

CHAPTER 2

A REVIEW OF GRAPHICAL AUTHENTICATION

2.1 OVERVIEW

This chapter provides explanation on graphical password as a whole. It starts with the definition of graphical authentication, a list of existing graphical authentication schemes with their characteristics, usability and security. This chapter also explains on the types of graphical authentication and discusses graphical authentication from the aspect of usable security. In the usability perspective, this chapter reviews on the aspect of ease of use the authentication process, memorability and time taken for user to use the particular authentication system. While, in the security perspective, the aspects covered are about the password entropy and possible attacks on the current authentication scheme either using simple text, encrypt each characters or graphical images.

2.2 DEFINITION

When authenticating users, graphical authentications are referring to graphical passwords. That is an alternative method of proving that the right users are trying to access the right resources. Previously, text password is so familiar that might think changes are not necessary, but text passwords have been revealed to have weaknesses and vulnerable to many kinds of security problems, and based on much researches, graphical authentication is promising alternative (Schechter et al., 2010; Biddle et al., 2010; Fulkar et al., 2012). There are many variations of how graphical authentication

is defined, but generally, it can be defined as the use of a secret that a human user inputs to a computer with the aid of the computers' graphical input (e.g. mouse, stylus, or touch screen) and output devices (Bandyopadhyay et al., 2009). In simple words, graphical authentication is a system that authenticates users by the use of images.

Previous researchers reported that when using a graphical-based recognition password, users were able to successfully remember the target images through a six-year separation from the last use of the password (Tullis et al., 2011). This indicates that visual recognition authentication could improve the overall recollection performance in users, while maintaining high security protocols. The implementation of graphical recognition could hold the key to creating effective secure authentication systems in the future. Altogether, the idea of graphical authentication is to let users choose their secrets in form of patterns, points or related to images, which can help them in term of memorability, and also advantageous in the aspect of security.

2.3 USER AUTHENTICATION PROCESS

The authentication process can be described in three phases: identification, authentication, and authorization. Users must first make some claim of their identity, provide evidence to substantiate this claim, and if successfully authenticated by the system, access rights are granted to the user. The authentication mechanisms was classified according to the following categories, primarily based on Renaud's model (Renaud, 2005):

1. **Something you know (recall):** A secret is shared between the user and the system. Users must recall and correctly enter their secret to authenticate themselves. Anyone who knows or guesses the secret will also be able to authenticate as the original user. Examples include passwords and PINs (Personal Identification Numbers).
2. **Something you recognize (recognition):** The user and the system share a secret. The system provides cues and the user must correctly recognize the secret. Anyone able to recognize the secret will be able to authenticate as the original user. Graphical passwords where users must recognize pre-selected images from a set of decoys fall into this category. Cued recall systems combine recall and recognition. Users must recognize the cue presented by the system and then use this cue to recall the secret shared with the system.
3. **Something you are (static biometrics):** Biometrics measures some unique physical characteristic of the user. These are more difficult to forge than the first two categories but introduce additional concerns. They may require specialized equipment, are difficult or impossible to change if compromised, and have potential privacy implications (e.g., they may make it difficult to create different identities for various purposes, and they enable organizations to cross-reference information about a user). Static biometrics includes fingerprint, iris, and facial scans, among others.
4. **Something you do (behavioural biometrics):** Some unique behavioural characteristic of the user can also be measured. Users authenticate by repeating

the required action. Examples include handwritten signatures and keystroke dynamics.

5. **Something you have (tokens):** Users must carry a token to be presented for authentication. Anyone who gains access to the token will be able to authenticate as the original user. These are often combined with a PIN or password to offer some protection in case the token is lost or stolen. A smart card, i.e., a card with embedded microprocessor chip, is an example of a token used for authentication.
6. **Where you are (location-based authentication):** Location information can be used to determine if a user is attempting to authenticate from an approved location. This is typically used as a secondary check to identify suspicious login activities. Approved locations may be specific, such as a user's once, or more general, such as identifying the city or country of origin.

