a PIN (Personal Identification Number), i.e., something a user knows. The use of a physical object or token, in this case a card, has prompted memory card systems to be referred to as token systems. Other examples of token systems are optical storage cards and integrated circuit (IC) keys. Memory cards store, but do not process, information.

Special reader/writer devices control the writing and reading of data to and from the cards. The most common type of memory card is a magnetic stripe card. These cards use a film of magnetic material, similar or identical to audio and computer magnetic tape and disk equipment, in which a thin strip, or stripe, of magnetic material affixed to the surface of a card. A magnetic stripe card is inexpensive, easy to produce and has a high storage capacity. The most common forms of a memory card are the telephone calling card, credit card, and ATM card. The number on a telephone calling card serves as both identification and authentication for the user of a long distance carrier and so must remain secret. The card can be used directly in phones that read cards or the number may be entered manually in a touch tone phone or verbally to an operator. Possession of the card or knowledge of the number is sufficient to authenticate the user. Possession of a credit card, specifically the card holder's name, card number and expiration date, is sufficient for both identification and authentication

for purchases made over the telephone. The inclusion of a signature and occasionally a photograph provide additional security when the card is used for purchases made in person.

The ATM card employs a more sophisticated use of a memory card, involving not only something the user possesses, namely the card, but also something the user knows, viz. the PIN. A lost or stolen card is not sufficient to gain access; the PIN is required as well. This paradigm of use seems best suited to IT authentication applications.

While there are some sophisticated technical attacks that can be made against memory cards, they can provide a marked increase in security over password only systems. It is important that users be cautioned against writing their PIN on the card itself or there will be no increase in security over a simple password system.

2.3 Smart Card

A smart card is a device typically the size and shape of a credit card and contains one or more integrated chips that perform the functions of a computer with a microprocessor, memory, and input/output. Smart cards may be used to provide increased functionality as well as an increased level of security over memory cards when used for identification and authentication. A smart card can process, as well as store, data through its microprocessor therefore, the smart card itself (as opposed to the reader/writer device), can control access to the information stored on the card. This can be especially useful for applications such as user authentication in which security of the information must be maintained. The smart card can actually perform the password or PIN comparisons inside the card.

As an authentication method, the smart card is something the user possesses.

With recent advances, a password or PIN (something a user knows) can be added for additional security and a fingerprint or photo (something the user is) for even further security. As contrasted with memory cards, an important and useful feature of a smart card is that it can be manufactured to ensure the security of its own memory, thus reducing the risk of lost or stolen cards. The smart card can replace conventional password security with something better, a PIN, which is verified by the card versus the computer system, which may not have as sophisticated a means for user identification and authentication. The card can be programmed to limit the number of login attempts as well as ask biographic questions, or make a biometric check to ensure that only the smart card's owner can use it. In addition, non-repeating challenges can be used to foil a scenario in which an attacker tries to login using a password or PIN he observed from a previous login. In addition, the complexities of smart card manufacturing make forgery of the card's contents virtually impossible.

The proper management and administration of smart cards will be a more difficult task than with typical password administration. It is extremely important that responsibilities and procedures for smart card administration be carefully implemented. Smart card issuance can be easily achieved in a distributed fashion, which is well suited to a large organizational environment. However, just as with password systems, care should be taken to implement consistent procedures across all involved systems.

2.4 Hand Held Password Generators

Hand-held password generators are a state-of-the-art type of smart token. They provide a hybrid authentication, using both something a user possesses (i.e., the device itself) and something a user knows (e.g., a 4 to 8 digit PIN). The device is the size of a shirt-pocket calculator, and does not require a special reader/writer device. One of the main forms of password generators is a challenge-response calculator. When using a challenge-response calculator, a user first types his user name into the IT system. The system then presents a random challenge, for example, in the form of a 7-digit number. The user is required to type his PIN into the calculator and then enter the challenge generated by the IT system into the calculator. The generator then provides a corresponding response, which he then types into the IT system. If the response is valid, the login is permitted and the user is granted access to the system.

