Chapter

New Graphical Password Scheme Containing Questions-Background-Pattern and Implementation

Bulganmaa Togookhuu, Wuyungerile Li, Yifan Sun and Junxing Zhang

Abstract

Security of authentication is needed to be provided superlatively to secure users' personal and exchange information, since online information exchange systems have been developed according to internet speed. Therefore, aim of the chapter is to develop current graphical password scheme based on recall, create and implement a new graphical password scheme composed of three layer verification. We programmed our scheme in order to use in section of anonymous information exchange system and user's registration of trading chat room. While we conducted survey on user by accessing participant to our system lied in participants' local network and we analyzed in accordance with the average length of their created password and statistical significant of entropy bit. From the survey of total participants, our scheme has statistical significance, furthermore it was proved that it can secure form a variety of attacks as entropy bit was high.

Keywords: graphic password, user authentication, QBP scheme and implementation

1. Background

Textual password mechanisms are the most commonly used, however with known weaknesses. The weaknesses include user fallibility in memorizing long or complicated passwords and the security risks posed by the use of short simple passwords.

One motivation for examining the application of graphical schemes is that humans have a remarkable capability to remember pictures. Second background of category is that most of the recall-based graphical passwords systems developed.

In addition, another motivation for this research is "what we build is what we remember more". Current forms of commonly promoted graphical passwords can be divided into three general categories: recognition-based systems, cued-recall systems and recall-based systems.

1. For the recall-based category, Jermyn et al. proposed a scheme, called "draw-a-secret (DAS)". A user asked to draw a simple picture on a 2D grid. During authentication, the user asked to re-draw the picture. If the drawing touches the same grids in the same sequence, the user is authenticated.

2. For the recognition-based scheme called pass point, users have to recognize their pass image on images when they see them again. When they register, the user either provides their own images or chooses from a collection provided by the system.

3. In a recall-based system, the user has to recreate their pass image every time they log in. This is similar to a written signature used to sign documents. A cued recall-based system provides cues to users to help them repeat their initial actions, such as selecting points in an image each time they log in.

One common problem for graphical passwords is the shoulder surfing problem: an on-looker can steal a user's graphical password by watching in the user's vicinity.

Therefore, the aim of this chapter is to develop existing graphical password scheme based on one's memory, create and implement a new graphical password scheme that is composed of three-layer verification.

1. Scheme of secret question and answer based on text

2. Scheme of choosing image based on recognition

3. Scheme of creating password using drawing based on remembering

We programmed our scheme in order to prove its superiority comparing with existing schemes. We attend on user survey that participants access to our system on local network. It was according to the average length of their created password and statistical significance of entropy bit. From the survey results of total participants, we find that our scheme is statistically significant, furthermore it was proved that it can secure a variety of attacks due to its high entropy.

2. Related work

Since it has been proved that images are easier to recall than text phrase, some people have been suggested graphical password as an alternate. Dirik et al. [1] classified the graphical password into three systems such as pure recall-based systems, recognition-based systems and cued recall-based systems [2]. People who use recall-based password system have to remember their password to access to system. Furthermore, one of the most famous studies of recall-based techniques was offered by Jermyn et al. [3].

The system of Govindarajulu et al. [4] that used doodles as recall-based systems, requires expensive equipment, such as a touchpad and digitizing tablet that are attached to a computer and users also need each time to learn how to use the system. Recognition-based graphical passwords systems lie in a variety of images used and user either chooses benefits provided by the system or provides their own images.

Hai Tao [5] draws the password using grid intersection points instead of grid cells. In addition, this scheme gave users a chance to select longer passwords and use colors, both resulting in greater password complexity than in DAS scheme. Hatching et al. [6] selected pass image one–by-one with the same sequence by drawing the curve starting from the given image (red rectangle) and ended the image marked with a green rectangle. While Thorpe et al. [7] set the selected location "X" marker near his or her previously chosen location, they used Google Maps and large password space.

