TQ-Model: A New Evaluation Model for Knowledge-based Authentication Schemes

Shah Zaman Nizamani[1] · Syed Raheel Hassan[2] · Riaz Ahmed Shaikh[2]

Abstract

Many user authentication schemes are developed to resolve security issues of traditional textual password scheme. However, only Android unlock scheme gets wide acceptance among users in the domain of smartphones. Although Android unlock scheme has many security issues, it is widely used due to usability advantages. Different models and frameworks are developed for evaluating the performance of user authentication schemes. However, most of the existing frameworks provide ambiguous process of evaluation, and their results do not reflect how much an authentication scheme is strong or weak with respect to traditional textual password scheme. In this research paper, an evaluation model called textual passwords-based quantification model (TQ-Model) is proposed for knowledge-based authentication schemes. In the TQ-Model, evaluation is done on the basis of different features, which are related to security, usability and memorability. An evaluator needs to assign a score to each of the feature based on some criteria defined in the model. From the evaluation result, the performance difference between a knowledge-based authentication scheme and textual password scheme can be measured. Furthermore, evaluation results of Android unlock scheme, picture gesture authentication scheme and Passface scheme are presented in the paper using the TQ-Model.

Keywords Authentication · Security · Passwords

1 Introduction

Textual password scheme is commonly used for user authentication because it is very easy to use. However, this scheme is weak against guessability and capture-based attacks. High percentage of textual passwords can be guessed by applying different types of dictionary attacks [1,2]. Textual passwords can also be captured through camera recording, network interception or spyware attacks because the passwords are directly entered in a login screen. The chances of capture-based attacks can be reduced through inserting a password indirectly in the login screen [3], i.e., on every login session a new password input is given.

Authentication security improves when the separate password is used for each user account but multiple textual passwords are difficult to memorize; therefore, users generally set similar passwords on different accounts [4,5]. Another issue with textual passwords is that the strong passwords, i.e., which contain a combination of alphanumeric characters and have larger length, are difficult to remember. The strong passwords are better for security against off-line guessability attacks [6]. Making a strong password easy to memorize is a challenge in textual and graphical password schemes.

Graphical passwords are considered to be better than textual passwords with respect to memorability [7] because pictures contain visual cues for password memorization. However, wrong selection of pictures in a graphical password scheme negatively affects the password memorability. For example, culturally familiar pictures are easy to memorize but unfamiliar pictures [8] are difficult to memorize.

One way of improving the security of authentication process is to add more than one factors for authentication [9]. A user may be logged-in after providing password and a code received in a device such as cell phone. Adding more than

B Shah Zaman Nizamani
shahzaman@quest.edu.pk

Syed Raheel Hassan
rhassan1@kau.edu.sa

Riaz Ahmed Shaikh
rashaikh@kau.edu.sa

[1] Quaid-e-Awam University, Nawabshah, Pakistan

[2] King AbdulAziz University, Jeddah, Saudi Arabia

one factors improves the security of authentication process but the login process becomes lengthy [10] as a result usage of multiple factors for authentication is limited.

Due to security and memorability issues in traditional textual password scheme, researchers have proposed many graphical password schemes [11,12]; some schemes are more secure while other schemes are easy to use. Relatively secure graphical password schemes have usability issues such as long authentication time and high input error rate, and they are difficult to learn. Easy-to-use graphical password schemes have many security issues such as low password space, and in most cases passwords are easy to observe from the login screen.

Many knowledge-based authentication schemes are proposed for replacing textual password scheme. Researchers have proposed many evaluation models and guidelines for analyzing the schemes. One of the main weaknesses of the evaluation models is that their evaluation process is often ambiguous, i.e., evaluators find difficulty in correctly assigning values to parameters of the models. For example, in evaluation model proposed by Mihajlov et al. [13], an evaluator has the option to select a value from the ten-point scale (0.0 to 1.0) for the parameter "convenience." In this model, the correct values are difficult to assign because the model does not provide clear definitions for all the scale points. Another issue with the evaluation models is that their analysis results do not clearly indicate the idea about strengths and weaknesses which exist in the schemes.

In this paper, an evaluation model (TQ-Model) is proposed for knowledge-based authentication schemes. In the proposed model, evaluation is done on the basis of different parameters. The evaluation process is simplified by defining criteria for assigning values to the parameters. Furthermore, TQ-Model is compared with two existing evaluation models, to highlight advantages of TQ-Model against the existing models.

The remaining paper is divided into seven sections. In Sect. 2, graphical password schemes and evaluation models are discussed. TQ-Model is explained in Sect. 3. In Sect. 4, PCCP scheme is analyzed with different evaluation models. Analysis of famous authentication schemes is given through the TQ-Model in Sect. 5. Limitations of the TQ-Model are discussed in Sect. 6. Finally, conclusion is given in Sect. 7.

2 Literature Review

This section consists of two parts. In the first part, famous graphical password schemes are described, whereas in the second part, evaluation models for authentication schemes are discussed.

2.1 Graphical Password Schemes

In textual password scheme, the passwords consist of alphanumeric characters, while in graphical password schemes, the passwords consist of graphical elements such as pictures, lines or some points inside a screen. The graphical password schemes which use pictures as password are called recognition-based schemes. The schemes which use lines as passwords are called pure recall-based schemes while the schemes which use points as passwords are called cued recall-based schemes. Some graphical password schemes use combination of two or more types of passwords. For example, in GOTPass (graphical one-time password) scheme passwords consist of pictures and lines.

Jermyn et al. [14] proposed a pure recall-based graphical password scheme known as DAS (draw-a-secret). In this scheme, a password consists of some lines inside a blank grid-based login screen. For authentication, users need to redraw the password lines in the login screen. This scheme is not resilient to shoulder surfing and spyware attacks because the passwords can be easily viewed and recorded from the login screen. A variation in the DAS scheme was proposed by Google in Android operating system known as Android unlock scheme [15]. In this scheme, passwords consist of some lines inside a 3 * 3 grid-based login screen. In this scheme, small amount of time is required for authentication but it has same security issues that exist in the DAS scheme [15].

Dunphy et al. [16] added background image in the grid-based login screen for improving password memorability. This new scheme is called as background DAS (BDAS). This scheme has memorability advantages but the passwords can be viewed and recorded from the login screen; therefore, BDAS scheme is also weak with respect to shoulder surfing and spyware attacks.

A graphical password scheme introduced by Microsoft in Windows 8 operating system is known as picture gesture authentication (PGA) [17]. In this scheme, the passwords consist of lines, circles or some points inside a picture. Users can set their own background picture for the login screen. This scheme provides large password space but it suffers from hot spot and shoulder surfing attacks.

Passface scheme [18] is a recognition-based graphical password scheme. In this scheme, 45 images are presented in five screens for password selection. Each screen contains nine images of human faces in a 3 * 3 grid-based login screen. A user has to correctly select one password image from each of the screen. This scheme has low password space as a result guessability attacks can be applied.

Wiedenbeck et al. [11] proposed a recognition-based graphical password scheme known as CHC (convex hull click). In this scheme, hundreds of icons are shown on the registration screen from which password images are selected.

