International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 9, September- 2014

PC Snooper - A Secure Service for User Identity Verification

Delitia M George
M.Tech Scholar
Department of CSE

Neethu Roy
Assistant Professor
Department of IT

***Abstract*: Most existing security measures for protecting a PC from unauthorized access is based on textual passwords. Since textual passwords are not a trusted measure as it is vulnerable to attack, the proposed method uses continuous user authentication by face recognition for securing a pc from intruders and attackers. PC owner can decide the privileges to PC, by setting different priorities and unauthorized access is prevented by method known as continuous user authentication by face recognition. This can be applicable to high security areas like defense, rocket launching, research centers etc. Continuous authentication of user helps to prevent intruders to enter in to a PC or a number of PCs. Username and passwords are replaced by biometric traits as face, fingerprint etc offer an emerging solution for trusted and secure authentication and this can be done transparently. Whenever the admin/owner of a PC or a network wants to know about the details of logs that the intruder has done in a PC, a software named Pc_Snooper can be installed in PC and it will run automatically whenever an intruder/outsider sit in front of a PC and do some work. The proposed framework authenticates every user continuously by recognizing the face and is done in a transparent manner. Thus each and every time Pc is secured.**

Keywords— Face recognition, Pc_Snooper, Continuous user authentication.

I. INTRODUCTION

Username and password are the most common authentication technique used to sign-on in to a PC. And this traditional password based authentication system allows the user to use PC by assuming that the user who enters the username and password is the actual authorized user. The lack of differentiation between the legitimate user and intruder who knows the login credentials give a chance to intruders to exploit PC as much as time he wishes. So it is very important to recognize the authorized user of PC at the log in time itself. And once the user identity has been verified, the system resources are available for the users who sign-on in to the system for a period of time until the user logout the system. Verification of user only at the login time does not guarantee security because of the following reasons.

- Legitimate user logged in to a system and leaves the PC unattended in the work area for awhile. Then any other persons can use that PC, as it is already ON and logged in by the legitimate user.
- If the PC can be stolen and the one who stole the PC knows the username and password can easily use the PC.

Due to the above problems, single authentication is not safe for a PC as we cannot guarantee that one who logged in to PC will use the PC whole time. Traditional textual based password authentication system suffers from two disadvantages.

1) Assumption that the user who enters the password is the actual authorized user of that PC.
2) Assumption that every time same user, that is the authorized one sit in front of PC.

This paper proposes a method to overcome the above disadvantages by continuous user authentication for securing a PC and tracking of intruder logs using software named Pc_Snooper. PC security is a serious concern as every PC contains valuable information about some persons or some organizations and so on. Even though PC can be secured by textual passwords, but the single log-in session does not guarantee sufficient degree of security. So that continuous authentication by face recognition is used here. This method can ensure that one who logged on to a PC is an authorized user. In order to monitor a person who sits in front of a PC, continuous monitoring system is developed instead of static authentication. Continuous monitoring system monitors a user every time when he comes in front of a PC and continues monitoring till he moves away from the PC. Whenever a person has to do some work in a PC, he is always looking on to the monitor. So face of the user can be easily captured. This is the technique used here. User is unaware of capturing his face, i.e. monitoring system works transparently. Continuous monitoring system observes user's presence in front of a PC using webcam and face recognition on a captured frame. The biometric trait used here for continuous authentication is face.

The main modules of the proposed method are

- Continuous user authentication by face recognition.
- Tracking of intruder details by Pc_Snooper.
- Web module for viewing intruder logs.

II. RELATED WORK

Computer system and network system security can be provided by user authentication. Most popular approaches for authentication of user are knowledge based methods (e.g. password) and token-based methods (e.g. smart card). Identification of a person based on physiological or behavioral characteristics is referred to as biometrics. Example of biometric traits includes fingerprints, hand geometry, face, voice etc. Biometric traits are unique and this can be used to identify persons [1]. When considering the implementation of any biometric device, performance is an important factor. False acceptance rate and false rejection rate are the important performance measures.

