Comparison of Graphical Password Authentication Techniques

Arti Bhanushali, Bhavika Mange, Harshika Vyas, Hetal Bhanushali and Poonam Bhogle
Computer Department,
K. J. Somaiya College of Engineering,
Mumbai, India

ABSTRACT

User Authentication is the most crucial aspect of cyber security. To prevent systems from various types of attacks, password protection to the system is usually provided. The most widely used authentication method using normal text passwords which contains a sequence of alphabets, numbers, and special characters). User mostly tends to choose text passwords which are easy for them to remember (eg. Their birthdate, phone number, etc)... However, even though the technique is user friendly, it is susceptible to many attacks. The other type of Authentication scheme is using Graphical Passwords. These passwords contain images which are easier for humans to remember than the long stream of characters in text passwords.

The paper discusses various approaches of using graphical passwords .The basic algorithms of graphical passwords are being compared based on security and usability parameters.

Keywords

Authentication, Graphical password, Security, Attacks, Password space, Password Entropy, Usability

1. INTRODUCTION

User authentication is the heart of security systems.

1.1 Basic Authentication Techniques

The authentication techniques can be distinguished in three types: knowledge based systems, token based system and biometrics based systems. [12]

1.1.1 Token based authentication system

This type of system refers to “what you have” type of authentication. Here key cards, smart cards, etc. are widely used in order to authenticate to a system. Many of the applications are using token based systems for authentication eg. ATM Machines

1.1.2 Biometric based authentication system

This type of system refers to “what you are” type of authentication. Here user can use his finger print, iris scan, palm scan, etc. as passwords for authentication. The main disadvantage of these systems is they are very expensive.

1.1.3 Knowledge based authentication system

These authentication systems include the “what you know” type passwords i.e. alphanumeric passwords. These systems include both text based passwords and picture based passwords. Picture based passwords also known as graphical passwords involves images or sometimes also referred to drawing passwords. Also it is a tendency that human remembers images easily as compared to text and numbers. Also they provide good resistance to many attacks and provide large password space as compared to text based passwords.

1.2 Types of Graphical Passwords:

1.2.1 Recall based graphical password technique

Recall based technique is further divided into two types

1.2.1.1 Pure recall based technique

Here, the user has to reproduce the password without any hint provided by the system. For example, DAS [10], Grid selection, etc. [11] are pure recalled based technique.

1.2.1.2 Cued recall based technique

in this technique, user is provided with some hint which helps him to recall the passwords he has selected during Registration phase. For example, Blonder [1], pass point [4], etc. are cued recall based techniques.

1.2.2 Recognition based graphical password technique

In this technique, user is provided with set of images from which he is supposed to select the correct image which he has selected during registration phase. For example, Passface [4], Hash visualization technique [3], Déjà vu [2].

2. ALGORITHMS

2.1 Draw A Secret (DAS) [10]

DAS algorithm is a pure recalled based technique in which user has to draw the pattern correctly without getting any hint from the system. In this technique, a grid is provided of size G*G. Each cell in the grid has some coordinates (x,y) assigned to it. The pattern drawn by the user is stored in the form of sequence of coordinates. Consider the following example in which the sequence of coordinates stored will be

(2,2), (3,2), (3,3), (2,3), (2,2), (2,1).

In this technique, the user is required to draw the pattern in one stroke. Thus at the time of authentication, the pattern needs to be redrawn in the same manner as it was done in registration phase without any pen up event. If the user successfully draws the pattern in the exact manner, he is authenticated. This technique is used widely in mobile applications for drawing pattern lock system.

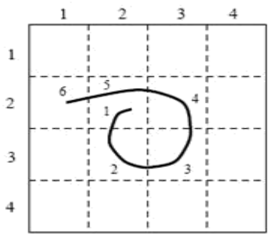

Fig 1: DAS [10]

2.1.1 Advantages

i. Alphabet independent hence there is no language restriction.

ii. Easy to implement.