For authentication, users need to click on a logical triangle formed by the password icons inside the login screen. Authentication process consists of multiple rounds of password selection; therefore, mean authentication time of the CHC scheme is more than one minute.

Shankara et al. [19] proposed a graphical password scheme for smartphones. In this scheme, a password consists of different images along with the time duration recorded during each image selection. For login, a user holds the same image buttons for the same time duration which was selected during the time of password selection. The time duration allocated for selecting an image is difficult to recognize by attackers but users also face the same difficulty for authentication.

Chakraborty et al. [20] proposed an authentication scheme for smartphones. Passwords of this scheme consist of capital alphabets and numbers. For authentication, a user has to correctly select alphabets or numbers of the password, depending upon the challenge received from the audio signals. This scheme resists online security attacks such as shoulder surfing and multiple recording attacks but it is weak against brute-force and dictionary attacks because this scheme provides only 36 elements for password creation.

2.2 Evaluation Models

For analysis of the authentication schemes, researchers have proposed different evaluation models or frameworks. In this section, these evaluation models are discussed.

Bonneau et al. [21] suggested a framework or evaluation model for user authentication schemes. In this framework, a list of features is identified with respect to security, usability and deployability. Evaluation is done by identifying status of all the features, i.e., whether a feature is fully implemented, semi-implemented or not implemented.

Mihajlov et al. [13] suggested a conceptual framework or evaluation model for security and usability evaluation of graphical password schemes. In the suggested framework, areas for evaluation are highlighted and the rating is given to each area or feature from “0” to “1.” The “0” rating shows a feature has a high level of deficiency while a rating of “1” shows no deficiency. In the proposed framework, quantification process is very ambiguous, and the evaluator may get different values on each evaluation session.

English and Poet [22] proposed a hierarchical model for the security evaluation of recognition-based graphical password schemes. In this model, hierarchies of different security attacks are defined. Evaluation is done by mapping a user scheme with the identified hierarchies. The model only deals with the security of recognition-based graphical password schemes, whereas other categories of graphical passwords are missing. Usability and memorability areas of user authentication schemes are also missing in the model.

Khodadadi et al. [23] highlighted the attributes for analyzing security and usability of recognition-based graphical password schemes. However, authors have not defined any method for quantification of the attributes. Also, they did not present attributes for recall-based and hybrid graphical password schemes.

Lashkari et al. [24] identified usability and security features for analyzing user authentication schemes. The researchers have provided a comparison of different recall-based graphical password schemes, based upon the identified features. The comparison is given through expert judgment, and only two level of rating is used for evaluation. With the help of identified features, a detailed level evaluation cannot be made for the authentication schemes.

Renaud [25] proposed a quantification model for analyzing the quality of web-based user authentication schemes. In this model, features or concerns are identified along with rating values. For evaluation, values need to be assigned to the features depending upon the performance of a scheme. In the proposed model, assigning correct values is a difficult task because no clear definition is given for selecting a value.

Velásquez et al. [26] proposed an evaluation frame- work called Kontun to select an authentication category for a specific application. In this framework, an authentication technique (knowledge-based, biometric or token-based) is identified which is suitable for a specific scenario. Knowledge-based authentication techniques require a password for authentication which may be graphical or alphanumerical. Biometric techniques use physical characteristics of a user for authentication, and token-based techniques require some hardware for authentication. This framework is easy to use but it only identifies one category of authentication technique, suitable for a particular application. This framework does not help in selecting an authentication scheme such as PGA, Android unlock and Passface.

Still et al. [27] proposed six usability guidelines for authentication schemes. These guidelines can help in improving the usability of the schemes. However, in authentication, security and usability have some conflicting requirements. Therefore, only utilizing usability guidelines may negatively affect security.

Evaluation models or frameworks have different strengths and weaknesses. Some evaluation models do not completely evaluate the authentication schemes such as Still’s model [27]. In some models, it is difficult to assign values to the parameters such as Mihajlov’s model [13], while results of some evaluation models do not give a clear understanding about the performance of the schemes such as Bonneau’s model [21]. In TQ-Model, these issues are solved by giving a simple quantitative approach for analyzing the authentication schemes.

3 TQ-Model

In TQ-Model, traditional textual password scheme is taken as a base for analyzing the knowledge-based authentication schemes. The reason for this approach is that all the authentication schemes are designed to solve the weaknesses of traditional textual password scheme.

TQ-Model contains 28 parameters for evaluation. The parameters cover security, usability and memorability aspects of an authentication scheme. Security parameters are derived from those aspects, which are exploited by various password security attacks [28]. For example, brute-force attack uses all password combinations or password space to break password. Therefore, "password space" is set as a security parameter of the model. Users' behavior of selecting the passwords also creates security risks from different attacks [29] such as dictionary attack. In order to highlight this issue, the TQ-Model contains a parameter called "educated password guessing." Similarly, passwords can be recorded or observed from login screens [30]; therefore, for measuring security of password insertion process, the parameters such as "password visibility" and "password logging" are added into the model.

Usability parameters of the TQ-Model can be divided into two categories. One category of parameters is quantitative nature [31] such as mean login time and mean registration time, and another category of parameters is qualitative nature such as graphical design and mental effort. Quantitative parameters are derived from the usability performance of textual password scheme, while qualitative parameters are mostly derived from usability heuristics [32] and usability evaluation methods [21]. However, in case of memorability aspect of the TQ-Model, all the parameters are derived from the field of human memory [33,34].

Evaluation is done by assigning a score or rating to each of the parameter of TQ-Model. Block diagram of the evaluation process is shown in Fig. 1.

The ratings are given on the basis of some criteria which are listed in Tables 1, 2 and 3. Criteria for all the parameters are set on the basis of traditional textual password scheme. When performance of a scheme appears within the range of textual password scheme, then zero or base rating is given. A positive rating is given when the performance is better than textual password scheme, while negative score is assigned when the performance is weaker than textual password scheme. Criteria for assigning scores are defined inside the model in order to minimize ambiguities of assigning scores. Security parameters of TQ-Model are explained in the following section.

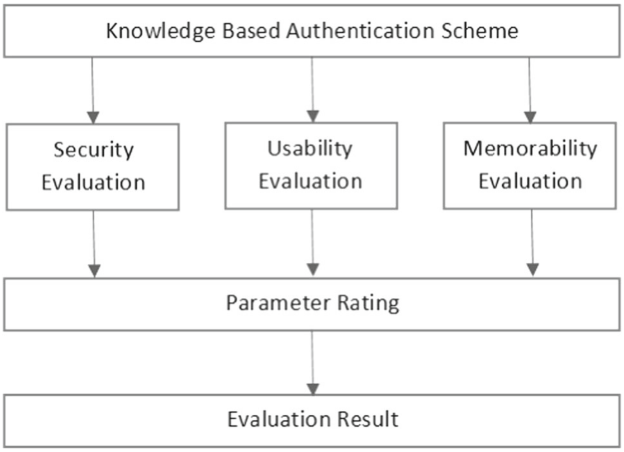

Fig. 1 Evaluation process

3.1 Security Parameters of TQ-Model

In Table 1, security parameters are listed along with criteria of different ratings. All the security parameters and their criteria for assigning scores are discussed here in detail.