Based on continuous user authentication a number of studies have been published [7] – [14]. Most of the methods are based on hard biometric traits (e.g. fingerprint, face). The study of Kwang *et al*. [15] Sim *et al*. [9] describe about the detection of face and fingerprint with a camera and a mouse. The mouse has an in-built fingerprint sensor. But their system suffered from low availability of biometric traits, even though they showed promising authentication results. For example fingerprint can be authenticated only if the user keeps his/her on the mouse embedded with a fingerprint reader. Also face image is not captured properly as user turn head away from the camera.

Continuous keystroke Dynamics is a paper published by P. Bours *et al*. [2] deals with a continuous authentication system which uses keystroke dynamics to recognize a person. The paper also describes a way of evaluating such a system by checking how many keys can be typed before an imposter is recognized. A multimodal biometric continuous authentication solution for local access to high security ATMs is proposed in [3]. An automatic tuning of decision parameters (threshold) for sequential multi-biometric score fusion is presented in [4]. Wearable authentication device (wrist band) can perform continuous authentication and is proposed in [5]. The user can transparently log-in through a wireless channel and authentication data can be transmitted to computers by simply approaching them in order to ensure continuous user authentication. Methods for securing passwords are proposed in [6]. A simple text based shoulder surfing resistant graphical password scheme allows a user to log-in to a computer more securely than the traditional password methods. A textual password along with color code is provided for every user to log-on in to a system. This will provide more security than text based passwords.

III. CONTINUOUS USER AUTHENTICATION BY FACE RECOGNITION

To analyze facial characteristics, facial recognition systems are used. A digital camera is required by this system to develop a facial image of the user for identification. One of the fastest growing areas in biometric technologies is the facial recognition technique. In order to ensure security to a PC, authentication method used in the proposed framework is face recognition. Whenever a user came and sits in front of a PC, face recognition process starts. The necessary equipment for the working of proposed frame is webcam, as it is the biometric device used to capture face of the user.

A facial recognition system consists of cameras that capture images of people and software that matches those pictures. The following three processes are included in every biometric device or system of devices.

- enrollment
- live presentation
- matching

Enrollment is the time when the user introduces his or her biometric information to the biometric device for the first time. Stored biometric template is formed by processing the enrollment data. Later, during the live presentation, i.e. whenever a registered user came in front of PC, the user's biometric information is extracted by the biometric device and processed to form the live biometric template. Lastly, the stored biometric template and the live biometric template are compared to each other at the time of matching, i.e. at the log-in time, to provide the biometric score or result. Details of how these systems work is given as follows.

There are many facial recognition methods, but they generally have series of steps to capture, analyze and compare a face to a database of stored images. These basic steps are given below:

A. *Detection*: Determines the locations and sizes of human face when the user came in front of a Pc or a laptop. Face detection algorithms [16]-[22] helps to detect face and ignores anything else, such as buildings, trees and bodies.

B. *Alignment:* The system determines the head's position, size and poses as the face is detected once. To register a face by the system, face needs to be turned at least 35 degrees toward the camera.

C. *Normalization:* In order to register and map the face into an appropriate size and pose, image of head is scaled and rotated. The head's location and distance from the camera is not considered for normalization. The normalization process is not affected by the light also.

D. *Representation*: The facial data is translated into a unique code by the system. For easier comparison of the newly acquired facial data to stored facial data this coding process is used.

E. *Matching*: The stored data is compared with the newly acquired facial data and (ideally) linked to at least one stored facial representation that is stored earlier.

Various face detection methods are given in fig. 1. Using any method face detection can be done. PC owner can decide who can use the PC. So that face of authorized users can be first trained and saved in to file by the owner or admin. In the proposed method, single user authentication is used. After training, whenever the authorized user came in front of PC, his/her face is recognized using any of the face recognition algorithms [23]-[25]. Only the authorized user's face is trained and unauthorized users are not

allowed to use PC, since the training image doesn't match with the face of intruders/unauthorized persons.

