The 8th International Conference on e-Business (iNCEB2009)
October 28th-30th, 2009

A HIGH QUALIFICATION BIOMETRIC FOR MOBILE INTRUDER DETECTION

P. Phoorivatana and P. Bhattarakosol

Department of Mathematics, Faculty of Science
Chulalongkorn University, Bangkok, 10330, Thailand
E-mail: premchai.p@student.chula.ac.th, pattarasinee.b@chula.ac.th

ABSTRACT

The security problem of the stolen mobile and data is an unsolvable for years. Numerous techniques have been proposed but the limitations to implement and maintain are the big issue that cause problem unsolved until now. Since biometric is one of the most popular indicators that is applied to the protection mechanisms, there are some uncompleted features that cause the system unsecured. Thus, this paper proposed the use of a biometric value, measured when the owner of the device is unlocking the system; this biometric is the time interval of the password entering. The experiment is drawn and the analysis process determines that this biometric is a high qualified indicator because the accuracy of the intruder detection is up to 90%.

Index Terms— Time interval, Biometrics, Authentication

1. INTRODUCTION

From the report of SOPHOS in the year 2008, in every 5 seconds, the average number of infected web pages is more than 15,000 sites which is three times more than the year 2007 [1]. This number indicates that the security of information is very loose although the Internet is counted as the main information resources of human and various researches have proposed the security techniques to protect such information.

Currently, there are various types of devices that have been developed as gateways to the Internet access; one of those types is the mobile device. Therefore, the intrusion from the Internet world will affect to the mobile device as an unavoidable issue. Thus, the mobile protection mechanism must be implemented in order to protect data in the mobile storage.

One weak point of the mobile phone is that the data can be accessed whenever a mobile holder passes the authentication process, if existed. The truth is that most of the mobile holders do not use passwords to lock their mobiles because of difficulty to remember. Therefore, when a mobile was stolen, all data in that mobile will be eliminated or accessed without permission. Thus, every mobile phone should be implemented with an automatic authentication technique that will not cause superfluous process to the owners.

The objective for the authentication technique is to identify something or someone. Nevertheless, traditional authentication techniques, like a password or hardware token, have vulnerabilities. For example, the legacy password locking technique is easily being broken, many techniques like dictionary attack or man-in-the-middle attack could be used to steal it without trouble. Therefore, the biometrics approach has been proposed to use in the authentication process in many researches. Based on various biometrics studies and researches, more than 90% of accuracy is claimed for the uniqueness [2].

The biometrics can be classified into two distinct categories: physiological biometrics, and behavioral biometrics. The physiological biometrics involved the physical human body, such as face recognition, fingerprint recognition, iris scanning and vein checking; the behavioral biometrics deal with human manners, such as gait recognition, keystroke dynamics, signature analysis and voice verification. These entire biometrics data have both strong points and weak points. For instance, the gait recognition which characterizes individuals by the way they walk can be influenced by weight, health condition, emotion, cloths, shoes etc. Thus, the measurement may give inaccurate results [3]. So, this paper proposes a new measurement biometrics using only the response time to enter password of each person and uses this time to indicate the owner of the mobile phone in the authentication process.

Based on various researches in biometric related to the authentication process, the summarization of these researches is in Section 2. Section 3 is the proposed authentication method using the response time as an identifier of mobile owners. Then, experiments to examine the proposed mechanism is performed and described in Section 4. The results of this experiment and is elaborated in Section 5. In Section 6, the comparison between the existing method that uses only the password lock and the proposed method will be elaborated. Finally, discussion and conclusion are drawn in Section 7 and Section 8 respectively.

2. RELATED WORK

In the research articles by (Anil K. Jain, 2004), it had mentioned that the biometrics is not secret; thus, if the invader has a ready knowledge of the information in the legitimate biometric identifier, they could fraudulently inject into the biometric system to gain access [4]. Therefore, even biometrics themselves are quite distinctive data, but lacking in the data security.

As a consequence, an identification system combined with fingerprint and cryptography is addressed according to the vulnerabilities of using the individual biometric information. This technique was proposed by (Hao Li and Peishun Liu 2006). The result of combining the fingerprint biometric technique with the encrypt password method can enhances the security of fingerprint reader from the fake fingerprint attacker which is the serious concern [5].

Additionally, Davrondzhon and Einar [6] investigated the robustness of the gait authentication system against attackers rather than evaluating the performance of individual attackers. Furthermore, they claimed that the biometrics information is easily to attain. Thus, various types of imposters aim for this weakness point.