When a password generator is used for access to a computer system in place of the traditional user name and password combination, an extra level of security is gained. With the challenge response calculator, each user is given a device that has been uniquely keyed; he cannot use someone else's device for access. The host system must have a process or a processor to generate a challenge response pair for each login attempt, based on the initially supplied user name. Each challenge is different, so observing a successful challenge-response exchange gives no information for a subsequent login. Of course, with this system the user must memorize a PIN. The hand-held password generator can be a low-cost addition to security, but the process is slightly complicated for the user. He must type two separate entries into the calculator, and then correctly read the response and type it into the computer. This process increases the chance for making a mistake.

Overall, this technology can be a useful addition to security, but users may find some inconvenience. Management, if they decide to use this approach, will have to establish a plan for integrating the technology into their IT systems. There will also be the administrative challenge for keying and issuing the cards, and keeping the user database up-to-date.

2.5 Biometrics

Biometric authentication systems employ unique physical characteristics (or attributes) of an individual person in order to authenticate the person's identity. Physical attributes employed in biometric authentication systems include fingerprints, hand geometry, hand -written signatures, retina patterns and voice patterns. Biometric authentication systems based upon these physical attributes have been developed for computer login applications. Biometric authentication systems generally operate in the following manner:

Prior to any authentication attempts, a user is "enrolled" by creating a reference profile (or template) based on the desired physical attribute. The reference profile is usually based on the combination of several measurements. The resulting template is associated with the identity of the user and stored for later use. When attempting to authenticate them, the user enters his login name or, alternatively, the user may provide a card/token containing identification information. The user's physical attribute is then measured. The previously stored reference profile of the physical attribute is then compared with the measured profile of the attribute taken from the user. The result of the comparison is then used to either accept or reject the user.

Biometric systems can provide an increased level of security for IT systems, but the technologies are still less mature than memory or smart cards. Imperfections in biometric authentication devices arise from technical difficulties in measuring and profiling physical attributes as well as from the somewhat variable nature of physical attributes. Many physical attributes change depending on various conditions. For example, a person's speech pattern may change under stressful conditions or when suffering from a sore throat or cold. Biometric systems are typically used in conjunction with other authentication means in environments requiring high security.

2.6 Cryptography

Cryptography also supports authentication through its widespread use in other authentication systems. For example, password systems often employ cryptography to encrypt stored password files, card/token system often employ cryptography to protect sensitive stored information, and hand-held password generators often employ cryptography to generate random, dynamic passwords. Cryptography is frequently used in distributed applications to convey identification and authentication information from one system to another over a network. Cryptographic authentication systems authenticate a user based on the knowledge or possession of a cryptographic key. Cryptographic authentication systems can be based on either private key cryptosystems or public key cryptosystems. Private Key cryptosystems use

the same key for the functions of both encryption and decryption. Cryptographic authentication systems based upon private key cryptosystems rely upon a shared key between the user attempting access and the authentication system. Public key cryptosystems separate the functions of encryption and decryption, typically using a separate key to control each function. Cryptographic authentication systems based upon public key cryptosystems rely upon a key known only to the user attempting access.

3 WHAT IS BIOMETRICS

Biometrics is the science of measuring physical properties of living beings. It is a collection of automated methods to recognize an individual person based upon a physiological or behavioral characteristic [13]. As illustrated in figure 1, the characteristics measured are face, fingerprints, hand geometry, handwriting, iris, retina, vein, voice etc. In present technology scenario biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions.