3. CRS graphical password scheme and concepts

Numerous researchers are concentrating and writing research papers on authentication and security of contemporary information system. One of them is shoulder surfing attacks unlocking smart phone used for everyday life [8–10]. Users, however, can create strong entropy or password consisted of long bits in terms of any single system, which is difficult to remember. Thus, we have improved security of Pass-Go scheme, added secret questions, answers and background image, processed and implemented a new scheme to solve the problem. It called "Questions-Background Image-Pattern (CRS)".

Thus, we have improved security of Pass-Go scheme, added secret questions, answers and background image, processed and implemented a new scheme to solve the problem.

Main activity of CRS runs according to principle choosing node dots instead of partition, similarly Pass-Go scheme. It can be easy not only to use but also beneficial to remember while it may create strong and complex password because of inserting background image in the view, similar to BDAS pattern.

Our CRS is consisted of triple verification parts to secure safety of password superlatively. For instance:

1. Scheme of secret question and answer based on text
2. Scheme of choosing image based on recognition
3. Scheme of creating password-using drawing based on remembering

when user has created a password only generated a new version by adding the traditional scheme of question and answer contained password feature to scheme of a graphical password. It can be used in web site of information trading and authentication phrase of trading chat room.

To refer systems based on modern web using graphical password scheme rarely, graphical password scheme based on recognition (selecting Chinese characters and various images) is used in authentication section of large searching systems like Android OS for smart phone pattern lock, Google and Baidu. Some psychologists assume that human brain remember graphical information better than others [11]. One of the researches revealed that how authentication and unlocking process influence based on phone user's behavior.

In accordance with Dual Coding Theory, cognition is consisted of two different sections such as nonverbal and verbal systems [12, 13]. Thus, user will pass following steps to register using our scheme. After choosing questions and answers to them and inserting optional background image behind the grid, graphical password is created and appeared. Then user will create password by connecting points lying on the board and drawing shape using straight line.

Therefore, we processed scheme which secures safety of password, combined with practice and implemented as a result of studying graphical password space theory.

Our proposed idea is devoted to advertising web site of anonymous information trading containing feature of test-based and graphical password and authentication section of trading chat room that trades secured file to contract safely. CRS scheme can be protected from various attacks since there is no personal information about the users on the website. While designing the scheme, we established a graphical password scheme, which is easy to use, interesting and strong, integrated by adding both BDAS [20] based on recall and Pass-Go [5] graphical password scheme to password like traditional test-based having secret questions and answers.

In our CRS scheme, there are 25 points on the 5 × 5 board and user connects points and draws optional image on free position using straight line. It is possible to mark eight directions freely by striking at least more than four points. Drew path from start point to end will be numbered 1–25. When reproduce, user need to select point drawn in previous step correctly and draw to end by recall previous imagination. This requirement aimed at creating strong drawing graphical password, which provides system security. Our scheme, thus, is divided to 5 × 5 grids, developed like consisted of overall 25 points and implemented in authentication section of system based on web. User should register in accordance with following scheme. The CRS scheme flow diagram (**Figure 1**).