IV. TRACKING OF INTRUDER DETAILS BY PC_SNOOPER

Pc_Snooper is a software application used to record system activities in a PC silently when the administrator is away from the PC. The details are collected for the further examination of the administrator. The main aim of this software is to create a log for main activities performed by the user. By using this log, it could be easy to know what was done in a system in the absence of owner.

It will run in background, and logs are kept hidden in the machine for later retrieval. This software is used to capture screen shots periodically. It also provides options for sending mail to the owner's email account about the log or intrusion detection alert sms to his mobile. Other features included in this software are listing out processes & applications running on the system, showing system related information, and make a list of addresses of the visited websites. The main objectives of Pc_Snooper are as follows.

- Silently watch the activities of the PC.
- Helps the Administrator to understand what has happened in the PC.
- Taking photo of the user at random using webcam.
- Screen shots are taken periodically.
- Key, Mouse events are recorded.
- File Operations are closely monitored.
- Browser histories with user login details are obtained.
- Data is stored in encrypted format.
- Only admin through the application can retrieve the data.
- User friendly.
- The operations should be safe and unauthorized access should not be allowed.

Different modules for the proper functioning of Pc_Snooper are given below.

A. Event Logging module
- Monitoring Key events and recording to log file
- Monitoring Mouse events and recording to log file

B. File Activities module
- Monitoring File create and recording to log file
- Monitoring File reading and writing and recording to log file

C. Browser Logging module
- Monitoring Browser activities and recording to log file
- Monitoring upload / download events and recording to log file

D. Applications Watch module
- Monitoring usage of User Application and recording to log file
- Monitoring system applications running and recording to log file

E. System Info module
- Monitoring System Info and recording if any changes , to log file

F. Screenshot Logging module
- Taking Screenshots and saving to hidden folder.
- Send screenshot pictures to admin via email
- Alert intrusion through SMS

G. Administrator module
- Update login details and save to the database
- Update email for mail sending
- Update monitoring start time to end time.

The most common user interface with a computer is keyboard. In Pc_Snooper the keypress events are recorded using key loggers. Hardware and software key loggers are there and the dominant form is software key loggers. Key loggers are hardware or software tools that capture characters sent from the keyboard to an attached computer. They store capture information in a log file. When software or hardware key loggers are used, the log files are stored on the compromised machine. Software key loggers are key loggers that capture keystroke information as it passes between the computer keyboard interface and the OS. They are implemented as traditional applications or kernel-based. In almost all malicious instances of this type of key logger, users participated in some way in the software's installation.