2.4 LIMITATIONS OF TEXT-BASED AUTHENTICATION

Text-based passwords are the most common form of authentication used to control access to information and other resources. Text-based passwords are widely used because of their simplicity and convenient mechanisms to use and implement. However, literatures regarding text-based password implementation and usage have long revealed that text-based passwords are actually a weak form of protection, partly because their vulnerabilities towards many kinds of security attack. This authentication also leads to memorability problems, where using long and complex passwords often cause the users to forget their passwords (Schechter et al., 2010).

There are several ways in which an intruder can attack password-protected systems. The most common form of attack is password guessing. People often choose their username, own name, identity card number, phone number, special interest as their passwords (Kessler et al., 2002). This is exposed to guessing attack especially when people like to keep details about themselves documented in a form of books or papers.

Next, possible attack is to steal a system's password file, an amazingly simple thing to do if the file is not assigned the correct access protection. While passwords are almost always stored in some encrypted or hashed form in the file, they are still susceptible to attack via a dictionary attack, where a large number of words are encrypted using the operating systems' encryption scheme in an effort to find a match in the password file (Kessler et al., 2002).

2.5 OVERVIEW OF GRAPHICAL PASSWORDS IMPLEMENTATION

2.5.1 Graphical Authentication

In the graphical passwords system, the user needs to choose memorable image. The process of choosing memorable images depends on the nature of the process of image and the specific sequence of click locations. In order to support memorability, images should have meaningful content because meaning for arbitrary things is poor. In this section, some graphical password systems based on recognition and recall-based are discussed. Graphical-based password methods have been proposed as a solution to the conventional password methods because graphic image are more easily remembered than texts which most of researchers have nominated them as “

picture superiority effect” (Chiasson et al., 2008). A literature on most of articles regarding graphical authentication suggests that they can be categorized into three groups as shown in Figure 2.1 (Ambekar et al., 2015; Biddle et al., 2010; Sobrado et al., 2002).

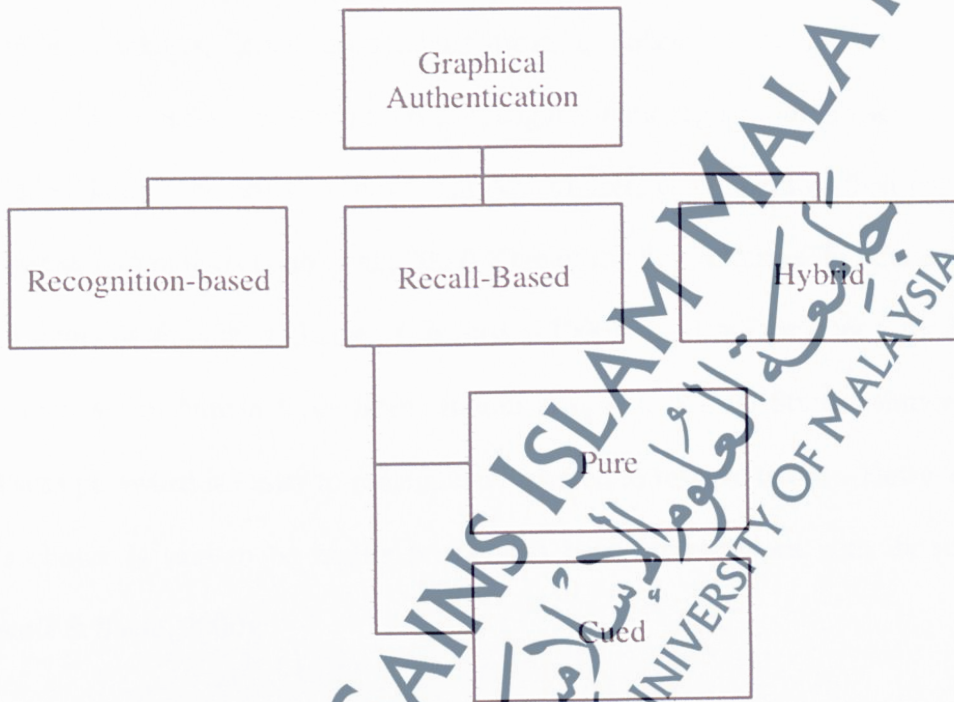


Figure 2.1: Group of Graphical Authentication

Mostly, recognition-based requires users to memorize a set of images during password creation, and then must recognize their images from among distractions to log in. Recall-based requires users to recall and reproduce a secret drawing, pre-selected during registration phase, while cued is different from pure as cued-recall gives hints or cues to help users recall and reproduce their passwords.