Another concerning in biometrics authentication technique is the measurement procedures. In the research of brain signatures [7, 8] shows that the EGG signals from the human brains can be used as alternative biometrics. Also, the authors indicated that their method has 97% accuracy. On the other hands, even their techniques provide high rate of reliability, the measurement devices and process are too complicated for handy digitizer tablets which confirmed by Kiran and Kunte [9] whose proposed the online-signature verification system using probabilistic feature modeling. They stated that their method analyze human signature for authentication is appropriated for many small size devices, such as palm and mobile phone.

Referring to researches mentioned above, most authentication methods that applied biometrics values have not been implemented in a practical way. Therefore, this paper proposes an authentication method that can be easily implemented and applicable for all sizes of devices, not only the mobile phone. The proposed mechanism is described as follow.

3. PROPOSED AUTHENTICATION METHOD

Since there are numerous biometrics and they are popular identifier that are used to identify a person, various biometrics are applied to find the best and accurate identifier. One popular biometric is the use of fingerprint and voice recognition to identify persons. Unfortunately, these two techniques cannot perfectly prevent the intruder when they intrude the system. Therefore, a fundamental method which is the use of password is still remained in the authentication system.

Nevertheless, until now there is research focuses in the difference of time interval when a password was entered by the owner and unauthorized persons. Thus, this paper intends to prove that there is a difference between time interval of password entered by the owner and intruders.

The main idea for the authentication technique is that the time interval when a password or a phase is entered by the owner must be different from the time interval measured when intruders enter the password or the phase of others.

For example, if A is the owner of a mobile phone X, then the time interval when A enters a password to unlock X will be $T(A)$. Then, when an intruder, B, enters A's password to unlock X, the time interval for this entering will be $T(B)$. The assumption for this authentication process is that $T(A)$ will always be different from $T(B)$.

Since people uses their devices several times, the time interval that is used to identify the owner is the average time interval measured in a time limit from time to time. The strength of this technique is that people are normally not change the rhythm of their movement, especially their fingers and thought. Thus, the time interval of an authenticated person will not be changed and cannot be emulated easily. In order to proof the accuracy of this authentication mechanism, the experimental process is performed and described in the following section.

4. EXPERIMENTAL PROCESS

This section describes the feasibility of the biometric authentication process using the response time. The details of the experimental are elaborated as follow.

4.1. Data Gathering

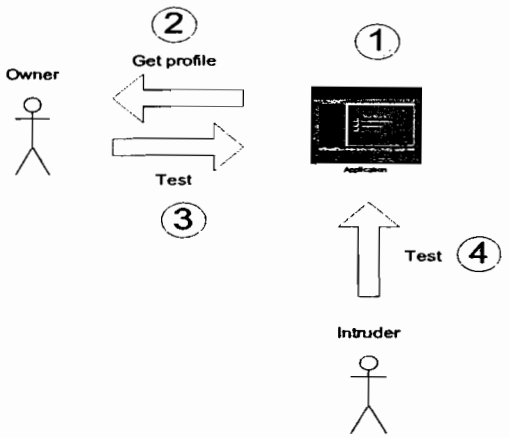


Figure 1. The data gathering process

From Figure 1, there are 4 steps in the data gathering process. In addition, there are two groups of samples: the owner group and the intruder group. The number of samples in the owner group is 30 persons while the intruder sample size is 100 persons.

The first step is the implementation of collecting application. This application is the implemented on the Microsoft Excel and consists of three sheets. The first sheet is used for interacting with samples. On the second sheet, it is used as the database of questions and answers which filled by samples. The last sheet contains the information of the

response time collected though the first sheet. Figure 2 shows all three sheets in the excel file and the algorithm to capture the time interval to the profile sheet is shown in Figure 3.

In the second step, samples in the owner group choose their own questions and passwords and record via the second sheet in the application. These questions and passwords are unlimited for each sample, but the number of questions and passwords must be larger than one. Moreover, there is no boundary for setting up the category of questions. Thus, all samples have freedom to enter whatever they prefer as same as real life.

After entering their profiles, the testing for finding time interval will be measured when a question from the profile is random by the implemented application and the owner enters the answer. This random process will be repeated 40 times per owner.

The last step for gathering data is to capture time interval of the intruders. In this process, samples in the intruder group must enter answers for all random questions of others and entering time will be measured and recorded. This process is repeated 20 times per person.

