BIOMETRICS AUTHENTICATION TECHNIQUE FOR INTRUSION DETECTION SYSTEMS USING FINGERPRINT RECOGNITION

Smita S. Mudholkar [1], Pradnya M. Shende [2], Milind V. Sarode [3]

[1, 2& 3] Department of Computer Science & Engineering, Amravati University, India
smi.mudholkar@gmail.com, shende_pradnya@rediffmail.com,
parthmilindsarode@rediffmail.com

ABSTRACT

Identifying attackers is a major apprehension to both organizations and governments. Recently, the most used applications for prevention or detection of attacks are intrusion detection systems. Biometrics technology is simply the measurement and use of the unique characteristics of living humans to distinguish them from one another and it is more useful as compare to passwords and tokens as they can be lost or stolen so we have choose the technique biometric authentication. The biometric authentication provides the ability to require more instances of authentication in such a quick and easy manner that users are not bothered by the additional requirements. In this paper, we have given a brief introduction about biometrics. Then we have given the information regarding the intrusion detection system and finally we have proposed a method which is based on fingerprint recognition which would allow us to detect more efficiently any abuse of the computer system that is running.

KEYWORDS

Intrusion detection, keystroke, Biometrics, Mouse dynamics, Authentication

1. INTRODUCTION

Biometric recognition forms a strong bond between a person and his identity as biometric traits cannot be easily shared, lost, or duplicated. Hence, biometric recognition is fundamentally superior and more resistant to social engineering attacks than the two conservative methods of recognition, namely, passwords and tokens. Since biometric recognition requires the user to be present at the time of authentication, it can also prevent users from making false refutation claims. Moreover, only biometrics can provide negative identification functionality where the aim is to set up whether a certain individual is really enrolled in a system even if the individual might refuse it. Due to these characteristics, biometric recognition has been widely hailed as a natural, reliable, and exceptional component of any identity system. Computer systems are targeted by three kinds of attacks [6]: (1) user-level, when a genuine user uses his rights to steel information, (2) system-level, when an intruder uses system calls to assault the system, and (3) network-level, when an attacker uses data stream to execute the attack. During the last years, huge advances have been made in handling system and network-level attacks. However, user-level attacks were dealt with mostly in combination with system-level attacks. This kind of attack is measured as the most persistent forms of intrusions [1]. A classic example of a user-level attack is a masquerade attack, where scrawled user impersonates another comprehensible user in order to gain access to sensitive information is a major problem these days, since it serves as a precondition for most of

DOI : 10.5121/ijcseit.2012.2106

the intrusions. The security services that contradict this threat are identification and authentication. Moreover, biometric recognition systems can operate in two modes [1]: identification mode, where the system identifies a person searching a large database of enrolled users for a counterpart; and authentication mode where the system verifies a person's claimed identity from his earlier enrolled pattern.

2. BIOMETRICS

Biometrics makes the use of biological terms that deals with data statistically. It verifies a person's uniqueness by analyzing his physical features or behaviors (e.g. face, fingerprint, voice, signature, keystroke rhythms). The systems record data from the user and compare it each time the user is claimed. A biometric system is a computer system that implements biometric recognition algorithms. A typical biometric system consists of sensing, feature extraction, and matching modules.

We can classify the biometric techniques into two classes:

- *Physiological based techniques* include facial analysis, fingerprint, hand geometry, retinal analysis, DNA and measure the physiological characteristics of a person.
- *Behavior based techniques* include signature, key stroke, voice, smell, sweat pores analysis and measure behavioral characteristics.

Biometric recognition systems based on the above methods can work in two modes: *identification* mode, where the system identifies a person searching a large data base of enrolled for a match; and *authentication* mode where the system verifies a person's claimed identity from his earlier enrolled pattern.

