World Research Journal of Pattern Recognition
ISSN: 2278-8557 & E-ISSN: 2278-8565, Volume 1, Issue 1, 2012, pp.-01-04.
Available online at http://www.bioinfo.in/contents.php?id=184

BIOMETRIC APPROACH TO COMPLEMENT A HOST-BASED INTRUSION DETECTION SYSTEM USING FINGERPRINT RECOGNITION TECHNIQUE

MUDHOLKAR S.S*., SHENDE P.M., KHARAT V.P., KHODWE S.S.

Department of Computer Science & Engineering, Amravati University, Yavatmal, Maharashtra, India.
*Corresponding Author: Email- smi.mudholkar@gmail.com

Received: February 28, 2012; Accepted: May 03, 2012

Abstract- Most of the presently available intrusion detection systems do not grant any authentication functionality in order to identify the users who access a computer system. In particular, insiders are able to misuse their concessions without being detected. Some intrusion detection systems aim to authenticate genuine users once they log in to the system, as well as to prevent access to unauthorized people who try to imitate other users. The main goal of this paper is to initiate and apply a new approach that uses the fingerprint technique to harmonize a host-based intrusion detection system in order to advance its level of authentication, which would allow us to detect more efficiently any abuse of the computer system that is running it.
Keywords- Fingerprint recognition, Biometrics, Intrusion detection system, HIDS.

Citation: Mudholkar S.S., et al. (2012) Biometric Approach to Complement a Host-based Intrusion Detection System Using Fingerprint Recognition Technique. World Research Journal of Pattern Recognition, ISSN: 2278-8557 & E-ISSN: 2278-8565, Volume 1, Issue 1, pp.-01-04.

Introduction

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 [1]. There are several attacks such as user level attack, system level attack and network level attack that try to negotiate a computer system using a variety of methods [1]. 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, behavioural biometric such as keystroke [2, 9] and Mouse Dynamics [3, 8] 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 recognition. Our aim in this paper is to bestow a host-based intrusion detection [4] system with a fingerprint identification system in order to authenticate users of a computer system in a more consistent way. This paper consists of introduction about biometrics and IDS then method is introduced that uses a fingerprint technique in order to increase the authentication capability of an IDS. Finally, before concluding, we have discussed and analyze the results of our method.

Biometric

The term biometrics is consequent from the Greek bio which means life and metric which means measure [6].Biometrics technology is simply the measurement and use of the unique characteristics of living humans in order to distinguish them from one another [5].Biometric systems work in two modes, the enrolment mode and the verification identification mode. In the first mode, biometric data is acquired using a user interface or a capturing device, such as a fingerprints scanner. Raw biometric data is then processed to extort the biometric features representing the characteristics, which can be used to differ the users. This conversion process produces a processed biometric identification sample, which is stored in a database as a template for future needs. Enrolled data should be free of noise and any other defects that can affect its comparison with other samples. In the second mode, biometric data is captured, processed and compared against the stored enrolled sample. Verification or identification process will

be conducted as par the type of application Verification process: conducts one-to-one matching by comparing the processed sample against the enrolled sample of the same user. For example, user authentication at login: the user declares his identity by entering his login name. He then confirms his identity by providing a password and biometric information, such as his signature, voice password, or fingerprint. To verify the identity, the system will compare the user's biometric data against his record in the database, resulting with a match or no match. Identification process: matches the processed sample against a large number of enrolled samples by conducting a 1 to N matching to identify the user; resulting in an identified user or a non-match order to evaluate the accuracy of a biometric system.

There exist two categories of biometrics (1) physical biometrics which measure the physiological characteristics of a person, such as fingerprint, iris scan, face recognition, and (2) behavioural biometrics which measure the behaviour of a person, such as keystroke dynamics and mouse dynamics [5, 7]. Fig 1 is showing different biometric systems.

Fig.1- Different biometric system

Intrusion Detection

What is Intrusion Detection System?

An intrusion detection system inspects all the network activities and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system [5]. One aspect of computer security will work to keep people from receiving unauthorized access by selecting good security passwords, using software to safeguard against well -known intrusions and so on. The IDS monitor the performance of the computer or the account and then give some kind of alert when suspicious activity is detect [4].