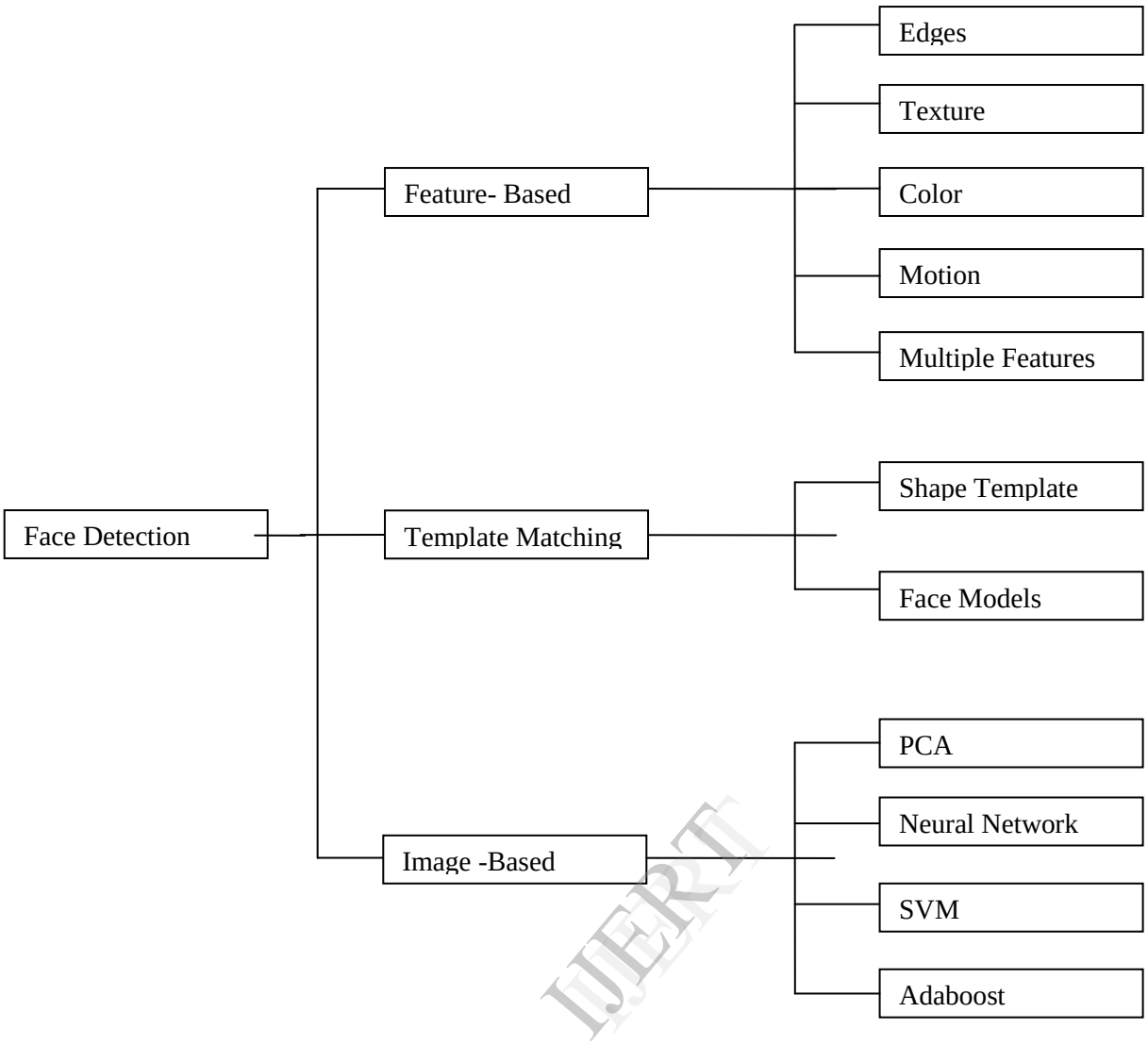

Fig.1. Various Face Detection Techniques

Key logging applications use a hooking mechanism (e.g., SetWindowsHookEx()) to capture keyboard data. Vendors often package solutions, like Perfect Key logger, as an executable or a DLL (Shetty, 2005).

Pc_Snooper has many modules and each module having its own functions. It is independent software and it tracks all user details, if the user is not an authorized one. Pc_Snooper is designed to monitor a computer, email use of its users, key press events and also the programs and process that are accessed by the users of a particular computer.

This paper discuss about a method that monitor a PC only when intruders or attackers log-on in to a system. Overall working is as follows. Admin /owner of PC can set 'Priority' in Pc_Snooper. Priority means that who can use a particular PC. Since admin is the only person who has privileges to access Pc_Snooper, nobody can change the priority. In order to protect a PC from unauthorized persons, admin/owner can decide who all has to use a particular PC. At the installation time of Pc_Snooper software in to a PC, the priorities can be set. There are 3 priorities.