The first scheme under the recall-based category is called Draw-A-Secret (DAS) (Jermyn et al., 1999). In this scheme, the user has to draw their password on a grid

using a mouse or a stylus. DAS offers good usability, but lacks in term of security, where recall-based schemes are usually vulnerable to a number of attacks such as shoulder surfing and social engineering.

After that, recognition-based schemes started to be proposed. In this category, users will choose images, icons or symbols from a collection of images. In the authentication process, the users need to recognize their registration choice among a set of candidates. The research shows that 90% of users can remember their password after one or two months (Gao et al., 2009). One of the first schemes introduced under this category is Passfaces (Brostoff & Sasse, 2000). In PassFaces, the user has to select their set of human faces from random images to log in. Studies showed that PassFaces password is easier to remember compared to text passwords. However, the user's choice is said to be highly predictable hence have issues with its security (Brostoff & Sasse, 2000).

These existing graphical schemes have then being extensively reviewed and enhanced by numerous researches throughout the years in order to improve its usability and security. Therefore, in 2007, hybrid schemes started to being introduced. In this category, the authentication will be typically the combination of two or more schemes. These schemes are used to overcome the drawbacks of a single scheme, such as spyware, guessing attack, brute force search and shoulder surfing. Zhao and Li (2007) proposed a scheme called Scalable Shoulder Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS). This scheme integrates both textual and graphical images, and it is resistant to security attacks such as shoulder surfing and spyware. Chiasson et al., (2008) introduced another hybrid scheme combining the

ideas from PassFaces, PassPoints, and Story. In this scheme, the user has to click only one point for each of given images. It is said that this scheme improved the usability where it is easier for the user to remember each click point.

The combination of graphical authentication schemes is claimed to increase the remembrance of the password and also make it more resistant to security attacks. It proved by one of the hybrid schemes that proposed by Elamathi et al., (2013) combining Cued Click Point (CCP) and sound signature. The user has to select one-click point in each image for a series of images in this system. In addition, user is also asked to select a sound signature corresponding to each click point. This sound signature assists the user to recall the click point on an image. The system shows good performance in terms of speed, accuracy, and ease of use (Elamathi et al., 2013).

2.5.2 Existing Graphical Authentication

Before the hybrid schemes emerge, the earlier graphical password methods are classified into two groups: Recognition-based and recall-based. Based on users' action when they authenticate into the system, the later part of this thesis will classify graphical authentication into three main categories; namely choice-based, click-based and draw-based. Basically, choice-based requires users to select their chosen images from a set of distracting images. The image selection can be continued for several rounds depending on the system settings. In addition, the set of images must be easy for human being to remember such as faces of people, places they visit, type of foods and things they have seen for a lengthy duration (Seng et al., 2011). Table 2.1 shows

the selection of images theme that chosen by the previous researcher for the existing graphical authentication scheme.

Table 2.1: Image selection in existing graphical authentication scheme

Graphical authentication scheme	Images theme
Passfaces (Brostoff & Sasse, 2000)	People faces
Deja Vu Graphical Scheme (Djamila & Perrig, 2000)	Abstract images
ToonPassword (Hinds & Ekwueme, 2007)	Cartoon characters
EGAS (Jali, 2011)	Random images theme
Ray’s Scheme (Ray, 2012)	Symbol
Windows Picture Password (Fatehah et al., 2015)	Scenery and environment
Graphical CAPTCHA (Shraddha et al., 2016)	CAPTCHA - varieties

Next, the click-based approach refers to the action of users clicking anywhere they prefer in a given image. These secret click points are the users’ passwords, while the draw-based method requires users to draw their secret on the provided grid/screen. In this case, the drawing is interpreted as the password in order to be authenticated. Graphical authentication has proven to gain much attention when the final Windows 8 build has been released to manufacturing. It offers a twist on security by letting the users to log in with a picture password as an alternative to a text password. As shown in Figure 2.2, which is the new feature in Windows 8 authentication is “Picture Password”, where the end user logs on to Windows by clicking a specific pattern on the lock screen.