3.1.1 Password Space

The password space needs to be high in order to improve security against guessability attacks. The password space depends upon the number of elements provided by an authentication scheme for password creation. Base rating for this parameter is set from 80 and 110 elements. This range is selected because textual password scheme contains 95 alphanumeric characters for password creation [35]; subtracting and adding 15 elements in the textual passwords range (95) will give the numbers 80 and 110, respectively. All the schemes which contain 80 to 110 elements will require almost same effort for password guessing as in traditional textual password scheme. Table 1 gives range of different ratings for this parameter.

3.1.2 Password Visibility

An attacker can view passwords through a camera recording or by directly observing a login activity. In textual password scheme, passwords can be viewed by recording a login session but the passwords are difficult to view directly from login screen without camera recording. Therefore, the base rating is assigned to the authentication schemes where passwords can be viewed through a camera recording but they cannot be viewed directly from the login screen. Positive score is assigned when passwords cannot be viewed through camera recording of a login session.

Table 1 Security parameters

Parameter	Criteria	Rating
Password space	Greater than 150 elements	2
	From 111 to 150 elements	1
	From 81 to 110 elements	0
	From 51 to 80 elements	−1
	Less than 51 elements	−2
Password visibility	Cannot be viewed by camera recording	1
	Can be viewed by camera recording	0
	Can be viewed directly from login screen	−1
Intersections required for password break	Recordings of more than 50 login sessions are required for password break	3
	From 26 to 50 login sessions required	2
	Up to 25 login sessions are required	1
	Single login session required	0
Educated password guessing	Cues and password dictionaries are not available for password guessing	1
	No cues available for guessing	0
	Cues available for guessing	−1
Password logging	Passwords cannot be captured by keystroke or mouse loggers	1
	Passwords can be captured by keystroke or mouse loggers	0
Password sharing	Very difficult to write passwords	2
	Require some description for password writing	1
	Passwords are easy to write	0
Password storage	Passwords can be stored with hashing algorithms	0
	Two-way encryption is required for password storage	−1
Eavesdropping	Actual passwords can be captured from a network or communication medium	0
	Actual passwords cannot be captured from a network	−1
Authentication factors	Single	0
	Two	1
	More than two	2

3.1.3 Intersections Required for Password Break

In textual password scheme, single recording of a single login session is enough for password capture because one-to-one mapping exists between key press and a password element selection. However, in some user authentication schemes, a password is captured after recording multiple login sessions such as CHC scheme [11]. The schemes which require large number of recordings or intersections are considered to be strong against observability attacks. Base or zero rating for this parameter is assigned when information of single login session is enough for password capture. A positive rating is given to the schemes where recordings of more than one login session are required for capturing a password.

3.1.4 Educated Password Guessing

A password may be guessed by using profile information of a user such as name, date of birth or favorite items. In recognition-based graphical password schemes, culturally familiar or attractive pictures have more chances of selection for the passwords [36]. The attacker may exploit the cues such as attractiveness, race or culture of a user for guessing a password. Abstract art pictures provide better security against educated guessing attack [37] because these pictures do not provide cues for educated password guessing attacks.

In textual password scheme, passwords are difficult to guess by profile information of a user. However, some textual passwords may be guessed by utilizing password dictionaries. Therefore, the base rating is assigned to the schemes where user profile information does not provide any cue for password guessing but small chances exist with dictionary attacks.

3.1.5 Password Logging

Spyware applications send authentication information to an attacker without consent of a user. In textual

Table 2 Usability parameters

Parameter	Criteria	Rating
Mean registration time	Less than 11 seconds	1
	From 11 to 20 seconds	0
	From 21 to 40 seconds	−1
	From 41 to 60 seconds	−2
	Greater than 60 seconds	−3
Mean login time	Less than 6 seconds	1
	From 6 to 10 seconds	0
	From 11 to 20 seconds	−1
	From 21 to 40 seconds	−2
	From 41 to 60 seconds	−3
	Greater than 60 seconds	−4
Password input methodology	Passwords are directly inserted	0
	Passwords are indirectly inserted	−1
Password input flexibility	Passwords are inserted through keyboard or mouse	0
	Either keyboard or mouse is used for password insertion	−1
Physical effort	No significant effort required	0
	Require some effort	−1
Mental effort	No effort required	0
	Require some effort for password element searching	−1
	High-level effort required for password element searching or insertion	−2
Requirements for execution	Hardware and software not required	0
	Software required	−1
	Hardware required	−2
	Both hardware and software required	−3
Effect of human disabilities	No effect of common disabilities	0
	Have effect of common disabilities	−1
Size of assets	Less than 100 kb	0
	From 101 kb to 500 kb	−1
	Greater than 500 kb	−2
Internal processing	No significant processing required	0
	High processing required	−1
Applicability	Execute smoothly on every kind of device	0
	Cannot execute smoothly on every kind of device	−1
	Designed for specific category of devices	−2
Learnability	Easy	0
	Moderate	−1
	Difficult	−2
Graphical design	Pleasant	1
	Average	0
	Dull	−1

password scheme, passwords can be recorded by keystroke loggers because exact password characters are inserted into a password field. Base rating for this parameter is given to the schemes where actual password elements are inserted into a password field or one-to-one mapping exists between one user action (keypress or mouse click) and a password element selection. A positive rating is given to the schemes where one-to-one mapping does not exist.

Table 3 Memorability parameters

Parameter	Criteria	Rating
Freedom of password selection	Users can upload pictures	2
	Wide range of options present	1
	Users cannot upload pictures	0
Pictures type (for recognition-based schemes)	Pictures contain common objects and presentation is also good	1
	Pictures contain common objects but presentation is not good	0
	Pictures contain unknown objects	−1
	Pictures contain unknown objects and presentation is also weak	−2
Pictures type (for recall-based schemes)	Objects inside a picture are familiar and well placed	1
	Objects inside a picture are familiar but not well placed	0
	No background picture is used	−1
	Objects inside a picture are unknown and not well placed	−2
Minimum password length	Less than 6	1
	From 6 to 8 elements	0
	From 9 to 12 elements	−1
	Greater than 12 elements	−2
Password selection rules	No restriction	2
	One restriction	1
	Two restrictions	0
	More than two restrictions	−1
Order	Not required	1
	Required	0
Password elements	Fixed	0
	Depend upon configuration	−1
	Variable	−2

3.1.6 Password Sharing

Textual passwords can be easily verbalized or written into a text file. The password file can be hacked or unintentionally shared with the attacker. Base rating for this parameter is given to the schemes where passwords can be easily written. A positive rating is given to the schemes where password elements are difficult to describe or write. For example, graphical password elements such as pictures or locations inside a picture are difficult to write or verbalize; therefore, unintentional password sharing is less in such type of passwords.