A. High
B. Medium
C. Low

Before going to discuss about different priorities, let's mention the face recognition module once again. The admin/owner of a PC can decide which persons can use the PC. So that the face's of persons who are allowed to use a PC should be trained first. The trained face is saved in to a file along with name as 'owner name'. Owner name refers to the name of person who is allowed to use a particular PC. Then at the log-in time, face of the person who tries to

log-in is compared with the trained images. If the face is recognized and the owner name is matched then only log-in process completes. Now check how the 'priority' of Pc_Snooper protects a PC.

A. *High*

If the priority is high, then at the log-in time of user itself, face recognition process starts. If the detected face is matched with the face that is already trained by the admin and if he/she is the current owner of PC, then log-n is completed. If an intruder/attacker came in front of PC and tries to log-in, then the face intruder is compared with trained faces. No match is found and at that time itself PC gets log-off. This means if the priority is high, then allotted users can only use a particular PC. If any other tries to log-in, within 10 seconds, PC gets log-off. So in high security areas, in order to protect a PC from unwanted access, 'High' priority can be set.

B. *Medium*

Everybody can use a PC as his/her wish. But if the user is not a legitimate one, then at the log-in time itself, when he/she comes in front of computer Pc_Snooper awake. Then all the user activities are tracked and recorded in to a log file. Whenever the authorized user/or the owner of that particular PC come in front of the computer, Pc_Snooper went to sleep. That means no tracking of user activities if the user is an authorized one and the current owner. Also an e-mail is sent to the original owner, whenever an intruder tries to log-in. Email contains all the log details that the intruder has done in the PC at a particular time. Admin/owner can set the time interval for sending email about the intruder data. Thus if the priority is 'medium' Pc_Snooper is responsible for tracking only unauthorized persons log activities.

C. *Do Nothing*

Everybody can freely use PC, without any fear of tracking. By setting the priority a PC can be secured. This has applications in high security areas and also in personal computers. Since every laptop has webcam, this application is easily implemented in laptops.

V. WEB MODULE FOR VIEWING INTRUDER LOGS

Admin/owner of a particular PC or a particular network can view all intruder details from anywhere using the web module. Log-in of admin is secured by shoulder surfing resistant graphical password scheme. After log in admin can view all recorded data of intruders by choosing date and time. Also webcam images and screen shots of every PC that are attacked by intruders can be viewed by admin by selecting the MAC addresses of PC in a network. Thus details regarding unauthorized access can be easily monitored and eliminated.

VI. CONCLUSION

This paper proposed a method for securing Pc from unwanted access through face recognition. As though face recognition is a complex task, the system uses OpenCV libraries for Local Binary Pattern as face recognizer. Continuous user authentication is provided for finding out intruders and prevents them from using a PC. Along with face recognition system, software named Pc_Snooper is used for tracking and recording user activities if the user is an intruder. Different priorities in Pc_Snooper are a very useful metric for allocation of Pc to users. This has application in many areas as in defense, aerospace, personal network etc. Also in luxurious vehicles this method can be implemented. So that robbery of vehicles can be prevented by setting priority for vehicle owners. Continuous authentication is the main part of the proposed framework, as single authentication has many disadvantages.