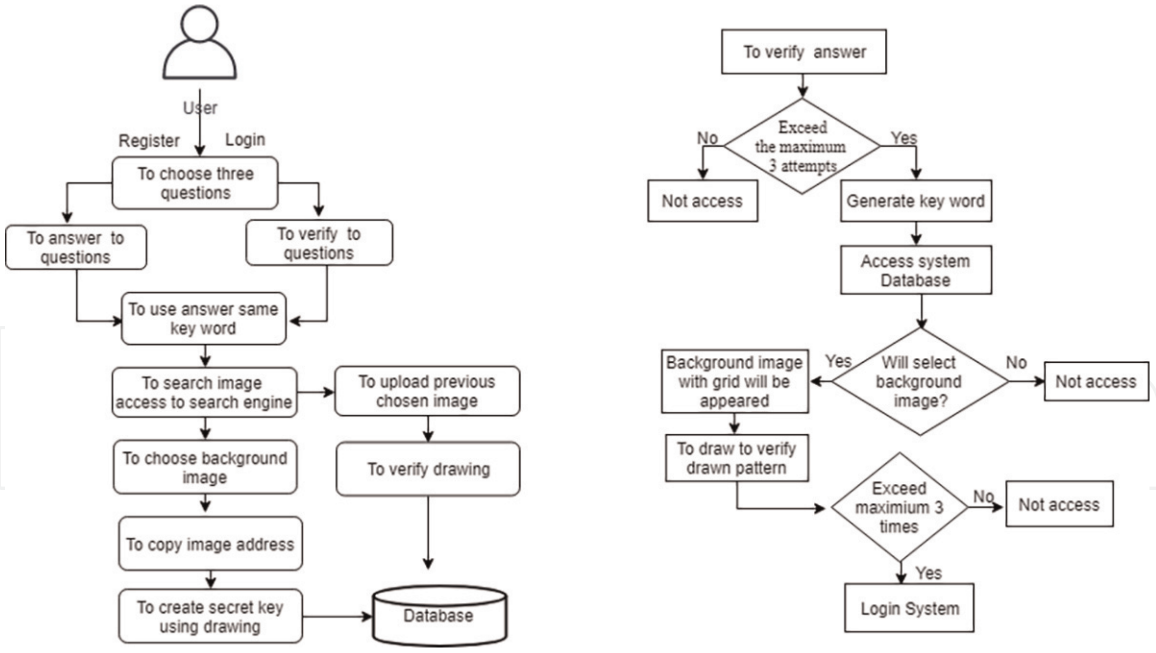

User
Register
Login
To choose three questions
To answer to questions
To verify to questions
To use answer same key word
To search image access to search engine
To upload previous chosen image
To choose background image
To verify drawing
To copy image address
To create secret key using drawing
Database
To verify answer
Exceed the maximum 3 attempts
No
Yes
Not access
Generate key word
Access system Database
Background image with grid will be appeared
Yes
Will select background image?
No
Not access
To draw to verify drawn pattern
Exceed maximium 3 times
No
Not access
Yes
Login System

Figure 1.
Register, login process, questions and answers verification.

4. Main unit of the CRS graphical password scheme

User accesses authentication page of system, selects and answers three of variety questions. Using secret question and answer in system authentication section is responsible for increasing overall bits' size of password. In order to prepare secret question and answer based on a user, we should obey prohibited regulations of international telecommunications industry and the FCC's Customer Proprietary Network Information (CPNI) that do not contain questions about user's personal information.

Password does not contain user's personal information such as e-mail address, surname, birth date, user's registration number and phone number. The password requires answers that are easy to memorize, adamant in terms of time, has feature to cover public, is difficult to guess and provides security. If attackers capture user's weak answer, they will experience trouble in every step to guess graphical password created by secret drawing or next step verification.

- We are required consisted of long characters question and answer from user to provide answer security. Therefore, we decided that minimum of answer character is ≤4, maximum of accepting answer can be composed of ≤10–26 (letter, number and exclusive character) when answer using collocation.

- Questions will appear with original text as user selects question. However, answer was saved by cryptographic hash function. Users need to select a new question's pack again and create new one if they forget answer. If session idle both will warn to answer secret question within 3 minutes and move to next step (verification step).

- Images which are appropriate to find using chosen three answers of questions like keywords will be revealed separately on three web guides from system base.

- When user selects one image and copies location code (copy image address), the image will be the background image of our system and inserted behind grid. One advantage of this way helps to deceive attackers who want to obtain background image.

- Board inserting background image should be 5 × 5 grids while user will select from 25 points on 2D board and draws by pen-up from start to endpoint under pen-drag movement. User need to connect under following rule and mark as a line.

    - User needs to select at least four points.

    - Previous points can choose by concurring, if there is no neighbor point.

    - It confirms to connect points using only straight line and mark.

    - It is impossible to select by jumping over next point without choosing previous point.

    - User can create number of optional images in free positions.

The fifth step improves Pass-Go scheme, solves haziness of graphical imagination and increases password space.

5. To verify secret drawing

Firstly, to select and answer to secret question; secondly, to create password using drawing; thirdly, to create graphical password using secret drawing.