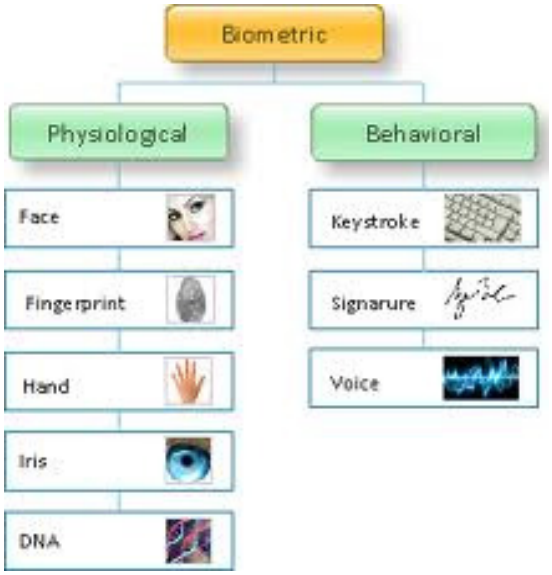

Figure 1 Categories of biometric

2.1 Types of Biometrics

2.1.1 Facial Recognition

The facial recognition systems differentiate between the background and the face. This is important when the system has to identify a face within a throng. The system then makes

use of a person's facial features – its peaks and valleys and landmarks – and treats these as nodes that can be measured and compared against those that are stored in the system's database. There are around 80 nodes comprising the face print that the system makes use of and this includes the jaw line length, eye socket depth, distance between the eyes, cheekbone shape, and the width of the nose.

Figure 2 Facial recognition

Advantages:

- It is not intrusive.
- It is hands-free, and continuous.
- It can be done from a distance even without the user being aware they are being scanned.

Disadvantages:

- Many systems are less effective if facial expressions vary. Even a big smile can render the system less effective.
- Face recognition does not work well include poor lighting, sunglasses, long hair, or other objects partially covering the subject's face, and low resolution images.
- Facial recognition system requires actual management of large databases.

2.1.2 Iris Recognition

Iris recognition is an automated method of biometric identification which uses mathematical pattern recognition techniques on video images of the irises of an individual's eyes, whose complex random patterns are unique and can be seen from some distance. Iris cameras perform recognition detection of a person's identity by analysis of the random patterns that are visible within the iris of an eye from several distances. It combines computer vision, pattern recognition, statistical inference and optics. The iris is the colored ring around the pupil of every human being and like a snowflake, no two are the same. Each one is unique in its own way, exhibiting a distinctive form.

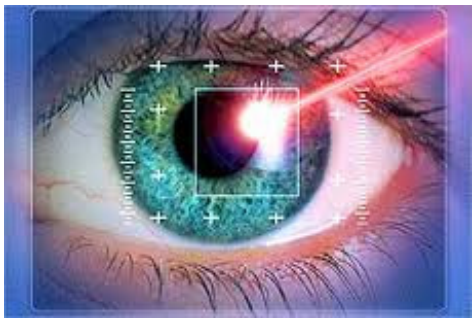

Figure 3 Iris Recognition

Advantages of Iris Recognition:

- Iris-scanning technology is not very intrusive as there is no direct contact between the subject and the camera technology.
- It is non-invasive, as it does not use any laser technology, just simple video technology.
- The accurateness of the scanning technology is a major benefit with error rates being very low, hence ensuing a highly reliable system for authentication.

Disadvantages of Iris Recognition:

- The iris is a very small organ to scan from a distance. It is a moving target and can be covered by objects such as the eyelid and eyelashes.
- Subjects who are blind or have cataracts can also cause a challenge to iris recognition, as there is difficulty in reading the iris.
- The camera used in the process needs to have the correct amount of illumination. Without this, it is very complicated to capture an accurate image of the iris.

2.1.3 Keystroke

The functionality of this biometric is to measure the dwell time (the length of time a key is held down) and flight time (the time to move from one key to another) for keyboard actions. Keystroke biometrics work on the basis of multiple feature extraction being used to create a profile of an individual. This profile is used to identify or authenticate the user. Keystroke analysis is concerned with the frequency, accuracy, the pause between strokes and the length of time a key is depressed.

