INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)
ISSN 2278 – 7631 (Print)

Theoretical Analysis of User Authentication Systems

Manish Giri
Department Of Computer Science, BUIT, Bhopal, M. P., India
Divakar Singh
HOD of CSE, BUIT, Bhopal, M.P., India

Abstract:
Effective user authentication techniques are used to protect information and system safety. Text password authentication technique is the most common computer authentication method. There are many techniques for user authentication to secure the data and information. In this paper we are theoretical analyzing some authentication techniques with their pros and cons.

Key words*: graphical password, authentication, security, token, biometric*

1. Introduction

Authentication, secure operations and development of secure system; these are the most important areas for human computer interaction [1]. In the paper, our main focus is on authentication problem. Submission of username and text password is the basic authentication process which is not very secure in this era. Researches shows that the remembering the passwords are the main problem with text based password which are either simple name any of person, place, lovable thing or any dictionary word that can be easy to memorize, but these passwords can be easy to guess or break, a cracker can break these passwords by dictionary attack and brute force attacks within 30 seconds [2]. Another password is combination of alphabets, number and special symbols, but this type of passwords are difficult to memorize. Remembering different passwords for different accounts are also very difficult.
In the literature, several techniques have been proposed to overcome the limitations of alphanumeric with special symbol text password technique.

2. Authentication Techniques

There are four types of techniques here we are categorizing

- Text based authentication technique.
- Token based authentication technique.
- Biometric based authentication technique.
- Graphical password authentication techniques.

2.1. Text Based Authentication Technique

Text based authentication technique is simplest and widely used technique. In this, user simply enters their user name and password. User named may be some unique name or any email-id and password may be any combination of alphabets, digits and special symbols.

Figure1 Text Based Authentication

Here User name is unique according to the user or a unique email id. There are different levels of password can be selected according to the user. Simplest password is the combination of alphabets or lovable name of any person, place or things. But it can be easily cracked be hackers easily. To provide difficulty to it, user can make any combination of alphabet, digits and special symbols that is very difficult to gauss by any person. But is hard to memorize but these passwords can easy to guess or break, a cracker can break these passwords by dictionary attack and brute force attacks within 30 seconds [2].

2.2. Token Based Authentication Technique

In these days Token based techniques are widely used, the main examples of the token based technique are the smart cards, ATM card and key cards. These token based authentications techniques also use the knowledge based techniques. For example ATM cards use a PIN number.

Figure 2: ATM Card

But this techniques is also got unsecured because sometimes it happens that all the money of your account has been stolen form the ATM machine where you had got transition from ATM card.

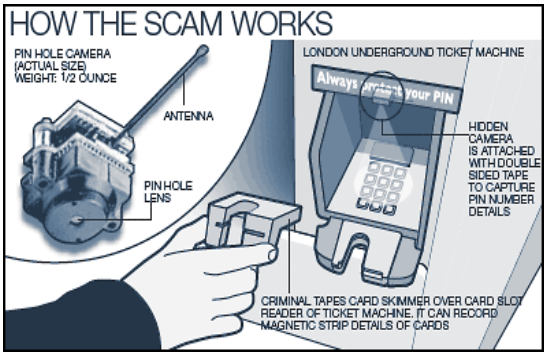

Figure 3: SCAMING Work In ATM

Hackers put a scanner where ATM inserted that scan and copy the ATM code which is encrypted in black magnetic part of ATM card and there is a hidden camera of size 0 and with a little weight about ½ OUNCE is fitted very secretly about the keyboard of ATM machine which copy the users secret password and sent it through small but powerful antenna to the hackers system.

So customer should be very careful when he/she get transition from ATM. Customer should be aware that there is no camera putted in the ATM machine from where you are getting transition and whenever you are entering the password from the keyboard that should be hidden from the hand or fully covered from the body so nobody can watch it outsider.

Figure 4: ATM Password Entering

2.3. Biometric Based Authentication Technique

Examples of Biometric based authentication techniques, such as fingerprints, iris scan, of facial recognition, are not yet widely adopted. The major drawback of this technique is that such systems improvement becomes very expensive [3]. However, this type of approach provides the highest level of security.

Figure 5: Ratina Scanning

Figure 6: Verifying Identity

Figure 7: Thumb Impression

Knowledge based techniques are the most widely used authentication techniques and include both text based and picture based passwords. Here we are using the knowledge based authentication in graphical passwords scheme [4].

2.4. Graphical Password Authentication

Human can remember pictures better than the text based passwords or the combination of alphanumeric with symbolic passwords so the proposal is to graphical passwords are the alternative to the text based password schemes and it is more easy to use and more secure than text based password[5].

First technique is recognition based and second is recall based graphical authentication techniques.

- **Recognition Based Technique**
  In recognition based techniques, user select some images and choose some points or pixel position on the images, at the time of authentication user click on the images, if the clicked points are matched with the right points, then authentication process become success.
- **Recall Based Authentication Techniques**
  Second approach is recall based authentication, in which user create or selected an image which he has selected previously at the time of registration. If the reproduce thing is same as the previous thing the user become authenticated.
  After applying these techniques the result are obtained that 90% of all users successfully authenticated with these techniques,

While only 70% succeeded using text based passwords [4].