As a result of integrating cited-above sections, password containing long bit will be created. Bit size is different depending on choice of answer's character. The bit entropy has estimated by traditional test-based password (if it is ≤28 bits, they are greatly weak; if it ≤28–35 bits, they are weak; if it is ≤36–59 bits, they are probable; if it ≤60–127 bits, they are strong and if it ≤128+ bits, the greatly strong).

When users register to system firstly, they will pass following steps such as answering to secret question, inserting background image behind blank grid and creating password using drawing on it. To access, user reproduces previous 2 steps and verifies by reproducing previous secret drawing. After checking every step in any condition on system, user can access successfully, if every data is correct in verification steps. If access right was canceled after making over three attempts in any step, user needs to create from beginning. Although it is a strict requirement, it can provide security.

5.1 Implementation and evaluation

We used JavaScript, node.js and developed in condition of Linux operating system. User ID, password and other associated data will be saved in SQLite database in server part. The proposed CRS can be used in website of information trading and user authentication section of trading chat room. We solved the problem and processed scheme, which is easy to use by improving current password scheme and providing security superlatively. Implementation step is consisted of following sections.

1. User can select three of optional questions and answer to them.

2. User finds image from search engine using answer like keyword.

3. User selects only one image and inserts background image.

4. A 5 × 5 grid consisted of 25 points, which will be inserted on background image.

5. For probability of selecting overall points, n-gram probability will be estimated based on Markov model.

6. Selected points will be estimated by probability of decreasing sequence.

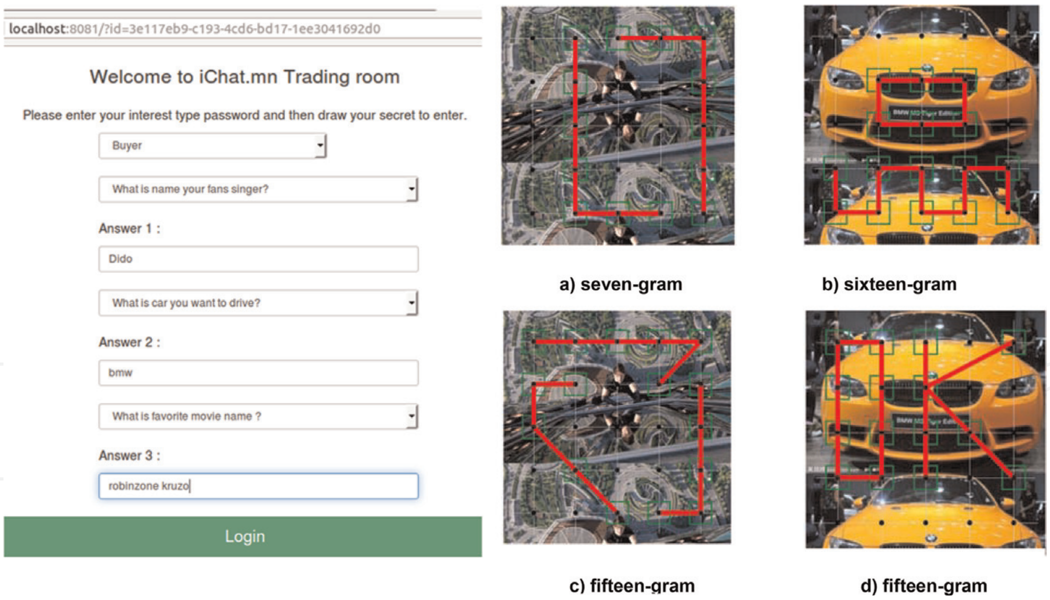
7. We program under scheme and estimate password strength according to user's study.

5.2 Implementation interface

Our scheme will select intersection of two-dimensional coordinate pairs based on recall instead of cell. In this section, we will study start and end of safe pattern and sub-pattern, and then estimate through Shannon's entropy. Mono-grams will be probability of selected N-point on overall pattern to estimate entropy of start and end point. To estimate N-gram, we have estimated probability of X point appearing in entropy pattern or Nth using N-1 point and used (**Figure 2**).