Figure 4 Keystroke

Advantages of Keystroke:

- Keystroke recognition system is simple to implement due to the fact that it does not require any specific hardware.
- It is relatively easy to learn.

Disadvantages of Keystroke:

- The performance of the keystroke is affected by various circumstances of the human users, such as a hand injury or fatigue of the legitimate user.
- Limited accuracy.
- The systems developed for this biometric method are costly since they use neurological methods and dedicated terminals.

2.1.4 Mouse Dynamics

Mouse dynamics can be described as the characteristics of the actions received from the mouse input device for a specific user while interacting with a specific graphical user interface. A mouse action can be classified into one of the following categories:

- Mouse-Move (MM): general mouse movement,
- Drag-and-Drop (DD): the action starts with mouse button down, movement, and then mouse button up,
- Point-and-Click (PC): mouse movement followed by a click or a double click, and
- Silence: no movement.

The characteristics of mouse dynamics can be described by a set of factors generated as a result of analyzing the recorded mouse actions. These factors represent the components mouse dynamics signature for a specific user, which can be used in verifying the identity of the user.

Figure 5 Mouse dynamics

Advantages of mouse dynamics:

- Mouse dynamics does not required special hardware device for data collection.
- Low cost and low invasiveness.

Disadvantages of mouse dynamics:

- The performance of the mouse dynamics is affected by various circumstances of the human users, such as a hand injury or fatigue of the legitimate user.
- Limited accuracy

2.2 Reasons for using Biometrics

Using biometrics for identifying human beings offers some reward like it can be used to identify you as you. Tokens, such as smart cards, magnetic stripe cards, photo ID cards, physical keys etc can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed. Moreover, today's fast-paced electronic world means people are asked to remember a huge number of passwords and personal identification numbers for computer accounts, bank ATMs, e-mail accounts, wireless phones, and web sites and so on. Biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less exclusive authentication for a variety of applications. The biometric authentication provides the ability to require more instances of authentication in such a quick and easy manner that users are not bothered by the additional requirements. As biometric

technologies mature and come into wide-scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users.

2.3 Challenges in Biometric Authentication

The different challenges in front of biometric system are as follows:

2.3.1 Privacy Issues:

An inconsequential way to include biometric authentication in smart card- based password authentication is to scan the biometric characteristics and store the extracted biometric data as a template in the server. During the authentication, a comparison is made between the stored data and the input biometric data. If there is an adequate cohesion, a biometric authentication is said to be successful. This method, however, will raise some security risks, mainly in a multiserver environment where user privacy is a concern. Servers are not fully secure. Servers with weak security protections can be broken in by attackers, who will obtain the biometric data on those servers. And also servers are not 100 percent trusted. Server-X could try to login to Server-Y on behalf of their common clients, or distribute users' biometric information in the system. In both the cases, user privacy will be compromised, and a single-point failure on a server will relegate the whole system's security level from three-factor authentication to two-factor authentication.

2.3.2 Error Tolerance and Nontrusted Devices

One challenge in biometric authentication is that biometric characteristics are prone to various noise during data collecting, and this natural feature makes it impossible to reproduce precisely each time biometric characteristics are measured. A biometric authentication protocol cannot simply compare the hash or the encryption of biometric template. Instead biometric authentication must endure failures within a rational bound. Another issue in biometric authentication is that the verification of biometrics should be performed by the server instead of other devices, since such devices are usually remotely located from the server and cannot be fully trusted.

3. INTRUSION DETECTION SYSTEM

3.1 What is intrusion detection system?

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies apprehensive pattern that may specify a network or system attack from someone attempting to crack into or compromise a system. One facet of computer security will work to keep people from receiving unauthorized access by selecting good security passwords, using software to protect against known intrusions. The IDS examine the performance of the computer and then give some kind of alert when apprehensive activity is detected.