For instance, Gmail carries basic IDS which enable the users to verify whether anyone has signed in to their account from a different location. 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 malicious 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 alerts the system administrator in case there is a break in security. Firewalls do a very good job of filtering incoming traffic from the Internet; however, there are ways to evade the firewall. For example, external users can connect to the Intranet by dialling in through a modem installed in the private network of the organization. This kind of access would not be observed by the firewall. Therefore, an Intrusion detection system (IDS) is a security system that monitors computer systems and network traffic and analyzes that traffic for possible aggressive attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization.

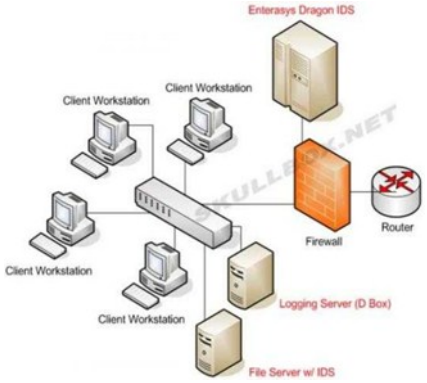

Fig. 2- Intrusion Detection System

Types of Intrusion Detection Systems

IDSs can be divided into following categorized:

- Network-based intrusion detection, which runs at the gateway of a network and examine all incoming packets. And it has network-based sensor.
- Router-based intrusion detection, which is installed on the routers prevents from entering intruders into 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.

Host-based Intrusion Detection

Host data sources are profuse and varied, including operating system event logs, such as kernel logs, and application logs such as syslog. These host event logs contain information about file accesses and program executions associated with inside users. Host-based systems are designed more to prevent the system from insiders than from outsiders. Host-based systems focus mainly on exploitation of privilege. Insiders do not have to use vulnerabilities because they are already in the network and have their own privileges. However, outsiders must use vulnerabilities to get inside the network and gain privileges. Host-based systems provide poor real-time response and cannot effectively protect against one-time atrocious events. They are, however, excellent at detecting and responding to long term attacks, such as stealing of data or aggravated employees. Host-based systems maintain a large database of behavioural information that can be mined for trends indicative of misuse.

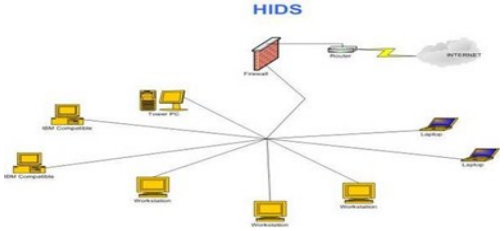

Fig. 3- Host-based intrusion detection

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 fingerprint. These 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 live fingerprint to the fingerprint template stored in a database to determine the identity and validity of the person requesting access.

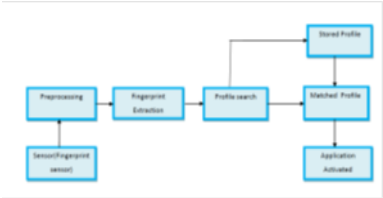

Fig. 4- Flow of Fingerprintprint Recognition

Architecture and Implementation

To achieve our aim, we choose the language Visual Basic for the implementation of the fingerprint identification system, which uses the Microsoft Visual Studio compiler and runs using. Net platform. The operating system we have chosen is Microsoft XP. And for capturing the fingerprints we have selected the fingerprint scanner which shown in fig [5].

Fig. 5- Fingerprint scanner

Architecture

Fig. 6 illustrates the main architecture of introduced system.The introduced system basically consist of two steps enrollment and authentication. The enrollement phase include capturing a fingerprint using fingerprint scanner then extracting the features of the fingerprint and storing it as a template in the database. The second phase i.e. the authentication phase consists of capturing the fingerprint of the claimed person then extracting its features and then comparing it with the stored template in the database. If the input fingerprint matches with the template in the database then the system will be unlocked and if they do not match then alert will be generated and after several unauthorized attempts the system will be shut down.

Fig. 6- Block diagram of fingerprint Recognition system

Fingerprint Identification Algorithm

Introduced Fingerprint Identification System consists of two processes [5].

1. The enrollment process: This process consists of capturing a person's fingerprint using a fingerprint capturing device. During the enrollment process, the system extracts the features of fingerprint as template and stores it into a database (see Fig. 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 and determining whether the two match. If the two fingerprints match, then the computer will be unlocked, otherwise, an alert will be sent (see Fig. 8).