Figure 2.2: Graphical password in Windows 8

Android on the other hand has always been popular with its security feature called pattern-draw lock screen as shown in Figure 2.3. In this scheme, users need to enter any pattern on the screen in order, which basically consists of nine dots, and then recreate the pattern when they want to access their devices.

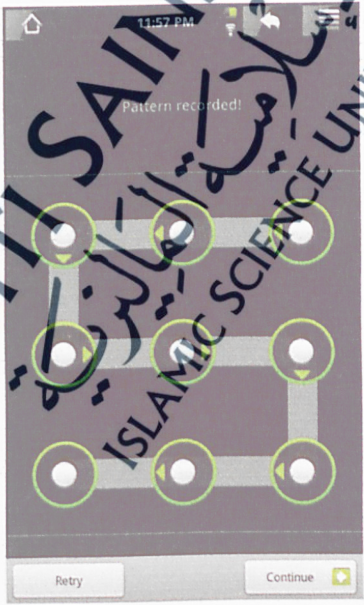


Figure 2.3: Pattern-draw lock screen in Android (Version: 5.0.2 LRX22G)

These examples have shown that there have been growing interests in using graphical authentication as main authentication schemes; however a number of usability and security issues hinder the process of successful establishment of these schemes.

Nowadays, online banking site allows users to manage their financial at the tip of their fingers anytime and everywhere, which makes it so convenient. However, users must realize that it is risky and they must always make sure that the site is secured before they do any transactions. One of the examples of online banking sites is Bank Islam Malaysia Berhad (BIMB) Internet banking online. In order to strengthen the security of its site, BIMB has incorporated graphical authentication into their online banking system. To log in, users have to enter their username, and then “Private image” and “Private word” will be shown as Figure 2.4. If the shown image and word are the correct ones as users have chosen during registration process, then it safe for the user to precede the login process by entering password. This process is to avoid phishing. Otherwise, users are advised not to continue logging into the system because malicious sites are probably controlling it.



Figure 2.4: Confirmation of user authentication in BIMB online banking
(Accessed: 30 October 2016)

2.5.3 Existing Hybrid Schemes Authentication

Throughout years, the numerous researchers introduced the hybrid scheme to make an enhancement of graphical authentication based on usability and security aspects. As mention before, hybrid scheme is the combination of two or more authentication schemes (Jali, 2011). For the group of graphical authentication scheme includes recognition-based and recall-based. Some of the examples of the hybrid schemes are Enhanced Graphical Authentication System (EGAS) (Jali, 2011) and Ray's Scheme (Ray, 2012).

Enhanced Graphical Authentication System (EGAS) is a combination of choice-based (recognition-based) and click-based (recall-based) methods (Jali, 2011). As explained in Section 2.5.2, choice-based refers to the action of users selecting their chosen images from a set of distracting image. Click-based refers to the action of users clicking anywhere they prefer in a given images. This scheme requires users to choose their preferred images from a set of images, and to select click-points in each of the images. The example of EGAS's login interface is showed in Figure 2.5.



Figure 2.5: EGAS login interface (Jali, 2011)

The novelty feature in EGAS is that it allows users to define the number of images and number of click-points they would like to use as password. From the usability aspect, the test's result of this scheme showed that the login time was reasonable, user's clicking accuracy was high, and the passwords were also memorable to the users. However, the main limitations of this scheme are the 'hot-image' and 'hotspot' problems, where users tend to choose predictable images and predictable click-points. This could lead to security issues such as guessing attacks (Fatehah et al., 2015).