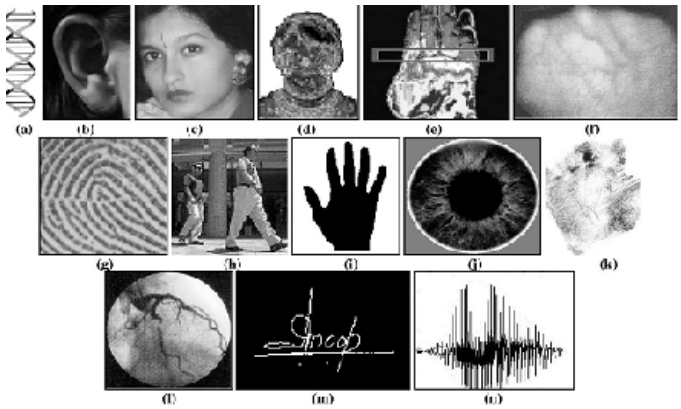

Figure 1:- Examples of Various Biometric Characteristics: (a) DNA, (b) Ear, (c) Face, (d) Facial Thermogram, (e) Hand Thermogram, (f) Hand Vein, (g) Fingerprint, (h) Gait, (i) Hand Geometry, (j) Iris, (k) Palmprint, (l) Retina, (m) Signature

As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. Biometrics involves using the different parts of the body such as the fingerprint or the eye, as a password or form of identification. Currently, in crime Investigations fingerprints from a crime scene are being used to find a criminal. However, biometrics is becoming more public. Iris scans are used in United Kingdom at ATM's instead of the normal codes [8]. In Andhra Pradesh, India, iris recognition is being used to issue house hold ration cards. Practically all biometric systems work in the same manner. First, a person is enrolled into a database using the specified method. Information about a certain characteristic of the human is captured [5].

This information is usually placed through an algorithm that turns the information into a code that the database stores. When the person needs to be identified, the system will take the information about the person again, translates this new information and then compares the new code with the ones in the database to discover a match, as shown in Figure 2.

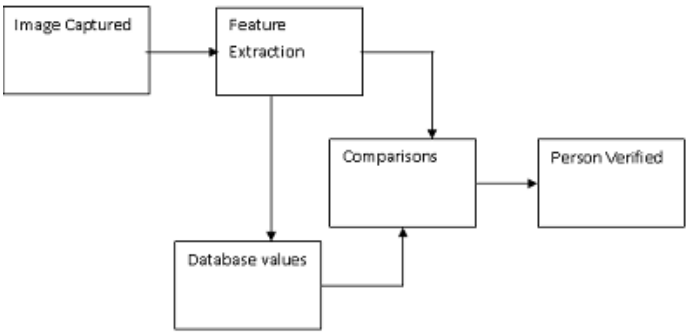

Figure 2:- Block Diagram for Biometric Recognition

Biometrics works by unobtrusively matching patterns of live individuals in real time against enrolled records. Leading examples are biometric technologies that recognize and authenticate faces, hands, fingers, signatures, irises, voices, and fingerprints. Biometric data are separate and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information. Requirements of a biometric feature are uniqueness, universality, permanence, measurability, user friendliness, collectible, acceptability. Biometrics can be categorized based on comfort, accuracy, availability, costs. As one can see, determining an 'optimal' biometric method is hardly possible. For biometric methods ranking high in accuracy, fingerprints currently have the lowest costs.

4 WHY ONLY BIOMETRIC RECOGNITION

The increased need of privacy and security in our daily life has given birth to this new area of science and technology. Biometric techniques, such as fingerprint verification, iris or face recognition, retina analysis and hand-written signature verification, are increasingly becoming basic elements of authentication and identification systems. However, any human physiological or behavioral traits serving as biometric characteristics are personal data protected by privacy protection legislation [6]. Biometric techniques according to data protection principles, purpose, proportionality and security, provided in international legislation. This analysis leads to the desired properties of biometric systems in the form of

functional and non-functional requirements, in order to support developers minimizing the risk of being non-compliant to privacy protection legislation, and to increase user acceptance.