REFERENCES

[1] A. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. IEEE Trans. CSVT, 14(1):4 – 20, Jan. 2004.
[2] P. Bours. Continuous keystroke dynamics: A different perspective towards biometric evaluation. INFORMATION SECURITY TECHNICAL REPORT, 17:36–43, 2012.
[3] A. Altinok and M. Turk, "Temporal integration for continuous multi-modal biometrics," *Multimodal User Authentication*, pp. 11-12, 2003.
[4] L. Allano, B. Dorizzi, S. Garcia-Salicetti, "Tuning cost and performance in multi-biometric systems: a novel and consistent view of fusion strategies based on the Sequential Probability Ratio Test (SPRT)", Pattern Recognition Letters, Volume 31, Issue 9, pp. 884–890, 2010.
[5] S. Ojala, J. Keinanen, J. Skytta, "Wearable authentication device for transparent login in nomadic applications environment," *Proc. 2nd In-ternational Conference on Signals, Circuits and Systems (SCS 2008)*, pp. 1-6, 7-9 Nov. 2008.
[6] Yi-Lun Chen, Wei-Chi Ku*, Yu-Chang Yeh, and Dun-Min Liao*," A Simple Text-Based Shoulder Surfing Resistant Graphical Password Scheme*," in IEEE 2nd International Symposium on Next-Generation Electronics (ISNE) - February 25-26 , Kaohsiung , Taiwan
[7] F. Monrose and A. D. Rubin, "Keystroke dynamics as biometrics for authentication," *Future Generation Comput. Syst.*, vol. 16, pp. 351–359, 2000.
[8] A. Altinok and M. Turk, "Temporal integration for continuous multimodal biometrics," in *Proc. Workshop on Multimodal User Authentication*, 2003, pp. 131–137.
[9] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verification using multimodal biometrics," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 687–700, Apr. 2007.
[10] A. Azzini, S. Marrara, R. Sassi, and F. Scotti, "A fuzzy approach to multimodal biometric continuous authentication," *Fuzzy Optimal Decision Making*, vol. 7, pp. 243–256, 2008.
[11] A. Azzini and S. Marrara, "Impostor users discovery using a multimodal biometric continuous authentication fuzzy system," *Lecture Notes in Artificial Intelligence*, vol. 5178, pp. 371–378, 2008.
[12] H.-B. Kang and M.-H. Ju, "Multi-modal feature integration for secure authentication," in *Proc. Int. Conf. Intelligent Computing*, 2006, pp. 1191–1200.
[13] C. Carrillo, "Continuous Biometric Authentication for Authorized Aircraft Personnel: A Proposed Design," Master's thesis, Naval Postgraduate School, Monterey, CA, 2003.
[14] Klosterman and G. Ganger, Secure Continuous Biometric-Enhanced Authentication Carnegie Mellon University, Tech. Rep. CMU-CS-00-134, 2000.

[15] M. A. Turk and A. P. Pentland, "Face recognition using eigenfaces", IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Proceedings CVPR '91.
[16] John Wright, Allen Yang, Arvind Ganesh, Shankar Sastry, and Yi Ma. "Robust face recognition via sparse representation", To appear in IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI), 2008.
[17] Turk.M, and Pentland.A, "Eigenvalues for recognition," Journal of Cognitive Neuroscience, vol. 13, no. 1, pp.71-86, 1991.
[18] P. Sinha, B. Balas, Y. Ostrovsky, and R. Russell, "Face recognition by humans: Nineteen results all computer vision researchers should know about," Proceedings of the IEEE, vol. 94, no. 11, pp. 1948–1962, 2006.
[19] X. He, S. Yan, Y. Hu, P. Niyogi, and H. Zhang, "Face recognition using Laplacianfaces," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, no. 3, pp. 328–340, 2005.
[20] R. L. Hsu, M. Abdel-Mottaleb, and A. K. Jain, "Face detection in color images," IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 696–706, May 2002.
[21] J. Cai & A. Goshtasby & C. Yu, "Detecting Human Faces in Color Images", Wright State University, University of Illinois, 1998.
[22] C. Garcia and G. Tziritas, "Face detection using quantized skin color region merging and wavelet packet analysis," IEEE Transactions on Multimedia Vol.1, No. 3, pp. 264–277, September 1999.
[23] P. Jonathon Phillips, Hyeonjoon Moon, Syed A. Rizvi, and Patrik J. Rauss, "The FERET Evaluation Methodology For Face-Recognition Algorithms", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 10, OCTOBER 2010.
Rabia Jafri and Hamid R. Arabnia, "A Survey of Face Recognition Techniques", Journal of Information Processing Systems, Vol.5, No.2, June 2009.
[24] Alice J. O'Toole, P. Jonathon Phillips, "Face Recognition Algorithms Surpass Humans Matching Faces over Changes in Illumination", ," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, NO. 9, September 2007.