The conditional entropy is estimated by Shannon's formula [21] (F_N: N-gram entropy).

$$F_N = -\sum_{i,j} p\left(b_{i,j}\right) \log_2 p\left(b_{i,j}\right) + \sum_i p(b_i) \log_2 p(b_i) \qquad (1)$$



localhost:8081/?id=3e117eb9-c193-4cd6-bd17-1ee3041692d0

Welcome to iChat.mn Trading room

Please enter your interest type password and then draw your secret to enter.

Buyer

What is name your fans singer?

Answer 1 : Dido

What is car you want to drive?

Answer 2 : bmw

What is favorite movie name ?

Answer 3 : robinzone kruzo

a) seven-gram

b) sixteen-gram

c) fifteen-gram

d) fifteen-gram

Figure 2.
CRS—graphical password user interface. (a) User selects questions and answers, (b) most frequently drawn points, (c) few drawn points and (d) average drawn points.

Here, b_i is (n − 1) grams, b_j is an arbitrary point which has not been chosen and $P(b_{i,j})$ is the N-gram probability of $b_{i,j}$. It can be marked from upper left corner by representing “0” like modern android phone lock. For example, it will be expressed by following formula if bigram is b_i = 01″ and b_j = 02″.

$$p(b_{i,j}) = p(''012'') = \frac{\#of\ occurrences\ of\ trigram\ ''012''}{sum\ of\ occurrences\ of\ all\ trigrams} \tag{2}$$

While guessing entropy, [22, 23] is one metric that can be used to measure the strength of a (password) distribution. The method determines possible connections from start point to the endpoint.

6. Used in research methodology

6.1 Point selection (N-grams)

To create a password using our scheme, overall 25 points will connected and it will be marked by sequence of line. Thus, we will concentrate on N-gram and establish probability having the strongest feature. In general, it is assumed that N-gram having enough probability is significant to estimate probability taken from [24].

For instance, when n = 2, we need to learn 25 × 24 = 600 values and we need to learn when n = 3 in terms of our scheme 25 × 24 × 23 = 13,800 (slightly less than). Users usually created secret drawing using 15-gram and 16-gram probability. It was observed that a number of points’ choices were increased and image was drawn by enough long straight because of inserting background image.

6.2 Selecting start and end points

More than half of research participants (51.1%) started upper left or left side to choose start point. In addition, over half of our research participants chose upper left point as a start point and it is related to their mother language written from upper left point.

For all points having the same probabilities, the entropy of start point is 2.35 bits to a maximum of $\log_2{}^{61.9}$ bits compared. For male participants, they selected car and football images, set them on background image and expressed chosen average 18 spaces of start and end with much longer. For female participants, they selected flower and a variety of brands, set them on the background image and chose few points (chosen point's average is 19.3). To observe choice of end point, they chose lower right points more than other and estimated probability is 2.75 entropy bit. From the survey, the most frequent path is upper left and bottom right point and it defined that we can estimate points' averages.

6.3 Measure strength of password

Our password scheme is consisted of combination of character and graphical password and create strong password, which is longer over 128 bits by adding length of user's answered character. Many researchers aimed at measuring password strength using a variety of measuring methods. Thus, we measured password entropy established by text-based and graphical password separately.

$$H = \log_2 N^L = L \log_2 N = L\frac{\log N}{\log 2} \tag{3}$$

Password entropy measures condition that is impossible to predict and use longer password based on character (lowercase, uppercase and special characters). Optional password strength is measured by information entropy. Furthermore, possible password and number are expressed by $\log_2$ and every characters creating password will be processed independently. Therefore, information entropy of optional password is estimated by following [25] H-formula:

N is possible number of character, L is number of string (character) on the password and H is measurement of bit.

6.4 To encode graphical password and full password space

User-drawn image will be encoded by sequence of intersections represented by two dimensional coordinate pairs. Points passed through intersection points using mouse will be numbered by value from 1 to 25.