For example, Gmail carries basic IDS. This enables users to make sure whether anyone has signed in to their account from a different location. In crate looking at the list and only see your home IP address and phone number, everything is likely to be okay. In the event that some capricious IP address from Tokyo, Mumbai or Berlin is on the list, someone has surely compromised your email account. Whilst Gmail requires users to monitor things manually, there are automated systems to ensign disputed activity and give warnings. The question is where the intrusion detection system fits in the design. To put it in simpler terms, an Intrusion detection system can be compared with a burglar alarm. For example, the lock system in a car protects the car from theft. But if somebody breaks the lock system and tries to steal the car, it is the burglar alarm that detects that the lock has been broken and alerts the owner by raising an alarm. The Intrusion detection system in a similar way complements the firewall security. The firewall

protects an organization from cruel attacks from the Internet and the Intrusion detection system detects if someone tries to break in through the firewall or manages to break in the firewall security and tries to have access on any system in the trusted side and alerts the system administrator in case there is a break in security. Besides, Firewalls do a very good job of filtering incoming traffic from the Internet; however, there are ways to circumvent the firewall. For example, peripheral users can connect to the Intranet by dialing in through a modem installed in the private network of the organization. This kind of access would not be seen by the firewall. Therefore, an Intrusion detection system is a security system that monitors computer systems and network traffic and analyzes that traffic for probable aggressive attacks originate from outside the organization and also for system abuse or attacks originating from within the organization.

3.2 Types of Intrusion Detection Systems

IDSs can be of three types which are as follows:

- Network-based intrusion detection, which runs at the gateway of a network and observe all arriving packets. And it has network-based sensor
- Router-based intrusion detection, which is installed on the routers to prevent intruders from entering the network.
- Host-based intrusion detection, which receives the necessary audit data from the host's operating system and analyzes the generated events to keep the local node secure.

4. FINGERPRINT RECOGNITION

Fingerprint recognition describes the process of obtaining a digital representation of a fingerprint and comparing it to a stored digital version of a fingerprint. Electronic fingerprint scanners capture digital "pictures" of fingerprints, either based on light reflections of the finger's ridges and valleys, ultrasonic's, or the electrical properties of the finger's ridges and valleys. These pictures are then processed into digital templates that contain the unique extracted features of a finger. These digital fingerprint templates can be stored in databases and used in place of traditional passwords for secure access. Instead of typing a password, users place a finger on an electronic scanner. The scanner, or reader, compares the subsist fingerprint to the fingerprint template stored in a database to resolve the identity and validity of the person requesting access. Among all biometric techniques, fingerprint recognition is the most popular method due to the following advantages:

1) Universality—the size of the population with clear fingerprints exceeds the size of the population with passports.

2) High distinctiveness—still identical twins who share the same DNA have different fingerprints.

3) High performance—at the age of seven months, a fetus's fingerprints is fully developed, and their characteristics do not change in the absence of injury or skin disease. However, after a small injury the sample will raise back as the fingertip heals. The rareness of fingerprints can be determined by the pattern of minutia locations, local ridge orientation data, and combination of ridge orientation and minutia locations Therefore, fingerprint recognition has become a reliable method of personal identification.

4.1 Fingerprint Identification Algorithm

Introduced Fingerprint Identification System consists of two processes.[7]

1) The enrollment process: This process consists of capturing a person's fingerprint using a fingerprint capturing device. During the enrollment process, the system saves the persons fingerprint into a database (see Figure 7).

2) The authentication process: It is used to authenticate the claimed person. This process consists of comparing a captured fingerprint to an enrolled fingerprint in order to determine whether the two match. If the two fingerprints match, then the computer will be unlocked, otherwise, an alert will be sent (see Figure 8).