3.1.7 Password Storage

Information can be security with hashing or two-way encryption. For a password storage, hashing is more secure because hashed passwords are difficult to guess. Textual passwords can be stored with hashing, while there are some schemes where passwords need to be stored with two-way encryption. Base rating is given in the parameter when a scheme allows passwords to be stored with hashing, while negative rating is given when a scheme only allows two-way encryption for password storage.

3.1.8 Eavesdropping

In client server scenario, a password moves across different networks to reach on a server. If real password elements move within the communication channels, then chances of password capture increase. Therefore, it is better for a scheme to use encrypted or one-time password for authentication. In textual password scheme, password characters move across a network; therefore, base rating is given to the schemes where exact password elements moves in a communication channel.

3.1.9 Authentication Factors

In textual password scheme, a user is authenticated when required information (password) is provided. Authentication process can be more secured by adding more factors along with a password. For example, along with a password, a code may be required for authentication which may be received in cell phone. As single factor is required in traditional textual password scheme, therefore base rating is given to the schemes where single factor is enough for authentication.

3.2 Usability Parameters of TQ-Model

Generally, graphical password schemes are weaker than textual password scheme with respect to usability. Only Android unlock scheme provides better usability than textual password scheme in the domain of smartphones. The usability parameters and evaluation criteria are presented in Table 2. Usability parameters of the TQ-Model and criteria for assigning score are discussed here.

3.2.1 Registration Time

In textual password scheme, a very short amount of time is required for password registration. However, most graphical password schemes have a complex method of password registration, which may take more than one minute. Base rating for this parameter is given when registration time is up to 20 seconds, whereas negative rating is given when more than 20 seconds are required for password registration.

3.2.2 Login Time

Login time is very important with respect to the usability of an authentication scheme. In different knowledge-based authentication schemes, login time varies from few seconds to a couple of minutes. In textual password scheme, the range of login time is generally between 5 and 10 s. Therefore, the base rating is given when average login time is up to 10 s, whereas negative rating is given when average login time is more than ten seconds.

3.2.3 Password Input Methodology

Passwords are indirectly inserted into a login screen in order to improve the security of passwords from online attacks. For example, in cognitive authentication schemes [38] users do not need to click on password icons but they have to select a path which indirectly represents a password image. Although password security improves when passwords are indirectly inserted, this approach has usability disadvantages such as long authentication time and reduction of password input accuracy.

In textual password scheme, passwords are directly inserted into a password field. Therefore, the base rating is given to the authentication schemes where passwords are directly inserted, i.e., users click or type exact password elements.

3.2.4 Password Input Flexibility

Textual passwords can be easily inserted through keyboard or mouse. This flexibility is also required in graphical password schemes for ease of use. Base rating for this parameter is given when authentication credentials can be easily given through keyboard or mouse.

3.2.5 Physical Effort

In textual password scheme, users just need to type some password characters, which do not require significant physical effort. However, graphical password schemes may require some physical effort for password entry. For example, in PCCP (persuasive cued click-points) scheme [39] users need to select a password cell and click on the picture that appears after selecting the cell. This process of password elements selection is repeated multiple times; therefore, PCCP scheme is weak with respect to physical effort. Base rating is given to the schemes where selection of password elements does not require any significant physical effort, whereas negative rating is given when some physical effort is required for password selection.

3.2.6 Mental Effort

Authentication process becomes time consuming when password entry requires some computations or searching of the password elements. For example, in CHC scheme [11] users are required to search password elements from a list of one thousand pictures, as a result more effort is required for password image searching. In textual password scheme, passwords are recalled from memory, which does not require any mental effort except password recalling. Base rating is given to the authentication schemes where mental effort is required only for recalling the password elements.

3.2.7 Requirements for Execution

An authentication scheme may require a special hardware or software for proper execution. The hardware or software requirements may be at server side or client side. Textual password scheme can execute in ordinary configuration systems; therefore, negative rating is given to the authentication schemes which require some additional hardware or software for execution, and base rating is given to the schemes where such requirements do not exist.

3.2.8 Effect of Human Disabilities

Human disabilities such as low eyesight or other old age factors may hinder the authentication process; therefore, user interface of an authentication scheme needs to be resilient to such human disabilities. Textual password scheme does not contain such limitations. Therefore, the base rating is given to the authentication schemes where ordinary users can easily complete the authentication tasks, whereas a negative rating is assigned when the authentication process is difficult to complete with any physical disability.

3.2.9 Size of Assets

Traditional textual password scheme requires only two fields for authentication which are username and password fields, as a result small size of assets are required for login screen generation. Graphical password schemes may require large amount of assets for execution. Graphical password schemes require some graphical elements such as pictures for execution. The large size of graphical assets (such as pictures, CSS and JavaScript files) take some time to load authentication page, especially in the web-based environment, which negatively affects the usability of an authentication scheme. For example, Passface scheme [18] requires 45 images for authentication process, which may increase page loading time. Therefore, the base rating is given to the schemes where small size of assets are required for authentication.

3.2.10 Processing for Execution

Very small amount of processing is required in textual password scheme for login screen generation and password matching. However, graphical password schemes may require heavy processing for login screen generation or password matching. For example, 3D password scheme [40] requires a large amount of processing for password screen generation. For this parameter, the base rating is given when low processing is required for execution of the schemes.

3.2.11 Applicability

Textual password scheme can be easily used with any kind of device (desktop, mobile, etc) and environment. However, graphical password schemes may be difficult to execute after changing device or screen dimensions. For example, in CHC scheme one thousand password icons are recommended for authentication process and the large number of icons is not suitable for smartphone screen.

3.2.12 Learnability

New processes require some time for understanding. Authentication schemes become easy to learn when frequently used techniques or approaches are used for different authentication processes. A completely new authentication techniques are difficult to learn. Therefore, base rating for this parameter depends upon familiarity of the authentication process.

3.2.13 Graphical Design

Authentication process becomes easy when a scheme provides aesthetically pleasant graphical design and contains small number of steps for authentication. Rating for this parameter is given on the basis of graphical look and feel of an authentication scheme.

3.3 Memorability Parameters of TQ-Model

Authentication credentials are required to be remembered in knowledge-based authentication schemes. In textual password scheme, a password consists of alphanumeric characters, while in graphical password schemes, visual elements such as pictures or drawings are used for a password.

All the schemes where alphanumeric characters are used as password elements will have equal memorability ratings as in traditional textual password scheme. Therefore, the TQ-Model contains memorability parameters for analyzing graphical password schemes. All the parameters are given in Table 3. Memorability parameters of the TQ-Model and criteria for assigning score are discussed here.

3.3.1 Freedom of Password Selection

In textual password scheme, users are allowed to create any password from a limited set of alphanumeric characters, while in graphical passwords, a large number of images can be used for password selection or users may be allowed to upload their password pictures. Freedom of password selection has positive effect on password memorability.