4.2. Extracting Features

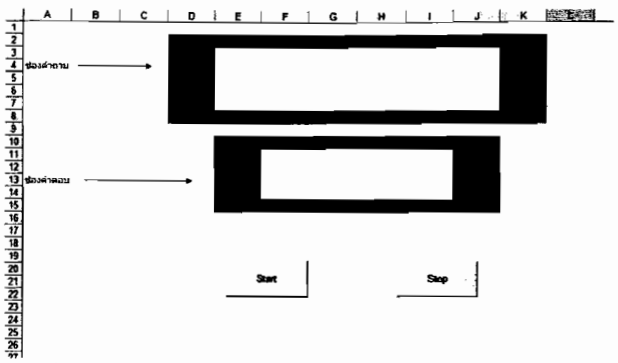
After obtaining all sample data, the data of the owner group will be separated into two subgroups. Each subgroup has all 30 owners, and randomly selects 20 time intervals for each owner. The first subgroup is used as the owner profile; the second group is used as the test profile to indicate the sample in the owner group, see Figure 4.

Based on the bias elimination method, the maximum and minimum values of time intervals will be eliminated before entering the analysis process. Thus, all outlier values will also be removed.

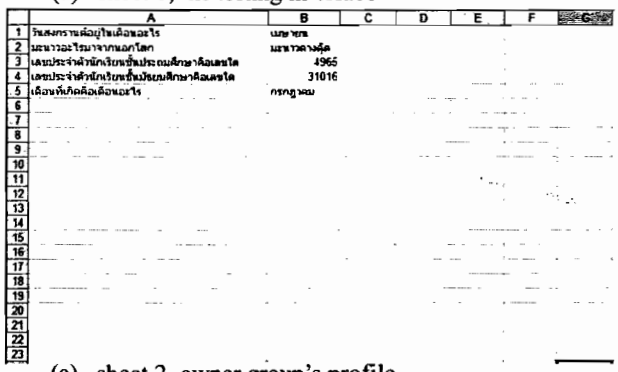
4.3. Analyzing Features

In the analysis process, there are two assumptions to be proved. The first assumption is to prove that the mean values of two subgroups separated from the same owner group are not significant different. This result will indicate that the entering time of a person will not be changed.

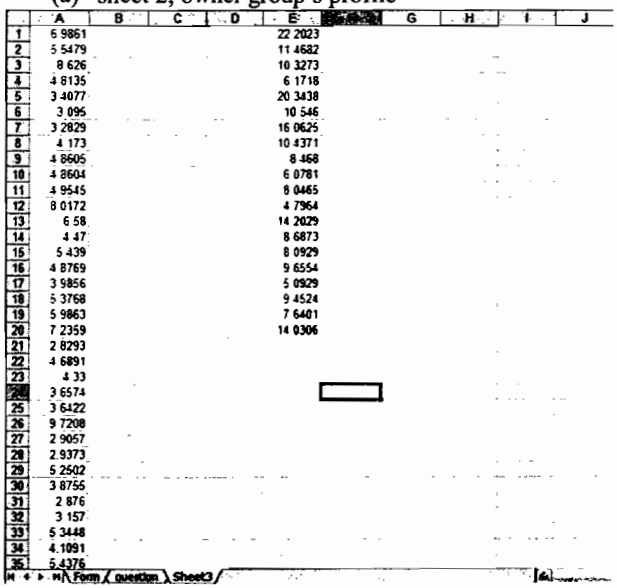
The second assumption is to prove that the mean values of the entering time interval of the owner group is different from the time interval of the intruder group. This result will indicate that persons cannot emulate other persons' behaviors although they know the answer to enter.



(a) sheet 1, the testing interface



(a) sheet 2, owner group's profile



(a) sheet 3, time collection values

Figure 2. Three sheets of the Microsoft Excel file

```
Sub Button1_Click()
   Sheets("Question").Select
   Range("A1").Activate
   Range(ActiveCell, ActiveCell.End(xlDown)).Select
   xx = Selection.Rows.count
   Randomize
   x = Int((xx * Rnd) + 1)
   count = "A" & x
   countans = "B" & x
   qst = Range(count).Value
   ans = Range(countans).Value
   Sheets("Form").Select
   ActiveSheet.Shapes("Question").Select
   Selection.Characters.Text = qst
   ActiveSheet.Shapes("Answer").Select
   starttime = Timer
Sub Button2_Click()
   ActiveSheet.Shapes("Answer").Select
   z = "" & Selection.Characters.Text
   If z = ans Then
      endtime = Timer
            anstime = Format(endtime - starttime,
"000.0000")
```

Figure 3. The time interval capturing algorithm

The statistical value for this analysis process is the *t*-value using *t*-test because *t*-test allows two groups comparison of mean values based on equal and unequal variances. Both tests run with the confident level of 95%.