Biometric access control systems are affordable and with the increasing sophistication of biometric technology, you can choose between several different biometric modalities such as fingerprint, finger vein, palm vein, facial recognition, hand geometry, voice and many others [7]. Normally, when an individual presents their physiological information to a biometric access control unit and is positively identified, the unit will send a signal to a door strike which will release and allow that individual access to a restricted area.

5 CONCLUSIONS

In this paper, we have seen what does the term authentication means and the basic classification of authentication techniques. After the detail study of different authentication methods, it is crystal clear that why we prefer Biometric technique as a solution. While biometric authentication can offer a high degree of security, they are far from perfect solution. Sound principles of system engineering are still required to ensure a high level of security rather than the assurance of security coming simply from the inclusion of biometrics in some form [14].

The influences of biometric technology on society and the risks to privacy and threat to identify will require mediation through legislation. For much of the short history of biometrics the technology developments have been in advance of ethical or legal ones.

6 FUTURE WORK

Biometric recognition is one of the best methods in auttication as well as security area. We enhance this work by implementing the existence research work and also study more biometric technologies such as DNA, Ear, Face, Facial Thermogram, Hand Thermogram, Hand Vein, Fingerprint, Gait, Hand Geometry, Iris, Palmprint, Retina and Signature recognition, that are available today in theoretically or practically [12]. On moving ahead, compare them to find out which one is the best option for the purpose of human identification.

REFERENCES

[1] Kresimir Delac and Mislav Grgic. A survey of biometric recognition methods. In Proceedings of the 46th International Symposium Electronics in Marine (ELMAR- 2004), pages 184–193, Croatia, June 2004.

[2] Hanna-Kaisa Lammi. Ear biometrics, 2005. http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Lammi.pdf.

[3] K.H. Pun and Y.S. Moon. Recent advances in ear biometrics. In Proceeding of the 6th IEEE International Conference on Automatic Face and Gesture Recognition, pages 164–169, Seoul, May 2004.

[4] Alfred Iannarelli. Ear Identification, Forensic Identification Series. Paramont Publishing, E.U.A., 1989.

[5] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld. Face recognition: A literature survey. ACM Computing Surveys, vol. 35, issue 4, pages 399–458, December 2003.

[6] P. J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone. Frvt2002: Overview and summary, 2002.http://www.frvt.org/FRVT2002/documents.htm.

[7] P. Jonathon Philips, Hyeonjoon Moon, Syed A. Rizvi, and Patrick J. Rauss. The FERET evaluation methodology for face-recognition algorithms. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 2, no. 10, pages 1090–1104, October 2000.

[8] Anil K. Jain, Lin Hong, and Sharath Pankanti. Biometric identification. Communications of the ACM, vol. 43, no. 2, pages 91–98, February 2000.

[9] S. Niyogi and E. Adelson. Analyzing gait with spatiotemporal surfaces. In Proceedings of the IEEE Workshop Non-Rigid Motion, pages 24–29, Austin, November 1994.

[10] Zongyi Liu and Sudeep Sarkar. Improved gait recognition by gait dynamics normalization. IEEE Transactions on Pattern Analysis and Machine Inteligence, vol.28, no. 6, pages 863–876, June 2006.

[11] Biometric News Portal. Hand vein biometric, 2006. http://www.biometricnewsportal.com/palm biometrics.asp.

[12] M. Villani, C. Tappert, Ngo Giang, J. Simone, H.St.Fort, and Cha Sung-Hyuk. Keystroke biometric recognition studies on long-text input under ideal and applicationoriented conditions. In Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW06), pages 39–47, New York, June 2006.

[13] John D. Woodward, Christopher Horn Jr., Julius Gatune, and Aryn Thomas. Biometrics: A look at facial recognition. Technical report, Rand Corporation, http://www.rand.org/pubs/documented briefings/DB396, 2003.

[14] Zhanna Korotkaya. Biometric person authentication: Odor, 2006. http://www.it.lut.fi/kurssit/03-04/010970000/seminars/ Korotkaya.pdf.