3.3.2 Pictures Type

Memory cues help in long-term memorization of information [41]. In textual passwords, only cognitive cues can be used for password memorization, such as a name of a person. Graphical passwords contain both visual and cognitive cues such as birth date and picture as a password element. Therefore, graphical passwords are generally easy to remember than textual passwords. However, a poor presentation or selection of pictures can eliminate the picture superiority effect [42]. Recognition-based graphical password schemes are fundamentally different from recall-based graphical password schemes. In such schemes, users have to correctly identify their password pictures, whereas in recall-based graphical password schemes, password elements (points or lines) need to be recalled. Therefore, criteria for the parameter “pictures type” are separately presented in the TQ-Model as shown in Table 3.

3.3.3 Minimum Password Length

Generally, minimum length of eight alphanumeric characters is followed in textual password scheme. The rating for this parameter for graphical password schemes can be given according to the textual password scheme. Criteria for this parameter are given in Table 3.

3.3.4 Password Selection Rules

Users can create a password from an available set of password elements (alphanumeric character or pictures) but they are restricted to set a certain kind of passwords in order to improve the password security. In textual passwords, users are restricted to select passwords from at least two categories such as small alphabets and numbers. Therefore, restrictions for password setting need to be such that passwords can be easily memorized.

3.3.5 Order

In textual password scheme, order of password characters is important, i.e., a user needs to enter password in the order in which password was registered. For memorability perspective, orderly recalling password elements may require extra effort. Therefore, rating "1" will be given for the authentication schemes where order is not important.

3.3.6 Password Elements

Separate passwords for different accounts are difficult to memorize; therefore, users generally set same or similar passwords in different accounts. Although setting same password in different accounts has security weakness, it decreases cognitive load on users for password memorization. For allowing a user to set same password across different implementations of an authentication scheme, a fixed set of password elements are required. In textual password scheme, a fixed set of password elements are used; therefore, rating "0" is given to all the authentication schemes where password elements are standardized or fixed.

4 Analysis of PCCP Scheme with Different Evaluation Models

In this section, PCCP (persuasive cued click-points) scheme [39] has been analyzed by three evaluation models that include TQ-Model, Bonneau's model [21] and Mihajlov's model [13]. The analysis has been conducted to find out the strengths and weaknesses of all the evaluation models. The reason for selecting Bonneau's and Mihajlov's model along with TQ-Model is that they provide complete analysis of the authentication schemes. Rest of the models either contain limited features for evaluation or they evaluate single category of authentication schemes. For example, the evaluation model proposed by English and Poet [22] only evaluates security aspect of recognition-based graphical password schemes. However, usability and memorability evaluation features are missing from the model.

4.1 Analysis of PCCP Scheme with Bonneau's Model

In Bonneau's evaluation model, different parameters are defined for analyzing security, usability and deployability aspects of an authentication scheme. The model works on the idea whether an authentication scheme offers benefits or not with respect to the defined parameters. Evaluation is done by mentioning, whether the parameters are fully implemented, quasi (little bit) implemented or not implemented in an authentication scheme (such as PCCP scheme). Tables 4, 5 and 6 show the analysis of PCCP scheme with respect to Bonneau's model.

Table 4 Security evaluation of PCCP scheme with Bonneau's model

Parameter	Rating
Resilient to physical observation	Not implemented
Resilient to targeted impersonation	Fully implemented
Resilient to throttled guessing	Quasi implemented
Resilient to unthrottled guessing	Not implemented
Resilient to internal observation	Not implemented
Resilient to leaks from other verifiers	Not implemented
Resilient to phishing	Implemented
Resilient to theft	Quasi implemented
No trusted third party	Implemented
Requiring explicit consent	Implemented
Unlinkable	Implemented

Table 5 Usability evaluation of PCCP scheme with Bonneau's model

Parameter	Rating
Memorywise effortless	Not implemented
Scalable for users	Not implemented
Nothing to carry	Implemented
Physically effortless	Not implemented
Easy to learn	Implemented
Efficient to use	Quasi implemented
Infrequent errors	Quasi implemented
Easy recovery from loss	Implemented

Table 6 Deployability evaluation of PCCP scheme with Bonneau's model

Parameter	Rating
Accessible	Not implemented
Scalable for users	Not implemented
Negligible cost per user	Implemented
Server compatible	Not implemented
Browser compatible	Implemented
Mature	Not implemented
Non-proprietary	Implemented

Table 7 Security evaluation of PCCP scheme with Mihajlov's model

Parameter	Rating
Secrecy	0.22
Abundance	0.66
Revelation	0.33
Privacy	1
Breakability	0.75

Table 8 Usability evaluation of PCCP scheme with Mihajlov's model

Parameter	Rating
Processing depth	0.34
Meaningful retrieval	0.75
Requirements	0.67
Convenience	0.4
Inclusivity	0.85

4.2 Analysis of PCCP scheme with Mihajlov's Model

In Mihajlov's evaluation model, different parameters are defined for analyzing security and usability dimensions of the authentication schemes, while memorability is considered to be a part of usability. Evaluation is done by assigning different scores according to the scale defined in the model. Tables 7 and 8 show the analysis of PCCP scheme with respect to Mihajlov's model.

4.3 Analysis of PCCP scheme with TQ-Model

In TQ-Model, the authentication schemes are analyzed on the basis of different parameters related to security, usability and memorability. Evaluation is done by assigning ratings to the parameters. Tables 9, 10 and 11 show the analysis results of PCCP scheme with respect to TQ-Model.

4.4 Analysis of the Evaluation Models

Evaluation process is easy in Bonneau's model as it contains a scale with only three values (fully implemented, quasi implemented and not implemented). However, it is difficult to know a detailed analysis of an authentication scheme in the Bonneau's model. For example, evaluation result shows that PCCP scheme does not implement the parameter "resilient to unthrottled guessing" (as given in Table 4), but this rating does not indicate how much weak PCCP scheme is against "resilient to unthrottled guessing."

Mihajlov's model is difficult to implement, and similarly, evaluation results are also difficult to understand. For example, in order to rate usability parameter "processing depth" an evaluator has to rate three sub-parameters which are cognitive

Table 9 Security evaluation of PCCP scheme with TQ-Model

Parameter	Rating
Password space	−2
Password visibility	−1
Intersections required for password break	0
Educated password guessing	0
Password logging	0
Password sharing	2
Password storage	−1
Eavesdropping	−1
Authentication factors	0

Table 10 Usability evaluation of PCCP scheme with TQ-Model

Parameter	Rating
Mean registration time	− 2
Mean login time	− 1
Password input methodology	0
Password input flexibility	− 1
Physical effort	− 1
Mental effort	− 1
Requirements for execution	− 2
Effect of human disabilities	− 1
Size of assets	− 2
Internal processing	0
Applicability	− 1
Learnability	− 1
Graphical design	0

Table 11 Memorability evaluation of PCCP scheme with TQ-Model

Parameter	Rating
Freedom of password selection	0
Pictures type	1
Minimum password length	0
Password selection rules	0
Order	0
Password elements	0

Table 12 Comparison of the evaluation models

Parameter	TQ-Model	Bonneau’s model	Mihajlov’s model
Evaluation parameters	Security, usability and memorability	Security, usability and deployability	Security and usability
Total parameters	28	25	10
Rating level	2 to 6	3	Level is not fixed
Rating scale	Numerical	Descriptive	Numerical
Ambiguity of evaluation	Small	Small	High
Evaluation process	Easy	Easy	Difficult
Evaluation result	Detailed	Summarized	Summarized
Comparative result	Yes (with textual password scheme)	No	No

effort, visual effort and rehearsal effort. It is quite possible that a wrong input may be given, as there is no clear definition of selecting a value. Evaluation results are also difficult to interpret because the results are presented in summarized format.