Firstly, the variances between groups must be tested. According to the separation of the owner group, the subgroups have equal variance with *p*-value=0.0878 > α=0.05. Thus, a statistical value to confirm the consistency of owner's behavior is calculated using *t*-test with equal variance.

Referring to Figure 4, two subgroups from the owner group profile are compared, a statistical value, *t*-value, is calculated. The result shows that owners will not change their behavior when press keyboard to answer the questions; thus, the mean time interval of the same person is not significant different in any time with p-value=0.1159 > α=0.05.

Before testing the difference between mean time interval of the owner group and the intruder group, the variances of these two groups must be evaluated; the result determines that variances of these groups are significant different with p-value=0.0049 < α=0.05. So, the calculation to confirm the difference between the owner and the impostors is the t-value obtained from t-test under unequal variance condition.

Based on the comparison of mean values shows in Figure 5, two sets of data from the owner group, 20 time intervals of 30 samples, and the intruder group, 20 time intervals of 100 samples are calculated for a statistical t-value. The outcome of this calculation confirms that there is a significant difference between the mean time interval of the owner group and the intruder group with p-value=0.0179 < α=0.05.

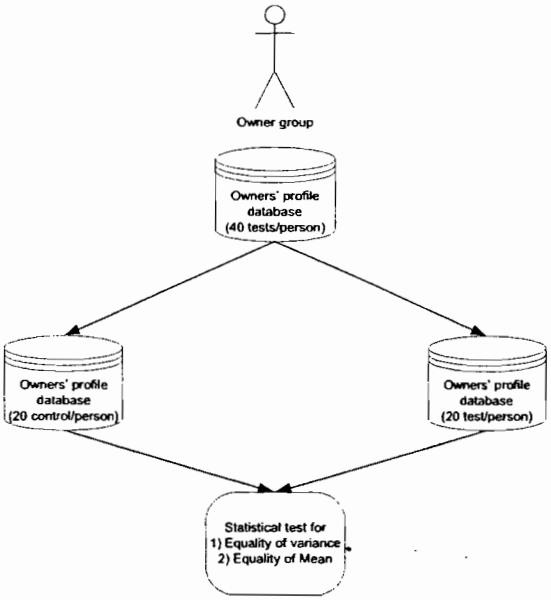


Figure 4. Testing process within the owner group.

5. RESULTS

As a consequence of the statistical value in the previous section, then the time interval which is a biometric value can be applied to identify a person. However, in order to ensure such assumption, the pair test has been performed for each person by comparing the mean time interval of each person with the mean time interval of intruders who would like to hack his/her system. The result has shown that using the time interval of each owner can detect the unauthorized person with 90% accuracy, as shown in Figure 6.

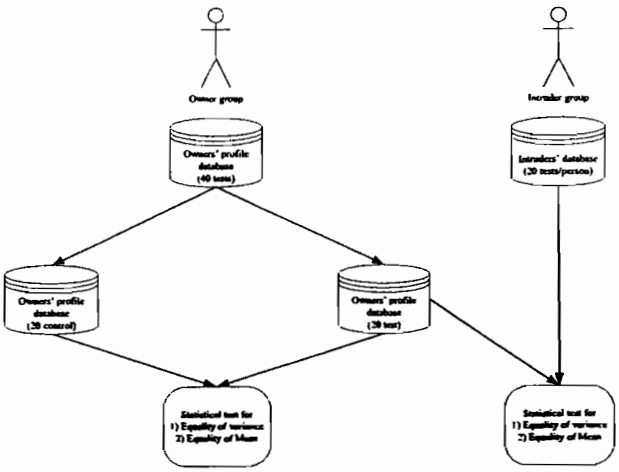


Figure 5. Testing process between the owner group and the intruder group

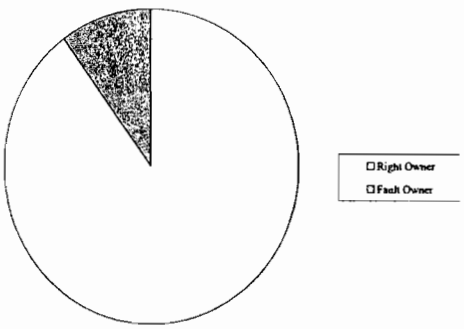


Figure 6. Result of individual testing for mean time interval

6. COMPARISON

From the result of this experiment, the comparison between the proposed method and the legacy system had been performed using the statistical method. The comparison performed by considering the response time value of the new method with the time value of the legacy method. Since the time value of the new method will be measured only when the users put the right password but the time value of the legacy method will be measured only the time when a user enters a password, no matter it is right or wrong. Thus, the comparison of mean time refers to the comparisons between the mean value of times obtained from new method and the mean value of times measured in the legacy method.

