I.J. Information Technology and Computer Science, **2012, 6, 24-29**
Published Online June 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2012.06.04

Robust Security System for Critical Computers

Preet Inder Singh
Department of CSE, Lovely Professional University (Punjab), Phagwara
Email: preetindermail@gmail.com

***Abstract*—**Among the various means of available resource protection including biometrics, password based system is most simple, user friendly, cost effective and commonly used, but this system having high sensitivity with attacks. Most of the advanced methods for authentication based on password encrypt the contents of password before storing or transmitting in physical domain. But all conventional cryptographic based encryption methods are having its own limitations, generally either in terms of complexity, efficiency or in terms of security. In this paper a simple method is developed that provide more secure and efficient means of authentication, at the same time simple in design for critical systems. Apart from protection, a step toward perfect security has taken by adding the feature of intruder detection along with the protection system. This is possible by merging various security systems with each other i.e password based security with keystroke dynamic, thumb impression with retina scan associated with the users. This new method is centrally based on user behavior and users related security system, which provides the robust security to the critical systems with intruder detection facilities.

***Index Terms*—** Thumb impression, Keystroke Dynamics, Computer Security & User Authentication etc.

I. Introduction

1.1 What are critical Systems

Critical systems are systems in which defects could have a dramatic impact on human life, sensitive information, the environment or significant assets. Such systems are expected to satisfy a variety of specific qualities including reliability, availability, security and safety. With the steady infiltration of computers and software in all aspects of our modern world, critical systems increasingly depend on software functionality. These systems are commonplace in many different products, ranging from aircraft systems to home use medical devices. Critical software must be embedded in the critical system/systems. Critical software can also be one element in a system of systems.

1.2 Need of Robust Security to Critical Systems

To protect the sensitive information from the intruder/hackers we need highest level of security for the critical systems. The number of critical computer/systems users and their databases are increasing day by day and robust security becomes the one of the challenging to these computers. Simple password based security system does not provide the robust security to these types of systems because simple password systems has many types of weakness. So, different types of attacks are possible on simplest password based system which is widely used because of its simplicity and easy to use. These are

1. *Phishing.*
2. *Keylogging.*
3. *A brute-force attack on the user's account (i.e. an attacker knows the userID and tries to guess the password).*
4. *A bulk guessing attack on all accounts at the institution.*
5. *Special knowledge or access attacks:*
   - *(a) Guessing based on information about the user.*
   - *(b) Shoulder surfing.*
   - *(c) Console access to a machine where password auto-fill is enabled or a password manager is in use.*

As can be seen, none of the password "best practices" offers any real protection against phishing or key-logging, which appear to be the most prevalent attacks. Strong passwords are just as susceptible to being stolen by a phisher or keylogger as weak ones, and changing the password frequently helps only if the attacker is extremely slow to exploit the harvested credentials. Hence, to overcome this problem the ultimate level of security system is developed.

Computer security has become an important issue in recent times. It has become necessary to control the access to computer systems due to more and more sensitive information being stored on them. Pattern recognition and classification is a technique that can be used to determine that an individual is really who he

says he is. Previous efforts have focused on handwriting analysis to determine the identity of the user, with limited success. More recently, classical pattern recognition techniques have been applied to the individual's typing technique to achieve user identification [l].

The number of computer uses has increased rapidly and so too has the use of internet applications such as e-commerce, online banking services, webmail, and blogs. All internet applications require the user to use a password authentication scheme to make sure only the genuine individual can login to the application. Passwords and personal identification numbers (PIN) have traditionally been used to access such applications [2, 3, 4]. However, it is easy for unauthorized persons to access these systems without detection. In order to enhance such password authentication systems, typing biometrics, known as keystroke, can be used as a transparent layer of user authentication.

The conventional security system can be shown in figure - 1 given below. The user which has the ID and corresponding password can easily logon to the computer system and access the resources [9].