The length of password is the number of coordinate pairs except pen-ups in the password encoding. Based on a password with length L, where adding one point (P2) or increasing the last through a unit of any directions of the least 3 and most 8, with length of L + 1, a new password will be made. When L = 1, the password has the minimal length.

$$PS \leq S1 + S2 + S3 + DP\ (n) \tag{4}$$

PS is the size of the full password space, S1, S2 and S3 are sizes of the textual passwords from users' responses to random challenges, and DP(n) is the size of the graphical password space.

7. CRS-new graphical password scheme evaluation

Since it is difficult to assess security of graphical password, we studied usage part and indicated survey result by conducting survey on our scheme. Because of it, user can choose numerous points to create password and chance to guess by attackers will be decreased.

We chose participants from foreign students living in school campus using collecting data method and gave instruction as how to execute work before conducting on survey. Then participants accessed to system existed in local network and created graphical password will be used to pass to trading chat room. We indicated demographical survey of overall participant and creating graphical password. Total 50 participants aged from 25 to 55 were enrolled in our survey and they worked and spent over 8 hours on computer-related internet environment.

7.1 Login time

We estimated average of spent overall time when total participants accessed to login and verification system. Unlocking the devices, users on average spent 2.6 minutes each day as presented by Harbach et al. [26]. Thus, we assumed that 3 minutes are enough to pass trading chat room and verify based on the survey. Depending on ability of computer usage, we deducted participants who spent more than 3 minutes from survey result.

In addition, the maximum of three answers that participants chose and answer to questions in the first step is 191.3 bits and the minimum of three questions is 23 bits. We divided participants' created password into long and short sections and we studied length of password using Kruskal-Wallis [27] tests method in terms of sufficiency changes of successful login. Consequently, short secret has $H(5) = 19:31$, $p<:02$ significance and long secret has $H(5) = 15:91$, $p<:04$ significant.

When classifying participants based on sex and comparing the length of straight drawing graphical secret, male created line with 18 average lengths whereas female created line with 19.3 average lengths. Participants chose 15-gram, 20-gram and created secret drawing and the maximum repeated of 15-gram is 14%. When estimated, the average of creating secret of participants is 1.08 sec. The maximum is 2.5 minute while the minimum is 0.30 sec.

7.2 Success rate

Due to the aggregate attempts from an individual, the success rate is determined on average with successful logins. During re-register and verifying 15 minutes after participants created secret successfully, different results were revealed. Total time to recall authentication is within 3 minutes and there are the maximum of three-access right to insert password three times in every verification sections. Total participants recall differently on three sections of verification: Recalling as one access is 38%, recalling as two accesses is 30%, recalling as three accesses is 16% and participant who cannot pass access number exceeding is 16%.

7.3 Password strength

The theoretical password space of a graphical password scheme is a security strength indicator defined by the total number of possible passwords. Recall schemes based on drawing shapes have been shown to suffer from tentative patterns [7, 28].

In cited-above survey, we suggested that bit entropy must be high to secure password used in system from attackers. Therefore, we shown our new graphical password scheme based recall entropy bit (**Figure 3**).

Table 1 shows the capacity of total bits of the graphical password based on traditional textual password and recalling by comparing them. For instance, when