In order to prove that there is a significant difference between the owner and the intruder groups, the confident level in this test is 99% and a statistical value, *f*-test has been calculated. The result has shown that there is a significant difference between mean time of the owner and the intruder since p-value = $0.00 < \alpha = 0.01$. Moreover, the calculated time interval of the intruder under the legacy system is (4.22, 4.52) which is totally different from the real time interval of the owner using the new method, (4.59, 4.93). Thus, the new method has high possibility to indicate the right owner of the system.

7. DISCUSSION

In the real world, mobile devices are easily stolen and the data stored in it will be in a risk mode. Therefore, various techniques have been proposed and implemented to protect the unauthorized usages from unwanted persons. One popular technology is to apply the biometric value to be the identifier, or applied as a preventer of the system. However, this biometric is very uncertainty when used. Thus, choosing the right biometric value is a challenge research. This paper proposed a time interval obtained during the owner of the mobile devices enter the unlock password or phase. The difference between the proposed method and other protection using biometric values is that this method is simple, easy to be implemented, and more significantly, the mean time interval for entering password of each person has been proved that this value is independent from the occasion and situation of the usage. Thus, there is a high possibility to implement this technique to any mobile devices with low cost of investment and maintenance but the quality and security of information is guaranteed and maintained.

8. CONCLUSION

Security of data stored in the mobile storage is very vital in some situation. Therefore, protecting the mobile devices from intruders or unauthorized accesses is the main issue that all mobile owners must be concerned. Although various researches have proposed methods and algorithms to protect both mobile devices and data, most of those can be obtained by high investment cost, problems in technological transfer, and some special equipment might have to be installed. Thus, this paper proposes a new simple technique using a biometric information occupied when the mobile's owner enter the password or phase to gain access to the system and data. The experiment and analysis results have shown that the selected biometric proposed in this paper is the suitable metric that can indicate intruders of the system with 90% correctness. Moreover, the simplicity of this method can apply to every device that needs to be authenticated before use.

9. REFERENCES

[1] SOPHOS: security threat report //Q1 08 http://www.sophos.com

[2] Rodwel PM, Furnel SM, Reynolds PL. "A Non-Intrusive Biometric Authentication Mechanism Utilising Physiological Characteristics of the Human Head", Computers & Security (2007), doi: 10.1016/j.cose.2007.10.001

[3] Kale, A.; Roychowdhury, A.K.; Chellappa, R., "Fusion of gait and face for human identification," Acoustics, Speech, and Signal Processing, 2004. Proceedings. (ICASSP '04). IEEE International Conference on , vol.5, no., pp. V-901-4 vol.5, 17-21 May 2004.

[4] Jain, A.K.; Pankanti, S.; Prabhakar, S.; Lin Hong; Ross, A., "Biometrics: a grand challenge," Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on , vol.2, no., pp. 935-942 Vol.2, 23-26 Aug. 2004.

[5] Hao Li; Peishun Liu, "An Identification System Combined with Fingerprint and Cryptography," Computer and Computational Sciences, 2006. IMSCCS '06. First International Multi-Symposiums on , vol.2, no., pp.105-108, 20-24 June 2006

[6] Gafurov, D.; Snekkenes, E.; Bours, P., "Spoof Attacks on Gait Authentication System," Information Forensics and Security, IEEE Transactions on , vol.2, no.3, pp.491-502, Sept. 2007

[7] Hema, C.R.; Paulraj, M.P.; Kaur, H., "Brain signatures: A modality for biometric authentication," Electronic Design, 2008. ICED 2008. International Conference on , vol., no., pp.1-4, 1-3 Dec. 2008

[8] Dogaru, R.; Dogaru, I., "Biometric authentication based on perceptual resonance between CNN emergent patterns and humans," Cellular Neural Networks and Their Applications, 2002. (CNNA 2002). Proceedings of the 2002 7th IEEE International Workshop on , vol., no., pp. 267-274, 22-24 Jul 2002

[9] Kiran, G.V.; Kunte, R.S.R.; Samuel, S., "On-line signature verification system using probabilistic feature modelling," Signal Processing and its Applications, Sixth International, Symposium on. 2001 , vol.1, no., pp.355-358 vol.1, 2001