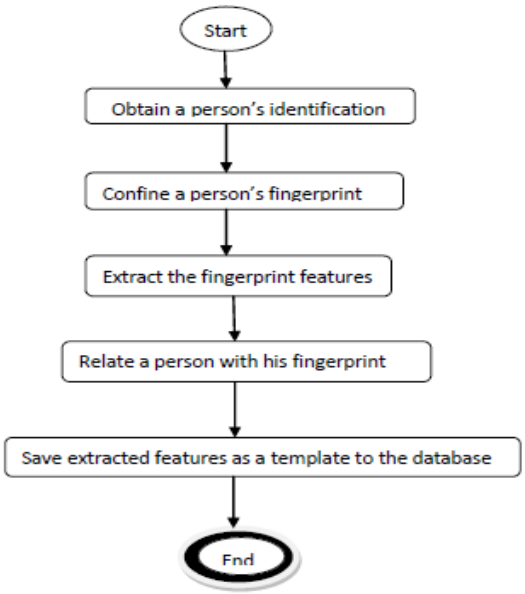

Figure 7 the enrollment process

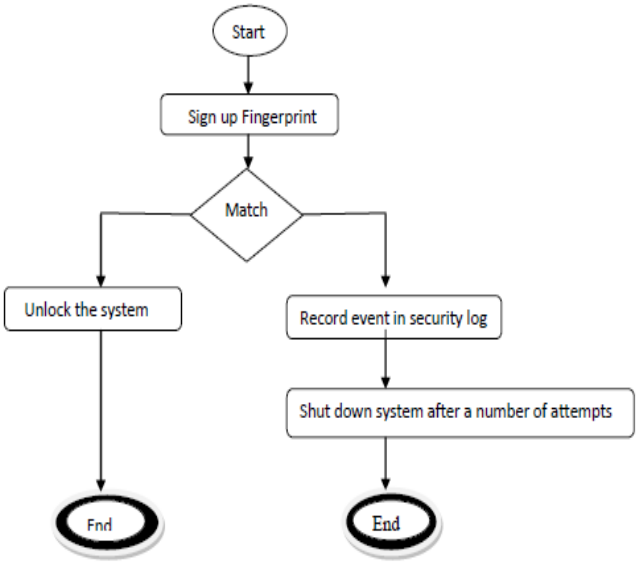

Figure 8 the verification process

4.2 Comparison with other techniques

- Some users do not use the mouse regularly in their work. Therefore, they could not be authenticated through a mouse dynamic system. On the other hand, all genuine users could enroll their fingerprint and use a fingerprint-based system.
- Attackers could impersonate a valid user's keystroke and get access to aware information without being noticed, while a fingerprint could not be copied.
- Difference between this technique and the mouse dynamics and keystroke techniques is that the latter may require hours and maybe days in order to train the system, and more time to authenticate a genuine user, while the Fingerprint Identification System needs less time to enroll a fingerprint, and to authenticate a user.

5. CONCLUSION

There are several attacks that try to negotiate a computer system using a variety of methods such as unauthorized access. These attacks could be reduced if an identification tool is used to complement already deployed intrusion detection system. The most reliable identification systems are based on biometrics. Therefore, several biometrics technologies start to accompany host-based Intrusion detection systems. Until Now, behavioral biometric was the only techniques that have been used so far, since they do not need any special devices. In contrast, some researchers proved that these techniques are not very efficient which was the motivation to design an identification system based on fingerprint technique.

REFERENCES

[1] A. Ahmed and I. Traore. Anomaly intrusion detection based on biometrics. *In 6th IEEE Information Assurance Workshop,* 2005.

[2] A. Ahmed and I. Traore. A new biometric technology based on mouse dynamics. *In Transactions on Dependable and Secure Computing, pages 165–179, 2007.*

[3] Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross. Biometrics: a grand challenge. *In Proceedings of the 17th International Conference on Pattern recoginition, pages 935–942, 2004.*

[4] D. Gunetti and C. Picardi. Keystroke analysis of free text. ACM transactions on information and System Security, 8(3), 2005.

[5] E. Lau, X. LI, C. Xiao, and X. Yu. Enhanced user authentication through keystroke biometrics. *In Computer and Network Security, Massachusetts Institute of technology, 2004.*

[6] J. McHugh. Intrusion and intrusion detection. International Journal of Information Security, 1:14–135, 2001.

[7] Khalil Challita, Hikmat Farhat, Khaldoun Khaldi. Biometric Authentication for Intrusion Detection Systems. *First International Conference on Integrated Intelligent Computing, 2010*