Then, Ray (2012) introduced Ray's Scheme (refer Figure 2.6), which is the combination of recognition-based and recall-based systems. The scheme is proposed for smart hand held devices. Since users have to input both their textual password and corresponding digits of the objects into this scheme, it resulted in a large password space. This makes Ray's scheme to be less vulnerable to brute force attack. Other than that, this scheme is also claimed to be resistant to dictionary attacks and social engineering attacks. From the usability aspect, this scheme eliminated the problems

with grid-based techniques where the users have to remember the exact coordinates of their password which is not easy.

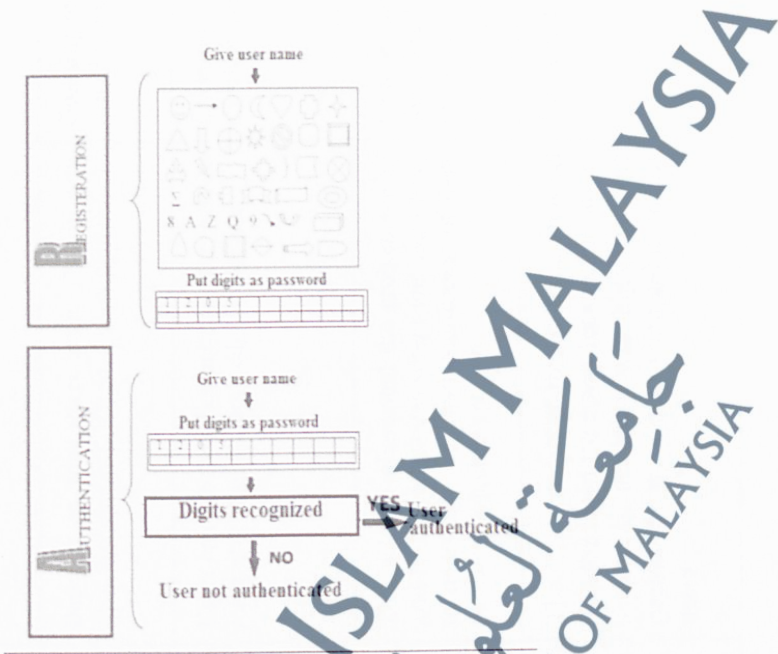


Figure 2.6: Ray’s scheme screenshot (Ray, 2012)

From previous studies in hybrid schemes, they only mentioned the combination of two graphical authentication, so the new development of hybrid scheme that combine more than two graphical authentication can improve the security drawbacks while maintaining usability in graphical password authentication. A comparison of other existing graphical authentications used previously is presented in Table 2.2.

Table 2.2: The comparison of usability and security in existing graphical authentication scheme

Scheme	Usability		Security
	<i>Authentication process</i>	<i>Memorability</i>	
Draw-based: Pattern Lock (Emanuel V. Z. et al., 2015)	Draw on grid with a stylus onto a touch sensitive screen to unlock applications.	Depends on what users draw. That is very easy to remember, but hard to recognize.	Guessing technique and shoulder surfing.
Click-based: IPAS (Almuairfi et al, 2013)	The system presents to the use one or more pieces of information in an implicit image form. The user is expected to "click" on the correct area the represents the "expected information" in an implicit form to complete the authentication	Users can use their favourite images; easy to remember than system assigned pictures.	Guessing technique and shoulder surfing.
Hybrid Scheme: Ray's Scheme (Ray, 2012)	Users have to input both their textual password and corresponding digits of the objects into this scheme	This scheme eliminated the problems with grid-based techniques where the users have to remember the exact coordinates of their password which is not easy.	Less vulnerable to brute-force attack and resistant to dictionary attacks and social engineering attacks.
Hybrid Scheme: EGAS (Jali, 2011)	Requires users to choose their preferred images from a set of images, and select click-points in each of the images.	The test's result of this scheme showed that the login time was reasonable, user's clicking accuracy was high, and the passwords were also memorable to the users.	Guessing technique.