3. Security from Password Attacks

3.1. Brute Force Attack

Brute force attack uses an algorithm that produces every possible combination of words to crack the password. Text based password contain 94^N number of space where 94 is the number of printable characters with space and N is the length. It has always proven successful against text based password because of its ability to check all possible combination of password [5]. That's why users are advised to select a stronger and complex password to prevent discovery from brute force attack. However, GUA proves more resistant to brute force attacks because attack software needs to produce all possible mouse motions to imitate passwords especially when trying to recall the graphical passwords [5].

3.2. Dictionary Attack

If any user uses a weak password that can be crack by dictionary attack after checking the word found in dictionary. Dictionary attack on GUA would be waste of time because graphical password is a method of using mouse input type recognition [6]. It is more difficult and complex to use the automated dictionary method to produce all possibility of a single user click of an image in recall based password attack than a text based attack [6-8].

3.3. Spyware Attack

This type of attack uses a small application which installed on a user's computer accidentally or secretly to record sensitive data during mouse movement or key press. This is a type of malware which secretly store this information and reports back to the attackers system. With a few exceptions, these key-loggers and listening spywares are unproven in identifying mouse movement to crack graphical passwords. Even if the movement is recorded, it is still not accurate in identifying the graphical password. Other information is needed for this type of attack namely window size and position as well as the timing [9].

3.4. Shoulder Surfing Attack

Password can be identified by looking over a person's shoulder. This type of attack is more frequent in crowded areas where it is not infrequent for people to stand behind another queuing at ATM machines. There are some cases in which key pin number can be record using ceiling and wall cameras placed near ATM machines. Properly shield the keypad when entering the pin number can be avoid pin numbers being recorded or remembered by attackers [10-12].

3.5. Physical Attack

When a user directly accesses to the data from the server then it is called physical attack. It makes a chance for attacker to bypass the authentication process and directly access to the resources [5]. There are two situation are created in text password and graphical password by physical attack is possible to access the image gallery and password database. In the first situation, if image gallery is accessed by attacker, it is possible to change the images and make a miss functioning for the system in next login and registration processes. If attacker access to the password database then it is possible to login to the system by any user name [13-15].

4. Conclusion

This paper represents the comparison between different types of authentication process. There are some pros and cons of these techniques. Text based password technique is widely used but it is very unsecured. So it is very rarely used where high level of security needed. Token based techniques are widely used at this time but there are some drawbacks of this technique. Biometric techniques are not widely used due to their initial development cost and there maintenance cost, but it is very secure. Now a days developer working on the graphical password to overcome the drawbacks of the all above techniques.

5. References

1. A.S. Patrick,A. C. Long and S. Flinn, "HCL and Security System" presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA. 2003.
2. K. Gilhooly, "Biometrics: Getting Back to Business", in Computerworld, May 09, 2005.
3. Lin, P. L. and Huang, L. W. (2008), Graphical Passwords using Images With random Tracks of Geometric Shapes, 2008 Congress on Image and Signal Processing, IEEE 2008, pp 27-31
4. Gaurav Agrawal, Saurabh Singh, Ajay Indian, "Analysis of Knowledge based graphical password authenticaiton" SuperStar Virgo, Singapore, August 3-5, 2011.
5. Arash Habibi Lashkari, Azizah Abdul Manaf, Masin Masroom, "A Secure Recognition Based Graphical Password By Watermarking" in 11th IEEE International Conference on Computer and Information Technology, 2011
6. Chiasson, S., et. al., "Multiple Password Interference in Text Password and Click-Based Graphical Passwords", ACM, 2009.
7. Wiedenbeck, S., J.-C. Birget, And A. Brodskiy, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choce, in Symposium On Usable Privacy and Security(SOUPS)", 2005.
8. Dhamija, R. and A. Perrrig, D'ej'a Vu; "A User Study. Using Images for Authentication, in The proceeding of the 9th USENIX security Symposium", 2000, USENIX.

9. Man S., et al., “A password scheme strongly resistant to spyware, in Int. Conf. on Security and Management” 2004: Las Vegas.
10. Forget, A., S. Chiasson, and R. Biddle, Shoulder-Surfing Resistance with Eye –Gaze Entry in Cued-Recall Graphical Passwords. ACM, 2010
11. Lashkari A.H., S.F., Omar Bin Zakaria and Rosli Saleh, Shoulder Surfing attack in graphical password authentication. 2009, International Journal of Computer Science and Information Security (IJCSIS).
12. Man, S., D. Hong, and M. Mathews, A Shoulder-Surfing Resistant Graphical Password Scheme – WIW, in International conference on security and management. 2003: Las Vegas.
13. CAPEC, Standard Abstraction Attack Pattern List (Release 1.6). 2011, Common Attack Patterns Enumeration and Classification (CAPEC): USA.
14. Todorov, D., Mechanics of User Identification and Authentication. 2007: Auerbach Publications.
15. Gordon, P., Data Leakage- Threats and Mitigation, in InfoSec Reading Room. 2007, SANS Institute.