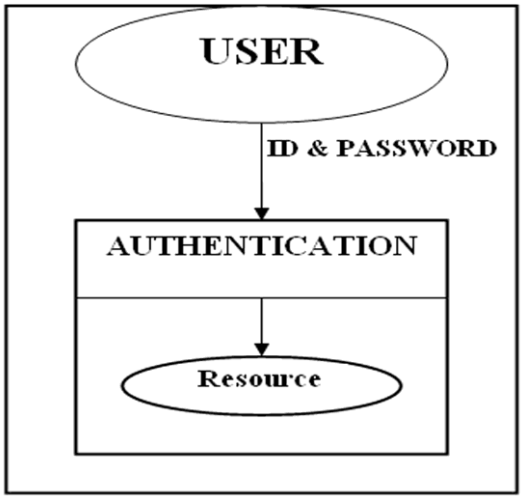

Figure 1: Conventional Security System

Due to the deficiencies in traditional password-based access methods/Security systems, the new security system comes into existence which provides higher level of security is the Keystroke biometrics, which seeks to identify individuals by their typing characteristics [15].

The idea of keystroke dynamics for recognition has been since World War II [5]. Operators were able to easily identify the sender from their key rhythms. Since then, many adaptations of this phenomenon have been studied. Keystroke dynamics is a process of analyzing keyboard typing characteristics or keyboard typing rhythms by monitoring keyboard inputs [6-8]. In other words, the system verifies how a person types. Keystroke verification techniques can be categorized as either static or continuous. Static verification system approaches study keystroke characteristics at a specific time.

Two widely used features are duration of the key time interval that key remains pressed, and keystroke latency time interval between successive keystrokes. A more robust way is to use a combination of these features to analyze a keystroke system. Time accuracy, trials of authentication and classifiers are other examples of ways to analyze a keystroke authentication system [10-12].

If the passwords are too simple and have meanings, they are easy to remember but vulnerable to attacks which use password cracker programs. If the passwords are more complex and random, they are difficult to remember and hence users have to write them down. In either case, the security of the systems is degraded.

Passwords typed at a keypad are easily observed or especially in areas where attackers could plant wireless cameras or hardware keystroke sniffers. Key loggers capture keystrokes and store them somewhere in the machine, or send them back to the adversary. Shoulder surfing is a well-known method of stealing other's passwords and other sensitive personal information by looking over victims' shoulders while they are sitting in front of terminals or in front of an ATM machine [13].

Biometric technologies are defined as automated methods of verifying or recognizing the identity of a living person based on physiological or behavioral characteristics [7]. Biometrics technologies are gaining popularity due to the reason that when used in conjunction with traditional methods of authentication they provide an extra level of security. Biometrics involves something a person is or does. These types of characteristics can be approximately divided into physiological and behavioral types [14]. Physiological characteristics refer to what the person is, or, in other words, they measure physical parameters of a certain part of the body. Some examples are Fingerprints, Hand Geometry, Vein Checking, Iris Scanning, Retinal Scanning, Facial Recognition.

Keystroke dynamics is considered as a strong behavioral Biometric based Authentication system [16]. Keystroke Dynamics is one of those subtle technologies that will raise the bar on access security without users ever knowing it.

The figure - 2 below shows where Keystroke Dynamics falls with respect to physical biometrics such as finger-print and other behavioral biometrics [17].