Choice-based (Hong et al., 2004)	Type in the code of pre-registered picture objects; can be very fast	Users have to memorize both picture objects and their codes. More difficult than text-based password	Brute force search and spyware
Choice-based (Jansen, 2004)	User register a sequence of images; slower than text-based password	Pictures are organized according to different themes to help users remember	Brute force search, guessing technique and shoulder surfing
Choice-based (Takada et al., 2003)	Recognize and click on the pre-registered images; slower than text-based password. Slower than text-based password	Users can use their favourite images; easy to remember than system assigned pictures	Brute force search, guessing technique and shoulder surfing

2.6 USABILITY IN USER AUTHENTICATION

In 2005, Cranor and Garfinkel edited the first book on "Security and Usability" (Sasse & Flechais, 2005), bringing together work from various researchers and highlighting different areas within the field. The main publication venue specifically for usable security research is in the website based on the usability and security keywords. Usable security remains an active and growing research area. Designing user interaction for security applications, and user authentication systems specifically raises some interesting challenges. The area of usable security can draw from existing Human-Computer Interaction (HCI) knowledge, but some fundamental differences must be taken into account.

In addition to legitimate users of a security system, there is a second group of users who are actively trying to attack the system. Such attackers will exploit any information leaked by, or that can be extracted through, the interface. They will also leverage any way that the system can be misused or any means to trick legitimate users into revealing confidential information. This makes it difficult to provide some forms of helpful feedback in the user interface, for example to help guide users towards correct passwords, as it may also help attackers. Security is typically a secondary task, if security obstructs users' primary goals, users will often try to circumvent the security measures (Sasse & Flechais, 2005). Users have poor mental models of security (Chiasson et al., 2006) and they may not even realize that their actions are insecure in the first place. Furthermore, they often misunderstand or underestimate the consequences of insecure actions.

Computer security suffers from the “barn door” property: if information or a system is exposed even for a brief time, there is no guarantee that it has not been compromised in an irrecoverable way (Whitten et al., 1999). The information may have been externally leaked to attackers, or available to malware resident on the system. While these represent security concerns, they are all directly related to users of the system and as such, solutions must focus as much on the HCI aspects of the system as on the technical security components. Usability problems may significantly impact the real-world security of the system. User interface design decisions may unintentionally sway user behaviour and often towards less secure behaviour. This may be a direct result of the particular interface, or may be compounded by external influences such as when users reveal their passwords to others due to social expectations. Furthermore, the easiest way of using a system is often also the least secure way. For example, users may choose very short, simple text passwords because these are easier to remember and enter than longer, more complex sequences of characters.

2.7 GRAPHICAL AUTHENTICATION SECURITY

Graphical authentication may offer better security than text-based passwords because many people like to use plain words rather than a combination of character, in an attempt to memorize text-based password. A dictionary search can often hit on a password and allow a hacker to gain entry into a system in seconds. But if a series of selectable images is used on successive screen pages, and if there are many images on each page, a hacker must try every possible combination at random. If there are 100 images on each of the 8 pages in an 8-image password, there are 100^8 possible combinations that could form the graphical password. If the system has a built-in delay of only 0.1 second following the selection of each image until the presentation

of the next page, it would take (on average) millions of years to break into the system by hitting it with random image sequences (Reddy et al., 2013)

Using long and complex combinations of passwords can cause problems with ease of use and memorability, and using simple passwords can result in a range of security problems such as risk to be exposed to password guessing, shoulder-surfing and social engineering techniques (Schechter et al., 2010). Despite the massive range of passwords that could be chosen, users consciously and subconsciously restrict the range of possible passwords (Biddle et al., 2010; Georgakakis et al., 2012). Motivated by these limitations of text-based passwords, graphical authentication comes in line to overcome these limitations and to be a better way of authenticating users.

2.7.1 Password Entropy

The reason why it is important to count the number of password patterns is because of its connection to the security of the scheme. To prevent brute force attacks it is necessary to have the possible password space big and since the password space consists of all possible patterns in a specific grid this question becomes essential (Rass et al., 2010).