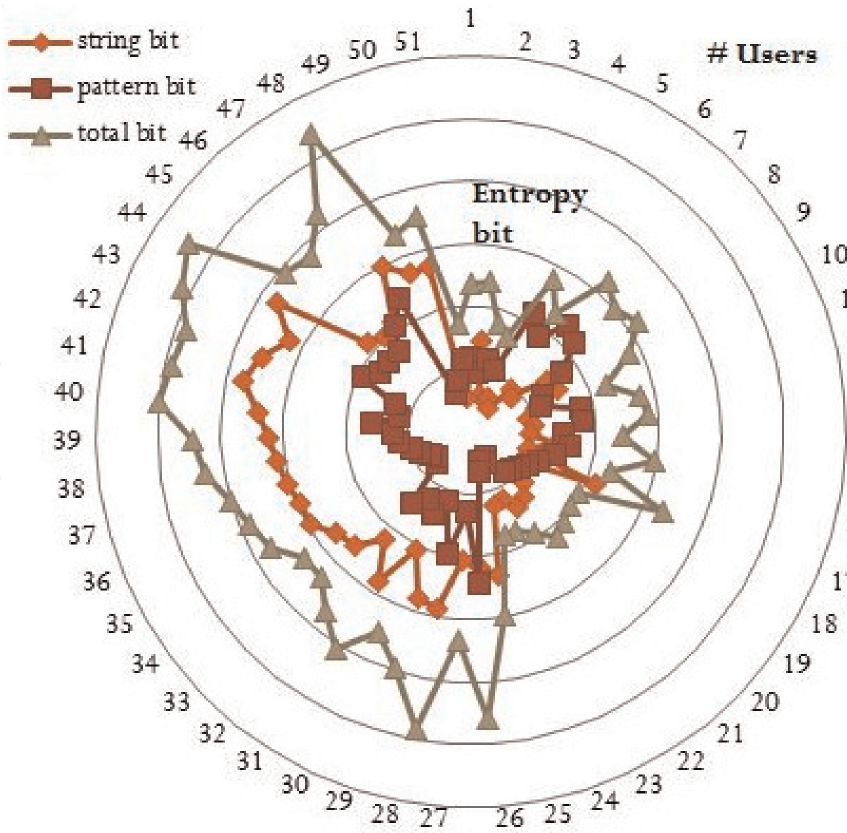


Figure 3.
Recall entropy bits and user number.

	Textual password (95^n) [13]	DAS [28]	BDAS [29]	Pass-go [5]	Proposed CRS scheme
Bits	$95^{28} = 2^{129}$	$2^{96.2}$	2^{76}	2^{256}	$\leq 2^{271}$

Table 1.
Compare full graphical password bit space.

we choose a textual password that has maximum 28 characters, it is worth with 129 bit. Maximum capacity of DAS scheme based on recalling was 96.2 bit while maximum capacity of BDAS model was worth with 76 bit. Maximum capacity of Pass-go model developed by improving DAS model based on initial recalling is 256 bit. Our CRS scheme was developed by combining advantages of above-given models and its maximum capacity is worth 271 bit. As a result, it can help to reduce risk of attack.

From view, **Table 1** proposed most bit-size for CRS scheme. We suggested that bit entropy must be high to secure password used in system from attackers.

8. Conclusions

This chapter provides introduction to graphical password, its study, new type of graphical password design, its implementation and its results. For large system, main problem is secret verification. Indeed, it is thing being developed to hammer out solution in any time. We proposed graphical password, based on user's habit and interest, is easy to use and created password consisted of strong entropy bit. Studied usability aspect of CRS graphical password by providing users with CRS graphical password and monitored their graphical password creation and their utilization.

Total of 50 users have participated in this study, and analyzed their time spent in CRS graphical password creation, how long they could remember it and strength of the password. Thus, it can secure a variety of attackers such as traceability of fingerprint smudges, dictionary, shoulder attack, brute force attack and so on. We can use our scheme providing password security for checking mail, service of social network messenger, internet bank, website of trading organization, training website and authentication of a variety of devices.

Author details

Bulganmaa Togookhuu[1], Wuyungerile Li[2], Yifan Sun[2] and Junxing Zhang[2]*

1 School of Engineering and Technology, Mongolian University of Life Sciences, Ulaanbaatar, Mongolia

2 College of Computer Science, Inner Mongolia University, Huhhot, Inner Mongolia, China

*Address all correspondence to: junxing@imu.edu.cn

References

[1] Dirik AE, Birget. Modeling User Choice in the PassPoints Graphical Password Scheme. In: Symposium on Usable Privacy and Security (SOUPS); 2007

[2] Delprato D. Mind and its evolution: A dual coding theoretical approach. The Psychological Record. 2009;**59**(2): 295-300

[3] Jermyn I et al. The design and analysis of graphical passwords. In: The 8th USENIX Security Symposium; Washington, USA. 1999. pp. 1-15