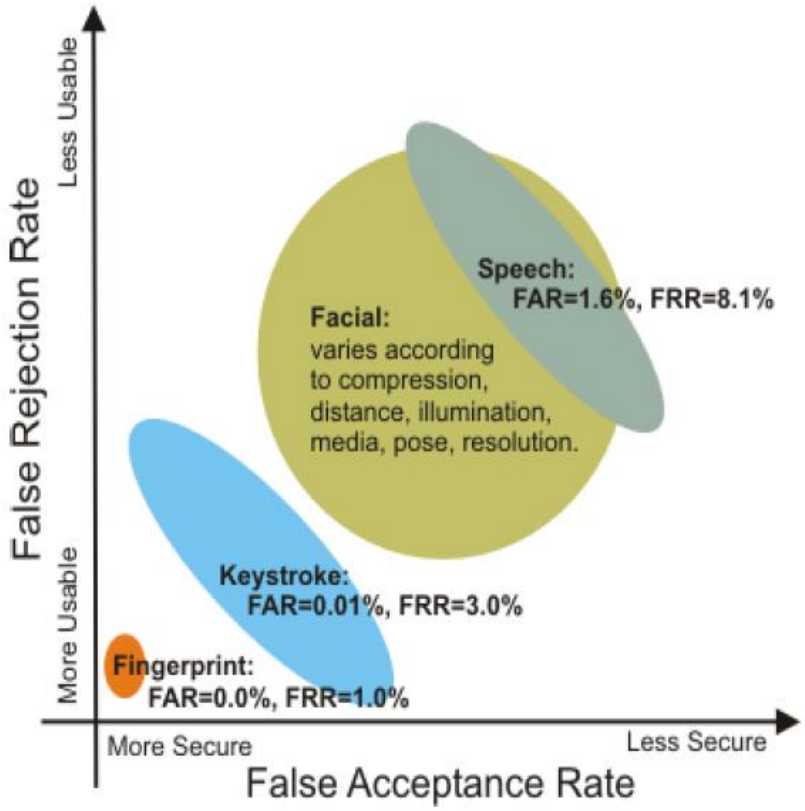

Figure 2: Keystroke Dynamic with other Behavioral Biometrics

As user-system interaction takes place via the biometric sensor, attacking the device that captures the biometric becomes the first obvious point of attack. Systems that can imitate biometrics have successfully been used for this purpose while instructions on how to create prosthetic fingers can already be found on the internet [18]. The success of attacks using prosthetic fingers is crucial from a security standpoint; researchers from Japan have demonstrated a success rate in attacks on such biometric devices in the range of 67-100% [20]. The major factor that determines the success rate of the attacks was found to be the quality of the original print. There are of course some biometric systems that can be enriched by incorporating aliveness detection methods but those cost significantly more while most current commercially available aliveness tests can be easily cheated [20].

The working of the biometric device is shown below in the figure–3. From the biometric sensors features are extracted and matches with the DB/Template according to which the decision can be made.

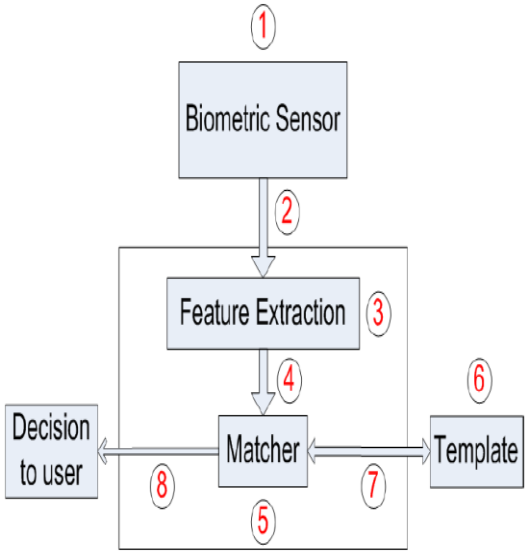

Figure 3: Working of Biometric Sensor/device

The remainder of this paper is organized as follows: Section 2 gives Proposed Security System for Critical Computers. Section 3 presents the Experimental results and advantages of the proposed system. Conclusion is given in the final section.

II. Proposed Security System For Critical Computers

In this proposed security system we are merging the different security techniques with one another to provide the robust security system for critical computers. No one single security system/technique is fully (100%) secured. Hence, to protect the critical computers from unauthorized users we merge the different security systems/techniques with one another to provide the robust security with intruder detection facility specially for critical computers like servers, Network administrator Computers in the organizations, Colleges or Universities.

2.1 First Level of Security to Critical Systems

The first level of security to the critical systems is the user ID and Password which is widely used for many years because of its simplicity and easy to use. The password should be long enough so that it is difficult for the intruder to guess or crack. The strength of the password depends upon the length of the password as well as its entropy. For example, User that chooses a password of 7 characters is said to provide between 16 and 28 bits of entropy.

2.2 Second Level of Security to the Critical Systems

The second level of security to the critical systems is to merge the Password with the keystroke dynamic, which is the behavior keystroke biometric system. . It a process of analyzing keyboard typing characteristics or keyboard typing rhythms by monitoring keyboard inputs. It analysis how you type but not what are you typing.