2.1.2 Disadvantages

i. The major disadvantage is that user cannot remember the exact stroke order.

ii. If user is not familiar with the input devices(mouse, joystick,etc) then the technique is difficult to use.

iii. Less password space.

2.2 Grid Selection Algorithm [11]

Grid selection algorithm is also a pure recall based authentication technique. It overcomes the disadvantages of DAS system i.e. with respect to password space and stroke count.

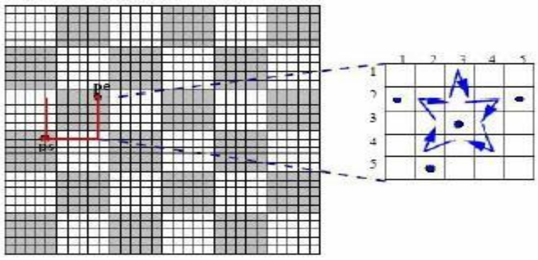

Fig 2:Grid selection[9]

The user is required to select a small region from a large rectangular grid. This region gets zoom in on selection, and then he is required to draw the password pattern as shown in the Figure 2.[14]

2.2.1 Advantages

Larger password space as compared to DAS Algorithm

2.2.2 Disadvantage

i. The disadvantage is that user cannot remember the exact stroke order.

ii. If user is not familiar with the input devices(mouse, joystick,etc) then the technique is difficult to use.

2.3 PassPoint Algorithm [4]

PassPoint Algorithm is a cued recall based technique. The system allows any natural image to be used which should be rich enough to have many possible click points. The role of the image is just to provide a hint to the user which helps in remembering the click points. During login, the click points should be selected in the same order as in Registration phase inside some adjustable tolerable distance. The tolerable distance can be set by the system say within 0.25 cm from the actual click point.

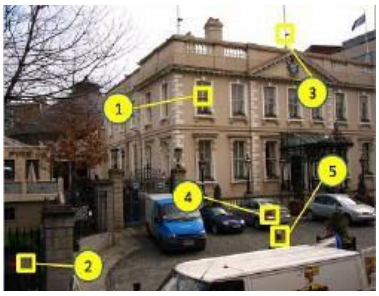

Fig 3: PassPoint[9]

2.3.1 Advantages

As in Blonder algorithm[1], user had to click on the predefined image at predefined region. PassPoint algorithm overcomes this by selecting any natural image and having as many click points as possible which make the system more secure.

2.3.2 Disadvantage

i. Time consuming.

ii. Difficult to memorize the click points, thus number of trials is required for authentication

2.4 Déjà vu Algorithm [2]

Déjà vu is a recognition based authentication technique. Here the user is provided with a random set of images. Which is generated using Hash visualization technique[3]? Here during registration of a new user, a seed value gets generated for that user which gets stored at a trusted server. Using this seed value one random mathematical formula is generated which is applied on each pixel value to get a new image. The output will be a random abstract image.

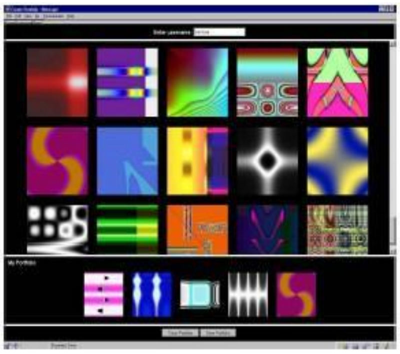

Fig 4: Déjà vu[2]

2.4.1 Advantages

Easy to remember

2.4.2 Disadvantages:

i. The seed values generated are stored on a trusted server. If the server fails, seed values get corrupted.

ii. Time consuming.

3. COMPARISONS OF ALGORITHMS

The above discussed algorithms are compared based on two parameters: Security and Usability.