When talking about the security of passwords a key concept is called entropy of the password space (Saevarsson, 2012). In an outcome space $X = \{x_1, x_2, \dots, x_n\}$ with the probability $p(x_i)$ of outcome x_i , the entropy of X is using the logarithm to base 2.

$$-\sum_{i=1}^n p(x_i) \log p(x_i)$$

Note that the entropy is always positive since $\log p(x_i)$ is negative. Using entropy is a standard way to evaluate a password space, the higher the entropy the better the password space. Table 2.3 shows the entropy for a few common types of passwords. The calculation is based on all standard keyboard characters ($n=94$), so entropy per character is $(\log_2 94) = 6.55$. As stated, the number of entropy for 8, 10, and 12 letters are higher, but how can users remember that kind of password? For example, can anyone remember 8 characters of this “Mc*Fz8^q” password?

Table 2.3: Password entropy for standard authentication scheme (Saevarsson, 2012)

Password Space	Entropy (bits)
8 letter password containing all letters and numerals	47.6
8 letter password containing all ASCII printable characters.	52.6
6 letter password with only lower case letters (a-z)	28.2
PIN number, 4 numeric characters (0-9)	13.3

Table 2.4 stated that most of the choice-based graphical schemes were just weak as their entropy predictions were small as compared to the traditional passwords of length eight in Table 2.3. Possible ways to address this are increasing the number of decoy images and the number of authentication rounds. However, it would take long time to login then this could reduce the ease of use of the method. The passpoint scheme that based on click-based graphical scheme was comparable with the traditional passwords of length six; with the scheme of hybrid (Zhao & Li, 2007) could be said as providing effective security as their scheme was comparable with the passwords of length seven or eight (Jali, 2011). From the previous studies, it suggested that the combination of authentication scheme had provided better usability

while maintaining the security. The combination of graphical authentication scheme (hybrid scheme) was discussed in this thesis.

Table 2.4: Password entropy for graphical authentication scheme (Jali, 2011)

Scheme	Authentication Information	Entropy (bits)
Passfaces: Users had to recognize and pick the pre-registered images. (Brostoff & Sasse, 2000)	Authentication round = 4 (9 images per round) Target = 1 image per round Decoy = 8 images per round	$4 * (\log_2 9) = 12.68$
Passimages: Users had to correctly choose six images from amongst a set of decoy images. (Charruau et al., 2005)	Authentication round = 4 (25 images per round) Target = 6 images Decoy = 94 images	$4 * (\log_2 25) = 18.58$
Passpoint: Users can choose any image they prefer and the system does not need any predefined click-region or well-marked boundaries. (Wiedenbeck et al., 2005)	Authentication round = 1 Target = 5 clicks Image size, I = 450x330 Tolerance, T = 20x20 Password space = (I/T) ~ 371 (points to click)	$5 * (\log_2 371) = 42.67$
Hybrid Scheme: Integrates both textual and graphical images. (Zhao & Li, 2007)	Target = 4 clicks, 4 colours & 4 objects Assuming password space = 300 (points to click)	$4 * (\log_2 300 * 4 * 4) = 48.92$

2.7.2 Security Attacks in Existing Graphical Password (Saranya & Bindu, 2014)

This section discusses attack types based on password capture. The most common threats to password-based authentication system are shoulder-surfing, phishing, social engineering, brute-force, dictionary, and spyware attack. The definitions of each type of threat are as below:

1. **Shoulder Surfing Attack:** Shoulder surfing attack refers to attack the user passwords by using direct observation techniques. Main direct observation technique is looking over someone's shoulder, to get the password. Shoulder surfing attack mostly occurs in public places because it is really easy in a crowd to stand near someone and look at them entering a password or any secret key.
2. **Phishing:** This attack is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email or other communication channels.
3. **Social Engineering Attack:** Social engineering is the attack, in which human gains the sensitive information from the human interaction. In this type of attack, attacker tries to obtain the information about an organization or computer systems from the user itself to act like an employee. The attacker doesn't use any electronic technique of hacking in this kind of attack as he or she uses only human intelligence and tricky conversation to get the information he wants. When attacker gets some of information from one source, then he or she may gather information from other sources within the same organization to get the complete information and add to his or her credibility.
4. **Brute-Force Attack:** This attack is a trial and illegal method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys.
5. **Dictionary Attack:** This is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key

necessary to decrypt an encrypted message or document.