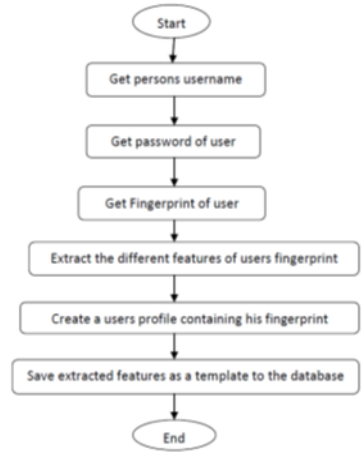

Fig. 7- the enrollment process

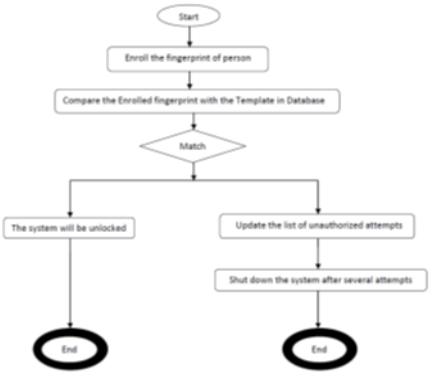

Fig. 8- the verification process

Simulations and Results

Simulations

In our experiment, 50 users were enrolled and their profile was created along with fingerprints stored into the database. In order to get access to the system, a user authenticated him/her using his/her username, password, and fingerprint. The application checked the username and password for a match, as well as the fingerprint taken from the device (i.e. the Fingerprint scanner) against the template stored in the database. Access was granted in case of a match, otherwise it was denied. During that time, the system monitored all the actions that occurred on the system, and stored the list of all unauthorized and authorized attempts.

Results

During the testing period, 27 legitimate users tried to access the system and they were authenticated. On the other hand, 15 illegible users tried to access the system, and they all were rejected. Thus the system works properly as per requirements.

Comparison with Other Techniques

- Some users do not use the mouse frequently in their work. Therefore, they could not be authenticated through a mouse dynamic system. On the other hand, all legitimate users could enroll their fingerprint and use a fingerprint-based system.
- Attackers could impersonate a legitimate user's keystroke and get access to sensitive information without being noticed, while a fingerprint could not be copied.
- A key difference between this method and the mouse dynamics and keystroke techniques is that fingerprint recognition requires less amount of time to authenticate a person as compare to mouse dynamics and keystroke.

Conclusion

Identifying attackers is a major problem which is faced by both organizations and governments. Recently, the most used applications for prevention or detection of attacks are intrusion detection systems. Generally we use tokens for authentication such as smart cards, magnetic stripe cards, photo ID cards, physical keys etc which can be lost, stolen, duplicated, or left at home. So instead of using such tokens it is more beneficial to use biometrics as a weapon to identify the users. Because of high cost of fingerprint scanner, only mouse dynamics and keystroke was used in case of IDS. But these methods are not much effective. Moreover, nowadays fingerprint scanner is becoming less expensive and they can be easily available so it is better to use fingerprint recognition technique to authenticate the users. And so fingerprint recognition is becoming the primary means of identification used by Governments and law enforcement agencies. Thus the introduced method is easy to authenticate user and preventing the system from different kinds of attacks.

References

[1] Ahmed A. and Traore I. (2005) *In 6th IEEE Information Assurance Workshop*.
[2] Lau E., LI X., Xiao C. and Yu X. (2004) *In Computer and Network Security, Massachusetts Institute of technology.*
[3] Ahmed A. and Traore I. (2007) *In Transactions on Dependable and Secure Computing*, 165-179.
[4] McHugh J. (2001) *International Journal of Information Security*, 1, 14-135.
[5] Khalil Challita, Hikmat Farhat and Khaldoun Khaldi. (2010) *First International Conference on Integrated Intelligent Computing.*
[6] A book on Usable Biometrics by Lynne Coventry.
[7] Ahmed Awad E. Ahmed, Issa Traor A. (2006) *World Scienti c Review*. 9in x 6in.
[8] Akif Nazar, Issa Traore, Ahmed Awad E. Ahmed. (2008) *International Journal of Pattern Recognition and Artificial Intelligence,* 22(3), 461-495.
[9] Gunetti D. and Picardi C. (2005) *ACM transactions on information and System Security*, 8(3), 2005.