The authentication schemes can be easily evaluated through TQ-Model because criteria of the rating are defined. For example, in PCCP scheme “−2” rating is given to the parameter “mean registration time” because average registration time for the PCCP scheme is 50.7 s which is equivalent to “−2” rating of the TQ-Model as given in Table 2. This rating clearly indicates that password registration process of PCCP scheme is very difficult in comparison with traditional textual password scheme.

Comparison of TQ-Model, Bonneau’s model and Mihajlov’s model is given in Table 12.

5 Evaluation of Different Authentication Schemes with TQ-Model

In this section, three authentication schemes are compared with the traditional textual password scheme with the help of the TQ-Model. The schemes are Android unlock scheme [15], picture gesture authentication (PGA) [17] and Passface scheme [18].

For the evaluation, all the schemes are analyzed against each parameter defined inside the model. The data for the schemes are extracted from literature review. The ratings for the parameters are given according to the extracted data. For example, a number of elements are considered before allocating a score for the parameter “password space.” In the PGA scheme, rating “+2” is given for the parameter “password space” as shown in Fig. 2. This rating is given according to the scale given in Table 1. Any scheme if contains more than 150 elements will be given rating “+2.” The PGA scheme contains more than 150 elements; therefore, this rating (+2) is given. Similarly, “−2” rating is given for both Android unlock and Passface scheme as they contain less than 51 elements for password creation. Usability and memorability evaluation is also done after considering all the features of the schemes against the parameters of the TQ-Model.

Security evaluation of all these schemes is presented in Fig. 2. The results show that PGA scheme is more secure than Android unlock and Passface scheme because this scheme has received the highest cumulative score against the security parameters.

Usability evaluation is shown in Fig. 3. Results show that Android unlock scheme is better than PGA and Passface scheme because it provides better performance against different usability parameters of the TQ-Model. PGA scheme is weakest among all the schemes as shown in Fig. 3.

Password memorability evaluation of all the schemes is shown in Fig. 4. Results show that overall performance of PGA scheme is better than other schemes with respect to memorability because most numbers of positive scores are assigned to this scheme.

By applying the evaluation process of TQ-Model, overall quality of the authentication schemes is shown in Fig. 5. Results show that PGA scheme is better than Android and Passface scheme with respect to security and memorability because it gets more quality points (3 in security and 4 in memorability). However, in case of usability PGA scheme is very weak among all the schemes because it has got “−10” points. With respect to usability, Android unlock scheme is better than other schemes.

6 Discussion

The finding of the proposed model is that it gives quantitative results same as other evaluation models, but the evaluation results of the TQ-Model are easy to understand as they are presented in comparison with traditional textual password scheme. Additionally, TQ-Model individually highlights strong and weak aspects of the authentication schemes by using different parameters. The implication of proposed model opens, for further research in the category

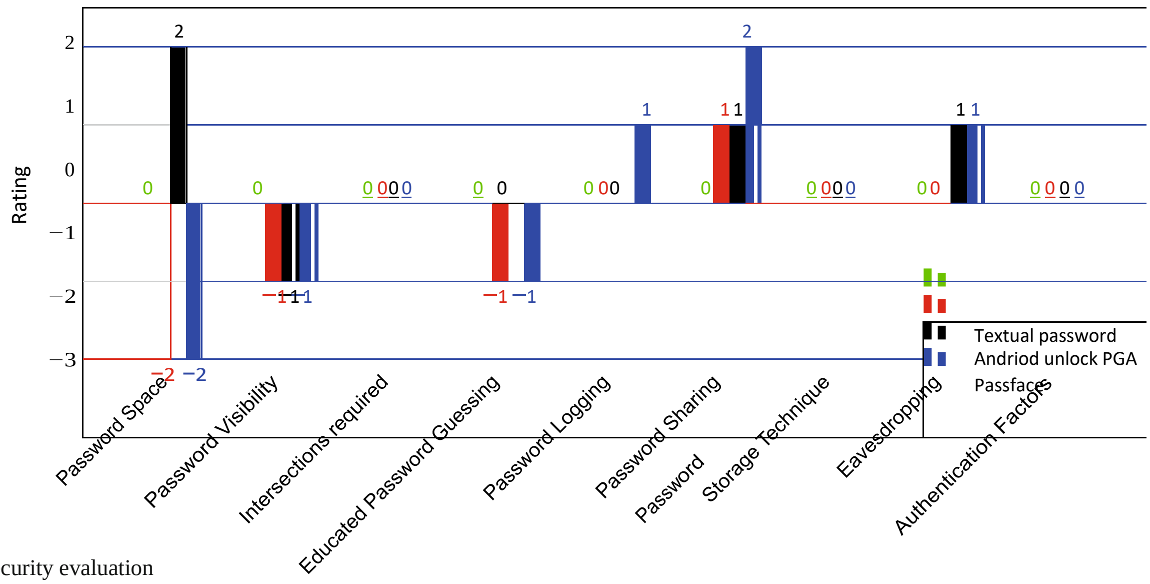

Fig. 2 Security evaluation

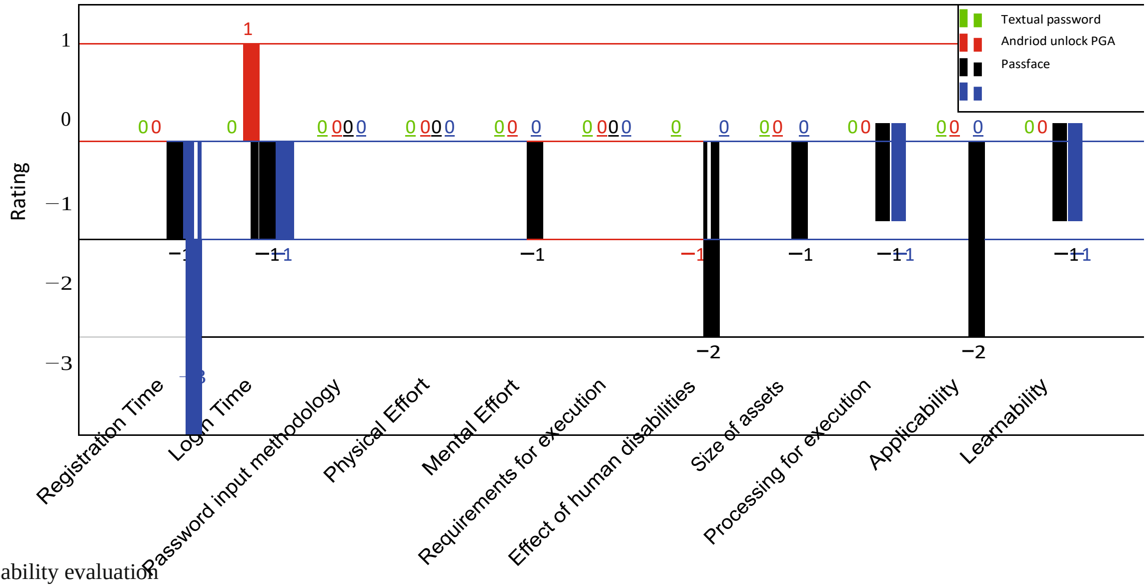

Fig. 3 Usability evaluation

of graphical passwords related to shoulder surfing attacks which are based on observability. Therefore, further research needs to be done in the area of observability of the schemes.