6. **Spyware Attack:** Spyware is a type of malicious software, which installed on computers with the aim of stealing secret information of users. Spyware attack is normally done by using a key logger or key listener. This malwares gathers information without user’s knowledge about gathering and leak this information to an outside source of attacker. A scheme could be resistant to this attack by using CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart), which is a program that generates and grades tests that are human solvable, but are beyond the capabilities of computer programs (Shraddha et al., 2016). CAPCTHA is a promising way to resist this attack in graphical authentication schemes. In Table 2.5, a graphical authentication scheme is considered to be resistant to spyware attacks if it uses CAPTCHA in its scheme. In this section, that is the comparison table as shown in Table 2.5 for aforementioned attacks based on the previous studies by Saranya and Bindhu (2014).

Table 2.5: The Attack Comparison Based on Three Graphical Password Methods

Methods		Schemes	Type of Attacks		
Recall-Based	Pure		Shoulder Surfing	Social Engineering	Spyware
		DAS	<i>N</i>	<i>M</i>	<i>Y</i>
		PassDoodle	<i>N</i>	<i>E</i>	<i>Y</i>
		PassShapes	<i>N</i>	<i>M</i>	<i>Y</i>
		Syukri	<i>N</i>	<i>M</i>	<i>Y</i>
	Cued	Blonder	<i>N</i>	<i>M</i>	<i>N</i>
		PassPoints	<i>N</i>	<i>D</i>	<i>N</i>
		CCP	<i>N</i>	<i>D</i>	<i>N</i>
		PCCP	<i>N</i>	<i>D</i>	<i>Y</i>
Recognition-Based		Deja Vu	<i>Y</i>	<i>D</i>	<i>N</i>
		PassFaces	<i>Y</i>	<i>D</i>	<i>N</i>
		Story	<i>Y</i>	<i>M</i>	<i>N</i>
		Cognitive	<i>Y</i>	<i>D</i>	<i>Y</i>
		GPI	<i>N</i>	<i>D</i>	<i>Y</i>

Hybrid Schemes	Jiminy	<i>N</i>	<i>D</i>	<i>Y</i>
	S3PAS	<i>Y</i>	<i>M</i>	<i>Y</i>
	CAS	<i>N</i>	<i>D</i>	<i>Y</i>
	PassHands	<i>Y</i>	<i>D</i>	<i>Y</i>
	CBFG	<i>Y</i>	<i>D</i>	<i>Y</i>

Table 2.5 summarizes the security of the different graphical password schemes they analyzed. ‘Y’ means Yes, that it is resistant to that form of attack. ‘N’ means No that the scheme is open to attack. In Social engineering attack, ‘E’ indicates Easy, as the attack is highly effective. ‘M’ denotes Middle that difficulty has increased. ‘D’ denotes the attack is difficult.

2.8 SUMMARY

This chapter presents a general overview of graphical authentication based on the previous studies that claim images are easier to remember than text-based and help in the usability aspect. This chapter also covered the types of graphical authentication and discussed graphical authentication from aspect of usable security. Some of the existing schemes are then explained to look at its security and usability aspect, and they are being summarized at the end. Based on the benefits of graphical authentication, it is highly anticipated that graphical authentication will dominate in the near future as the best authentication scheme. This chapter also suggested the new development of hybrid scheme that combine all of the categories of graphical authentication; choice-based, click-based, and draw-based. Generally, the topics and prospects of hybrid scheme authentication are also explained. Then, next chapter further discussed on the methodology used for the new development of an alternative hybrid scheme prototype, named as Choice-Click-Draw (ChoCD).