3.1 Security

Security of any algorithm can be understood by studying two aspects:

3.1.1 Resistance to various Attacks

3.1.1.1 Brute Force Attack

It is a cryptanalytic attack in which exhaustive key search is done. Here every possible option is taken into consideration to break the password until the correct one is found. The password space of text based passwords is 94^N, where N is the length of password and 94 is the number of printable characters excluding “space”[9]. The probability of success using this attack is more in textual passwords than graphical passwords because in graphical passwords it is difficult to track every movement of the mouse or input device.

3.1.1.2 Dictionary Attack

In this attack an exhaustive list of words example dictionary is used to break password. This dictionary consists of words which are most likely chosen by the user as passwords. Unlike brute force attack, dictionary attack uses a systematic key search to crack passwords, that considers only those possibilities which are most likely to succeed, but it cannot crack the password every time as in brute force attack.[9]

3.1.1.3 Spyware Attack

In this type of attack software gets installed on the user's computer which starts recording each and every movement of the mouse pointer or keys pressed by the user without user's knowledge. Spyware is not effective for cracking Graphical password because it considers only key pressing and mouse clicking events which may not be same all the time.[9]

3.1.1.4 Shoulder surfing Attack

As the name suggests, sometimes it is possible to find out the password of user by looking over the person's shoulder. This attack mostly occurs in crowded area where people are unaware of the people standing around him. Also some places like ATMs have cameras fitted inside. They can also record the PIN numbers of the user who is using the ATM machine.

3.1.1.5 Social Engineering Attack

This is also known as Description attack. It refers to psychological manipulation of people into performing actions and revealing confidential information. It performs various tricks to gain people's confidence and reveal their confidential information leading to different scams and frauds.

Thus the comparison of various Graphical Password Algorithm based on these attacks is as follows:

Table 1. Comparison based on Attack Resistance

Algorithms	**Resistance to attacks**	**Non-resistance to attacks**
DAS	Brute-force,Dictionary,Social Engineering	Shoulder surfing, Spyware
Grid Selection	Brute-force,Dictionary,Social Engineering ,Shoulder surfing	Spyware
Pass-point	Brute-force,Dictionary,Social Engineering	Shoulder surfing, Spyware
Déjà vu	Shoulder surfing, Spyware	Brute force, Dictionary, Social Engineering

3.1.2 Password Space and Password Entropy

3.1.2.1 3.1.2.1 Password Space:

Users can pick any element for their password in GUA; the raw size of password space is an upper bound on the information content of the distribution that users choose in practice. It is not possible to define a formula for password space but for all algorithms it is possible to calculate the password space or the number of passwords that can be generated by the algorithm.[9]

3.1.2.2 Password Entropy

Password entropy is usually used to measure the security of a generated password, which conceptually means how hard to blindly guess out the password. For simplicity, assume all passwords are evenly distributed, the password entropy of a graphic password can then be calculated as follows.

$$\text{Entropy} = N \log2 (|L||O||C|)$$

In other words, Graphical password entropy tries to measure the probability that the attacker obtains the correct password based on random guessing. In the above formula, N is the length or number of runs, L is locus alphabet as the set of all loci, O is an object alphabet and C is color of the alphabet.[9]

Table 2. Comparison on password space and entropy

Algorithms	**Password space**	**Password Entropy**
DAS	Low password space	Low password entropy
Grid Selection	Higher password space than DAS	Higher password entropy than DAS
Pass-point	Depends on	Depends on click

3.2 Usability

Features such as Easy to use, Easy to create, Easy to Memorize, easy to Learn, Design and screen layout, accurate and reliability are necessary properties to consider in designing a good graphical user algorithm. In the evaluation of graphical password several usability properties need to be measured. Among these are: (1) time to login, (2) number of mistyped passwords and (3) number of forgotten passwords after a certain period following the registration. Usability however can be considered a personal preference. Comparison table of usability attributes for considered techniques is given below.