[4] Noor Ain R, Singh D. Early learning malay vocabulary using speech technology: Dual code theory approach. In: Proceedings of the International Conference on Electrical Engineering and Informatics. 2011

[5] Tao H. Pass-Go: A New Graphical Password Scheme. Canada: Master of Applied Science, Electrical and Computer Engineering, University of Ottawa; 2006

[6] Davis D, Reiter K. On user choice in graphical password schemes. In: USENIX Security Symposium. 2004

[7] Wagner P. Cryptanalysis of a cognitive authentication scheme (extended abstract). In: IEEE Symposium on Security and Privacy. 2007

[8] Oorschot J et al. Graphical dictionaries and the memorable space of graphical passwords. In: USENIX Security Symposium. 2004

[9] Shokarev A, Kostyuchenko E. User authorization in the picture password system with application of digital watermarks. In: 2016 Dynamics of Systems, Mechanisms and Machines (Dynamics). 2016

[10] Ventura N et al. An approach password graphic for access control web. In: Conference on Information Systems and Technologies (CISTI). 2016

[11] Skinner G. Cyber security for younger demographics, a graphic based authentication and authorisation framework. In: IEEE Region 10 Conference (TENCON). 2016

[12] Dunphy P, Yan J. Do background images improve draw-a-secret graphical passwords. In: Proceedings of the ACM Conference on Computer and Communications Security (CCS); New York, USA. 2007

[13] Shannon C. Prediction and entropy of printed English. Bell System Technical Journal. 1951;**30**(1):50-64

[14] Cachin C. Entropy measures and unconditional security in cryptography [PhD dissertation]. https://cachin.com/cc/papers/d.pdf

[15] Sebastian Uellenbeck MD. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns, Publication Security, Human Factors, ACM, 978-1-4503-2477-9/13/11; 2013

[16] Wikipedia. Password Strength. Available from: https://en.wikipedia.org/wiki/Password_strength

[17] Marian H et al. A field study of smartphone (un)locking behavior and risk perception. In: Symposium on Usable Privacy and Security. Menlo Park, CA: USENIX Association; 2014

[18] Li L, Tsai M. Notice of retraction <br>a study on quality traceability of transmission assembling based on Kruskal-Wallis method. In: International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE). 2013

[19] Thorpe J, Salehi-Abari A. Usability and security evaluation of geo pass, a geographic location-password scheme. In: Symposium on Usable Privacy and Security (SOUPS); Newcastle, UK.

[20] Password Choosing and Using Security Questions. Available from: https://www.owasp.org/

[21] Shannon C. Prediction and entropy of printed english. Bell System Technical Journal. 1951;**30**(1):50-64

[22] Yan P. Do background images improve "draw a secret" graphical passwords? In: ACM Conference on Computer and Communications Security (CCS). 2007

[23] Bulganmaa T et al. New graphical password scheme containing questions-background-pattern and implementation. Procedia Computer Science. 2017;**107**:148-156

[24] Needham M. Prudent engineering for cryptographic protocols. IEEE Transactions on Software Engineering. 1996;**22**(1):6-15

[25] Karabey I, Akman G. A cryptographic approach for secure client—server chat application using public key infrastructure (PKI). In: International Conference for Internet Technology and Secured Transactions (ICITST). 2016

[26] Naman S, Khandelwal P. Two factor authentication using visual cryptography and digital envelope in Kerberos. In: International Conference on Electrical Electronics Signals Communication and Optimization (EESCO). 2015. pp. 1-6

[27] Micali S. Distributed split-key cryptosystem and applications, U.S. Patent No. 6026163; 2000

[28] Sudha M, Thanuja T. Randomly tampered image detection and self-recovery for a text document using Shamir secret sharing. In: IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). 2016

[29] Yang X, Xiao M. Verifiable secret sharing and distributed key generation based on hyperplane geometry. In: 2nd International Symposium on Dependable Computing and Internet of Things (DCIT). 2015

[30] Yingli Z. A Key Escrow Scheme to IOT Based on Shamir. ChengDu, China: Research Institute Electronic Science and Technology, University of Electronic Science and Technology of China; 2013