If the user enters the correct Password and typing behavior of the user matches with the existing pattern, then the system allows to enter into the next level of security otherwise the system does not allows the user to enter into the next level of security. The level of security can further be enhanced by locking the system after five failed login attempts and corresponding log file can be maintained at the backend helping the authored user to detect/find the intruder.

Now, to unlock the critical system, the level of security can be further be enhanced by demanding the additional key, that key may be the person date of birth or any other secret key. Hence, by merging the password with the keystroke dynamic the security strength of the critical systems can be increased.

2.3 Third Level of Security to the Critical Systems

The third level of security comes into play after the correct Password corresponding to ID, and by matching the user typing behavior at real-time. In this level the user thumb impression as well as the retina will be scanned by the Biometrics device/sensors. Again if it matches with the existing record/database, the user login is successful to the critical system and can access the system resources. If the user thumb impression and retina will not be matched the user login to the system fails and cannot access the system resources.

This level of security is very critical. Many biometric devices/sensors available in the market do not detect the aliveness of the persons/user which uses the biometric device. Hence, to achieve highest level of security we (Administrator) require special biometric device that can also check the aliveness of the user.

2.4 Forth Level of Security to the Critical Systems

After the successful login to the system the forth level of security comes into play. This is active only if the user wants to perform the critical operation on the critical system like update transaction/entry, write transaction/entry. So, at the time of updating operation and/or write operation can be performed by the user, the system needs the additional secret key which includes the minimum 8 characters with constraints like one special character, one upper case character, one digit.

Hence, by using the above levels of security, the security of the critical systems can be increased as shown in figure-3 below.

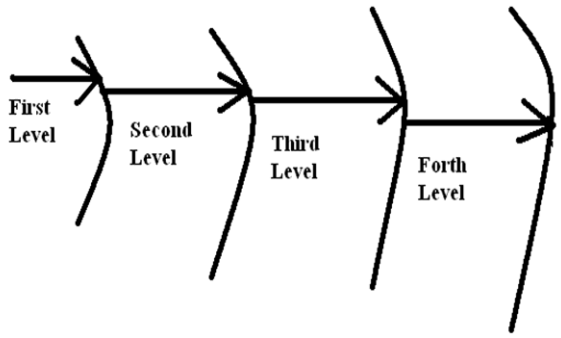

Figure 3: Levels of Security to Critical computer

III. Experimental Results

3.1 Data collection and Analysis

According to specified description of logical parameters as discussed below “300” readings from users have been taken in Visual Basic 6.0 as a front end and Microsoft Access 2003 as a backend by merging it with high quality biometric device (that check the *aliveness* of user) and it is found that to break the password with these *logical parameters* by *merging* it with b*iometric device* is impossible. It is also found that using these parameters the security of the simple password based system based on the user behavior is increased very much because it contains the multiple logical parameters as discussed below.

1. Password Length.
2. Number of trails.
3. Total time to enter the password.
4. Average time to enter the whole password.
5. Status means login is done or not.
6. Time difference between the two passwords if in the first attempt login is not done/successful.
7. Deviation from the current/actual password.
8. Length difference from the current/old attempt password.
9. If the password/Character is in the capital letter whether Shift key is used or not.
10. If the password/Character is in the capital letter whether Caps Lock is used or not.

3.2 Advantages of this proposed system

In summary the critical security system given in this paper having advantages like: -

a) Easy to deploy on the critical systems.
b) Provides the intrusion detection facility.
c) Can be implemented in wide range of applications where security is the primary factor.
d) Free from service provider faith ness circumference.
e) Check the aliveness of the user by using the high quality biometric device. Hence, security is further enhanced.
f) Hierarchical protection gives optimum use of security model with high processing speed.
g) It provides multi-user facility from same security environment.
h) Account can be protected by allocating the maximum number of attempts/trials to the user by locking the account, when login to account is un-successful. Hence, provides better security.
i) Logging of biometric access creates better forensic evidence; and can deter many internal threats to network security.
j) This technology does not require changes to existing network access policies; it more effectively enforces these policies.
k) This technology provides better audit control and promotes proper use of application licensing.
l) Provides high level of prevention from unauthorized access to resources and critical parts/sections of the system.
m) It is very difficult to break this security setup because it is depending upon multiple levels of security systems merging with each other.