Authentication systems use different types of credentials for identifying the users. These credentials may be in the form of some information (password), physical characteristics of a user or some hardware. The TQ-Model is limited for the systems which use some information for authentication. Further research is required in other categories of the login credentials.

Current password creation policies of textual passwords are taken as standard for setting base ratings in the TQ-Model. However, the base ratings can be updated when password

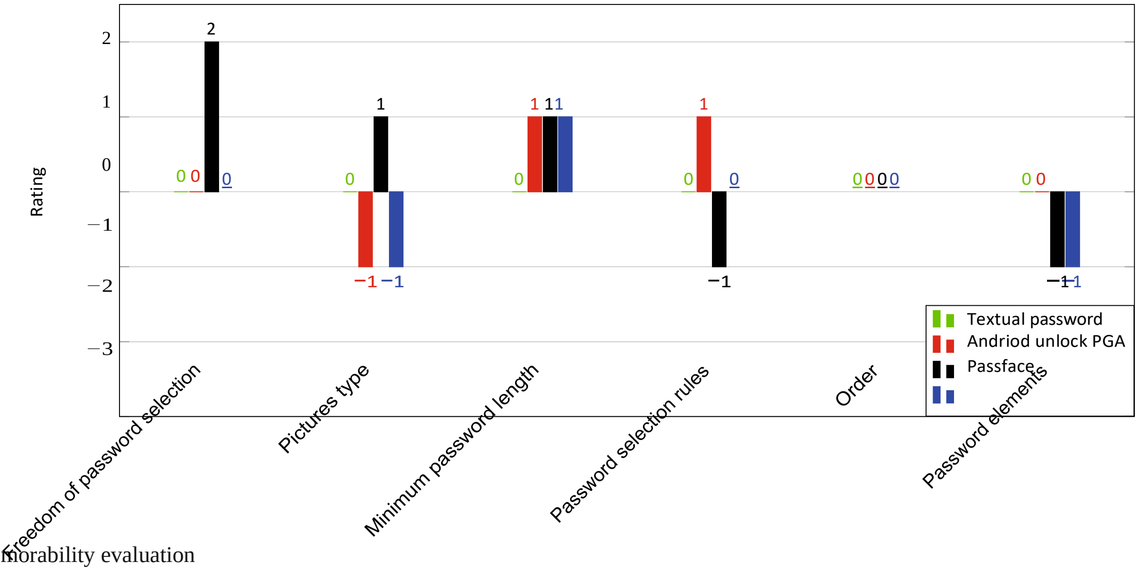

Fig. 4 Memorability evaluation

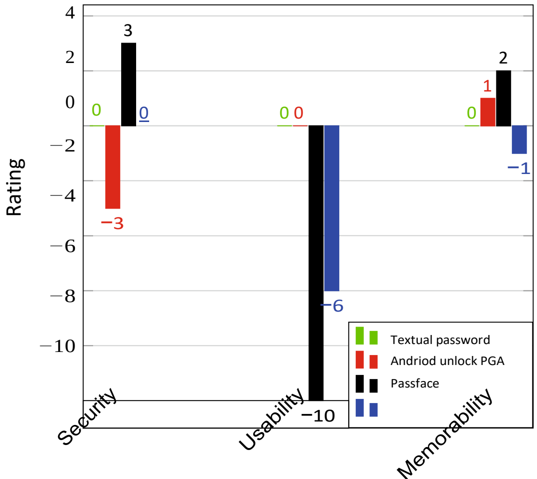

Fig. 5 Overall quality of the authentication schemes

setting policies of traditional textual password scheme change in future.

In the proposed model, there are some parameters which are qualitative by nature. Humans may have different perceptions for understanding things of qualitative nature. Therefore, the evaluator may provide slightly different values for qualitative parameters. However, this difference of input may not affect the overall evaluation result as shown in Fig. 5.

7 Conclusion

The main research problem as discussed in this paper is related to target the evaluation of different authentication schemes. Presently, no standard authentication scheme has been proposed; therefore, research is ongoing in the field of authentication. The evaluation models are important in analyzing efficiency of different authentication schemes. However, the current evaluation models are either difficult to use or their analysis results are difficult to interpret.

To overcome the above-mentioned issue, TQ-Model is proposed in this paper. In TQ-Model, the evaluation process is simplified as shown in the comparative study between TQ-Model and other evaluation models as given in Sect. 4. Evaluation results of TQ-Model are also easy to understand because all the evaluation results are presented in comparison with the traditional textual password scheme. TQ-Model is also helpful for identifying causes of failure in old authentication schemes. New authentication schemes can be pre-examined for identifying their weaknesses before going into public.

The TQ-Model is helpful in analyzing knowledge-based authentication schemes. Future research is required to develop an evaluation model which helps in analyzing token-based or biometric authentication techniques schemes. Although textual password scheme has been extensively used in academia and industry, this research will help both communities to get awareness about the possible weaknesses that exist in the current authentication systems.