Table 3: Comparison on usability features

Algorithms	Reliability	User-friendliness	Accuracy
DAS	Reliable as doesn't depend on click points.	Quite easy to use & implement.	Yes, as easy to memorize.
Grid Selection	Reliable than DAS due to larger space.	Less as compared to DAS.	High as depends on stroke count.
	High since		Less accurate

Pass-point	selection of natural images.	Difficult to memorize.	as requires sample training.
Déjà vu	Depends on access rights of server.	Less user friendly as user needs to remember the images sequentially.	Accurate due to its complexity.

4. CONCLUSION

The preliminary analysis suggests that graphical password techniques achieve better security than conventional textual passwords. They are more accurate and reliable than textual passwords .Among these studied techniques DAS is most applicable and user friendly but not secure due to its less password space. Grid selection technique overcomes the problem of less password space of DAS but not user-friendly due to its complexity .As far as Déjà vu is considered the login and registration phase becomes tedious due to handling of more images. Considering Passpoint and grid selection method, they are more secure and reliable, but Grid selection technique is not applicable.

Pass Points has the security advantage of a large password space over alphanumeric passwords. It also has an advantage in password space over Blonder-style graphical passwords and recognition-based graphical password, such as Déjà vu. The disadvantage of Passpoint is that it doesn't provide resistance to Spyware attacks. Some solution to this problem has to be given to achieve most reliable authentication system which is applicable in day-to-day life

5. ACKNOWLEDGMENTS

The authors gratefully acknowledge the contributions of Prof. Poonam Bhogle and thank her for her endless support and motivation, the college for providing the necessary infrastructure and platform for doing this research.

6. REFERENCES

[1] Blonder, G. E. Graphical Passwords, Murray Hill, NJ, US Patent, 1996

[2] Rachna Dhamija, Adrian Perrig; 2000, "Déjà Vu: A User Study. Using Images for Authentication", in the proceeding of the 9th USENIX security Symposium.

[3] Rachna Dhamija; 2000, "Hash visualization in user authentication", Proceedings of CHI 2000 ACM, The Hague, the Netherlands.

[4] Susan Wiedenbeck, Jim Watersa, Jean-Camille Birgetb, Alex Brodskiyc, NasirMemon; 2005a, "Design and longitudinal evaluation of a graphical password system", Academic Press, Inc. 102-127

[5] Toomaj Zangooei, Masood Mansoori, IanWelch;"A Hybrid Recognition and Recall Based Approach in Graphical Passwords"; OZCHI'12 Proceedings of the 24th Australian Computer Human Interaction Conference ACM New York

[6] Umar, M.S.; Rafiq M.Q. Ansari J.A.,"Graphical user authentication: A time interval based approach"; Signal Processing Computing and Control(ISPCC),2012 IEEE International Conferencettsburgh, Pennsylvania, USA, ACM

[7] Umar, M.S.; Rafiq M.Q.;"Select-to-Spawn: A Novel Recognition based graphical user authantication skim"; Signal Processing Computing and Control (ISPCC), 2012 IEEE International Conference

[8] X.Suo, Y.Zhu, and G. S. Owen, "Graphical Passwords: A Survey", in Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005), IEEE Computer Society, pp. 463-472, 2005.

[9] Arah Habib Lashkari."A new algorithm for graphical user authentication based on rotation and resizing"

[10] Jermyn Ian, A. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin; 1999, "The design and analysis of graphical passwords", Proceedings of the Eighth USENIX Security Symposium, USENIX Association 1–14.

[11] J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in 20th Annual Computer Security Applications Conference (ACSAC) Tueson, USA. IEEE, 2004.

[12] Information Security Principles and Practice by Mark Stamp - Second Edition.

[13] Di Lin, Paul Dunphy, Patrick Olivier, Jeff Yan; 2007, "Graphical Passwords and Qualitative Spatial Relations", Proceedings of the 3rd Symposium on Usable Privacy and security, Pennsylvania, ACM.

[14] Muhammad Daniel Hafiz, Abdul Hanan Abdullah, Norafida Ithnin, Hazinah K. Mammi; 2008, "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique"; IEEE Explore.