IV. Conclusion

This new method provides the robust security to the critical computers where we need the highest level of security by merging all the security systems with one another. It can be implemented into wide range of applications where security is the primary factor. This technology does not require changes to existing network access policies; it more effectively enforces these policies and provides better audit control and promotes proper use of application licensing. Hence with these levels of security system the ultimate level of security to the critical systems can be achieved.

References

[1] S. Bleha and M. S. Obaidat, “Dimensionality reduction and feature extraction applications in identifying computer users,” *IEEE Trans. Sys. Man. Cybem.*, vol. 21, pp. 452-456, Mar./Apr. 1991.

[2] Jain, A. R. a. A. "Information fusion in biometrics." Pattern Recognition Letters, 24(13), pp. 2115-2125, (2003).

[3] U.Dieckmann, R. W. F. a. "Bioid: A multimodal biometric identification systems." IEEE Computer, 33(2), pp. 64-68, (2000).

[4] F. Monrose, a. D. R. "Keystroke Dynamics as a Biometric for Authentication." Future Generation Computing Systems (FGCS), 12(12), pp. 351-359, (2000).

[5] Checco, J. C. “Keystroke dynamics & corporate security”. WSTA, 241 Maple Avenue, Red Bank, NJ 07701, 2006.http://www.wsta.org/publications/articles/1003_article06.html

[6] Davide Maltoni, D. M., Anil K.Jain, Salil Prabhakar Handbook of fingerprint recognition. New York: Springer, (2003).

[7] Anil K. Jain, Arun Ross, and Salil Prabhakar, "An Introduction to Biometric Recognition." IEEE Transactions On Circuits And Systems for Video Technology, 14(1), pp. 4-20, (2004).

[8] F. Monrose, a. D. R. "Keystroke Dynamics as a Biometric for Authentication." Future Generation Computing Systems (FGCS), 12(12), pp. 351-359, (2000).

[9] Preet Inder Singh, Gour Sundar Mitra Thakur, "Enhanced Password Based Security System Based on User Behavior Using Neural Networks" International Journal of Information Engineering and Electronic Business (IJIEEB), vol. 4, no. 2, pp.29-35, 2012.

[10] Modi, S. K., & Elliott, S. J., ”Keystroke Dynamics Verification Using Spontaneously Generated Password”, 40th IEEE International Carnahan Conferences Security Technology. Lexington, Kentucky, (2006).

[11] R. Stockton Gaines, William Lisowski, S. James Press, and Norman Shapiro "Authentication by keystroke timing: Some preliminary results". Rand Report R-256- NSF, (1980).

[12] Arau jo, L.C.F., Sucupira Jr., L.H.R., Lizarraga, M.G., Ling, L.L., Yabu-Uti, J.B.T., "User authentication through typing biometrics features". IEEE Trans. on Signal Processing, 53 (2), 851–855, (2005).

[13] J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better Authentication," presented at Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota, USA, 2002.

[14] Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Proceedings of the IEEE, Vol. 91, No. 12, Dec, pp. 2019-2040, 2003.

[15] A. Peacock, X. Ke and M. Wilkerson, "Typing patterns: A key to user Identification", IEEE Security and Privacy 2(5) (2004).

[16] Ahmed Awad E. Ahmed, and Issa Traore, "Anomaly Intrusion Detection based on Biometrics", Proceedings of the IEEE, 2005.

[17] John C. Checco," Keystroke Dynamics and Corporate Security", 2003.

[18] Arndt, C. (2005). The loss of privacy and identity, Biometric Technology Today.

[19] Matsumoto, T., H. Matsumoto, et al. (2002). Impact of Artificial Gummy Fingers on Fingerprint Systems. Optical Security and Counterfeit Deterrence Techniques IV, Proceedings of SPIE.

[20] FIDIS (2005). D3.2: A study on PKI and Biometrics. M. Gasson, M. Meints and K. Warwick**:** 1-138.

Preet Inder Singh: M.Sc computer Science from D.A.V College, Amritsar in 2010. Currently pursuing M.Tech (CSE) from Lovely Professional University, Phagwara, interested in Network Security, Multi-media and Artificial Intelligent Systems.