References

1. Ji, S.; Yang, S.; Hu, X.; Han, W.; Li, Z.; Beyah, R.: Zero-sum password cracking game: a large-scale empirical study on the crackability, correlation, and security of passwords. IEEE Trans. Dependable Secur. comput. **14**(5), 550–564 (2017)
2. Bošnjak, L; Sreš, J; Brumen, B.: Brute-force and dictionary attack on hashed real-world passwords. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1161–1166. IEEE (2018)
3. Ho, P.F.; Kam, Y.H.; Wee, M.C.; Chong, Y.N.; Yee, L.P.: Preventing shoulder-surfing attack with the concept of concealing the password objects' information. Sci. World J. **2014**, 838623 (2014). https://doi.org/10.1155/2014/838623
4. Gao, X; Yang, Y; Liu, C; Mitropoulos, C; Lindqvist, J; Oulasvirta, A.: Forgetting of passwords: ecological theory and data. In: 27th USENIX Security Symposium (USENIX Security 18), pp. 221–238 (2018)
5. Pearman, S; Thomas, J; Naeini, P.E; Habib, H; Bauer, L; Christin, N; Cranor, L.F; Egelman, S; Forget, A.: Let's go in for a closer look: Observing passwords in their natural habitat. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 295–310. ACM (2017)
6. Nizamani, S.Z; Hassan, S.R; Naz, R.: A theoretical framework for password security against offline guessability attacks. Indian J. Sci. Technol. (2017). https://doi.org/10.17485/ijst/2017/v10i33/115252
7. Komanduri, S; Hutchings, D.R.: Order and entropy in picture passwords. In: Proceedings of graphics interface 2008, pp. 115–122. Canadian Information Processing Society (2008)
8. Aljahdali, H.M; Poet, R.: Educated guessing attacks on culturally familiar graphical passwords using personal information on social networks. In: Proceedings of the 7th International Conference on Security of Information and Networks, p. 272. ACM(2014)
9. Jarecki, S; Krawczyk, H; Shirvanian, M; Saxena, N.: Two-factor authentication with end-to-end password security. In: IACR International Workshop on Public Key Cryptography, pp. 431–461. Springer (2018)
10. Das, S; Dingman, A; Camp, L.J.: Why johnny does not use two factor a two-phase usability study of the fido u2f security key. In: 2018 International Conference on Financial Cryptography and Data Security (FC) (2018)
11. Wiedenbeck, S; Waters, J; Sobrado, L; Birget, J.C.: Design and evaluation of a shoulder-surfing resistant graphical password scheme. In: Proceedings of the Working Conference on Advanced Visual Interfaces, pp. 177–184. ACM (2006)
12. Wiedenbeck, S.; Waters, J.; Birget, J.C.; Brodskiy, A.; Memon, N.: Passpoints: design and longitudinal evaluation of a graphical password system. Int. J. Human Comput. Stud. **63**(1), 102–127 (2005)
13. Mihajlov, M; Jerman-Blazič, B; Josimovski, S.: A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives. In: Network and System Security (NSS), 2011 5th International Conference on, pp. 332–336. IEEE (2011)
14. Jermyn, I; Mayer, A.J; Monrose, F; Reiter, M.K.: The design and analysis of graphical passwords. In: Usenix Security, Rubin, Aviel D (1999)
15. Uellenbeck, S; Dürmuth, M; Wolf, C; Holz, T.: Quantifying the security of graphical passwords: the case of android unlock patterns. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, pp. 161–172. ACM (2013)
16. Dunphy, P; Yan, J.: Do background images improve draw a secret graphical passwords? In: Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 36–47. ACM (2007)
17. Zhao, Z; Ahn, G.J; Seo, J.J; Hu, H.: On the security of picture gesture authentication. In: USENIX Security, pp. 383–398 (2013)
18. Passfaces: two factor authentication for the enterprise. http://www.realuser.com, May. Accessed 19 Nov 2018
19. Chakraborty, N.; Randhawa, G.S.; Das, K.; Mondal, S.: Mobsecure: a shoulder surfing safe login approach implemented on mobile device. Proced. Comput. Sci. **93**, 854–861 (2016)
20. Shankar, V.; Singh, K.; Kumar, A.: Ipct: a scheme for mobile authentication. Perspect. Sci. **8**, 522–524 (2016)
21. Bonneau, J, Herley, C, Oorschot, P.C Van; Stajano, F.: The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In: Security and Privacy (SP), 2012 IEEE Symposium on, pp. 553–567. IEEE (2012)
22. English, R; Poet, R.: Towards a metric for recognition-based graphical password security. In: Network and System Security (NSS), 2011 5th International Conference on, pp. 239–243. IEEE (2011)
23. Khodadadi, T.; Islam, A.K.M.M.; Baharun, S.; Komaki, S.: Evaluation of recognition-based graphical password schemes in terms of usability and security attributes. Int. J. Electr. Comput. Eng. **6**(6), 2939 (2016)
24. Lashkari, A.H; Saleh, D; Farmand, S; Zakaria, D; Bin, O.: A wide range survey on recall based graphical user authentications algorithms based on iso and attack patterns. arXiv preprint arXiv:1001.1962, Jan. (2010)
25. Renaud, K.: Quantifying the quality of web authentication mechanisms: a usability perspective. J. Web Eng. **3**(2), 95–123(2004)
26. Velásquez, I.; Caro, A.; Rodríguez, A.: Kontun: a framework for recommendation of authentication schemes and methods. Inf. Softw. Technol. **96**, 27–37 (2018)
27. Still, J.D.; Cain, A.; Schuster, D.: Human-centered authentication guidelines. Inf. Comput. Secur. **25**(4), 437–453 (2017)
28. Yan, J; Blackwell, A; Anderson, R; Grant, A.: The memorability and security of passwords–some empirical results. Technical report, University of Cambridge, Computer Laboratory (2000)
29. Mourouzis, T; Pavlou, K.E; Kampakis, S.: The evolution of user-selected passwords: A quantitative analysis of publicly available datasets. arXiv preprint arXiv:1804.03946 (2018)
30. Yang, Y; Lindqvist, J; Oulasvirta, A.: Text entry method affects password security. In: The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2014) (2014)
31. Roy, S.; Pattnaik, P.K.; Mall, R.: A quantitative approach to evaluate usability of academic websites based on human perception. Egypt. Inf. J. **15**(3), 159–167 (2014)
32. Nielsen, J.: Ten usability heuristics (2005)
33. Loftus, G.R.; Loftus, E.F.: Human Memory: The Processing of Information. Psychology Press, Hove (2019)
34. Borkin, M.A.; Bylinskii, Z.; Kim, N.W.; Bainbridge, C.M.; Yeh, C.S.; Borkin, D.; Pfister, H.; Oliva, A.: Beyond memorability: visualization recognition and recall. IEEE Trans. Vis. Comput. Gr. **22**(1), 519–528 (2015)
35. Jansen, W.: Authenticating mobile device users through image selection. WIT transactions on information and communication technologies, 30 (2004)
36. Davis, D.; Monrose, F.; Reiter, M.K.: On user choice in graphical password schemes. USENIX Security Symposium **13**, 11–11 (2004)
37. Dhamija, R; Perrig, A.: Deja vu-a user study: Using images for authentication. In: USENIX Security Symposium,**9**, 4–4 (2000)
38. Weinshall, D.: Cognitive authentication schemes safe against spyware. In: Security and Privacy, 2006 IEEE Symposium on, p. 6. IEEE (2006)
39. Chiasson, S; Forget, A; Biddle, R; Oorschot, P.C. van: Influencing users towards better passwords: persuasive cued click-points. In: Proceedings of the 22nd British HCI Group Annual Conference on

People and Computers: Culture, Creativity, Interaction-vol. 1, pp. 121–130. British Computer Society (2008)

40. Salian, N; Godbole, S; Wagh, S.: Advanced authentication using 3d passwords in virtual world. Int. J. Eng. Tech. Res. **3**(2) (2015)

41. Tulving, E.; Watkins, M.J.: Continuity between recall and recognition. Am. J. Psychol. **86**(4), 739–748 (1973)

42. De Angeli, A; Coventry, L; Johnson, G; Renaud, K.: Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. Int. J. Human Comput. Stud. 63(1):128–152 (2005)