CHARPATTERN: RETHINKING ANDROID LOCK PATTERN TO ADAPT TO REMOTE AUTHENTICATION

TASHTANBEK SATIEV

MASTER THESIS

THE DEPARTMENT OF COMPUTER ENGINEERING

TOBB UNIVERSITY OF ECONOMICS AND TECHNOLOGY

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

APRIL 2015

ANKARA

Approval of the Graduate School of Natural and Applied Sciences.

Prof. Dr. Osman EROĞUL
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Assoc. Dr. Erdoğan DOĞDU
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Prof. Dr. Kemal BIÇAKCI
Supervisor

Examining Committee Members

Chair : Prof. Dr. Ali Aydın SELÇUK

Member : Prof. Dr. Kemal BIÇAKCI

Member : Asst. Dr. Enver ÇAVUŞ

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

I hereby declare that all the information provided in this thesis was obtained with rules of ethical and academic conduct. I also declare that I have sited all sources used in this document, which is written according to the thesis format of the Institute.

Tashtanbek SATIEV

University	**:**	**TOBB University of Economics and Technology**
Institute	**:**	**Institute of Natural and Applied Sciences**
Science Programme	**:**	**Computer Engineering**
Supervisor	**:**	**Prof. Dr. Kemal BIÇAKCI**
Degree Awarded and Date	**:**	**M.Sc. – April 2015**

Tashtanbek SATIEV

CHARPATTERN: RETHINKING ANDROID LOCK PATTERN TO ADAPT TO REMOTE AUTHENTICATION

ABSTRACT

Android Lock Pattern is popular as a screen lock method on mobile devices but it cannot be used directly over the Internet for user authentication. In this thesis, we carefully adapt Android Lock Pattern to satisfy the requirements of remote authentication and introduce a new pattern based method called *charPattern*. Our new method allows dual mode of input (typing a password and drawing a pattern) hence accommodate users who login alternately with a physical keyboard and a touchscreen device. It uses persuasive technology to create strong passwords which withstand attacks involving up to 10^6 guesses; an amount many experts believe sufficient against online attacks. We conduct a hybrid lab and web study to evaluate the usability of the new method and observe that logins with *charPattern* are significantly faster than the ones with text passwords on mobile devices.

Keywords: Authentication, Graphical Password, Pattern-based Authentication, Android Lock Pattern, Usable Security, Usability Study.

Üniversitesi	**:**	**TOBB Ekonomi ve Teknoloji Üniversitesi**
Enstitüsü	**:**	**Fen Bilimleri**
Anabilim Dalı	**:**	**Bilgisayar Mühendisliği**
Tez Danışmanı	**:**	**Prof. Dr. Kemal BIÇAKCI**
Tez Türü ve Tarihi	**:**	**Yüksek Lisans – April 2015**

Tashtanbek SATIEV

CHARPATTERN: ANDROİD ŞEKİLLİ EKRAN KİLİDİNİ UZAKTAN KİMLİK DOĞRULAMA OLARAK YENİDEN DÜŞÜNME

ÖZET

Android Şekilli Ekran Kilidi, mobil cihazlarının ekranları kilitlemede yaygın olarak kullanılmasına rağmen doğrudan Internet kimlik doğrulamasında kullanılamamaktadır. Bu tezde, Android Şekilli Ekran Kilidini özenli bir şekilde güncelleyerek uzaktan kimlik doğrulama için uygun bir hale getirdik ve yeni bir şekil tabanlı kimlik doğrulama olarak charPattern ismini verdiğimiz sistemi önerdik. Geliştirilen yeni metot, çift giriş (parola yazma ve şekil çizme) imkanı vererek kullanıcılara aynı zamanda hem fiziksel klavye ile hem de dokunmatik ekranda oturum açmaya olanak sağlamaktadır. Bu metot, 10^6 seviyesine kadar saldırılara karşı güçlü şifreler oluşturmak için ikna etme teknolojisini (persuasive technology) kullanır (çoğu uzman bunun çevrimiçi saldırılara karşı yeterli olduğunu düşünmektedirler). Yeni yöntemin kullanılabilirliğini değerlendirmek amacıyla bir hibrit laboratuvar ve web çalışması yapılarak, mobil cihazlarda charPattern ile oturum açmanın metin şifreleri ile olanlardan çok daha hızlı olduğu gözlemlenmiştir.

Anahtar Kelimeler: Kimlik Doğrulama, Grafik Parola, Şekil Tabanlı Kimlik Doğrulama, Android Şekilli Kilidi, Kullanılabilir Güvenlik, Kullanılabilirlik Testi.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Prof. Dr. Kemal Bicakci, who gave me enormous, comprehensive support and high motivation to complete this thesis, conduct the complex research consisting of the implementation part, test, user study, survey and statistical analysis necessary for the thesis and a number of other researches through my master degree period.

I thank Prof. Dr. Ali Aydin Selcuk for being a chairman during my thesis defense.

My appreciation also goes to Assoc. Dr. Suleyman Uludag, under whose teaching I could deal with a number of problems during the implementation of the Android application.

I also thank Phd Candidate Ugur Cil, who helped me in designing DBMS, developing Android and Web applications.

My gratitude to TOBB University of Economics and Technology for providing me a scholarship throughout my study and to all staff members and assistants of the Computer Engineering Department of TOBB University of Economics and Technology for their deep teaching, advice, suggestions, which I appreciate the most.

The thesis is dedicated to my son, Altay.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

With the advent of new touch-pad technologies, authentication methods are becoming more critical attracting a number of researches in the realm of IT security. Among other hot challenges of Internet authentication methods on mobile devices, usability and security issues also arise. As a result of expanding use of mobile devices in the Internet surfing, being one the of main traditional authentication techniques for decades, the text-based authentication method which uses alphanumeric characters as a password is likely to lose its power due to usability and security issues.

While the text-based authentication is simple, cross-platform, habitual for most users, it has also well-known drawbacks. Using the text-based authentication, most users are subject to dictionary attacks due to its poor memorability [2]. In fact, each user is expected to utilize in average of five different active text passwords simultaneously [3] (regarding her cognitive ability) [4] which can critically reduce password entropy especially when the number of users' web or/and device accounts increases. In this case, users tend to reuse existing passwords for multiple accounts, and/or write passwords in open case (as a note) making exposed to offline dictionary or social-engineering attacks [5].

In addition to mentioned above drawbacks, the text-based authentication on mobile devices is not as user-friendly as on desktop computers. When users typing strong passwords on mobile devices they are compelled to bear the burden due to a soft keyboard with restricted set of alphanumeric characters and its small monitor size [6] which causes an increased number of login errors. One of the approaches to mitigate weaknesses in terms of usability and security of text passwords are password managers which also have its own security and usability drawbacks [7], [8]. As an alternative methods to the text-based authentication; lockPattern [9], biometric authentication [10] and other special techniques which work more user-friendly are proposed and currently work partially (not on all devices). Unfortunately, these techniques cannot completely supplant the text-based authentication owing to the lack of technical properties to run them on desktop computers. It is observed clearly when users try to perform entry to their Internet accounts from both of touchscreen devices and desktop computers frequently.

Taking into consideration of aforementioned usability and security issues of the traditional text passwords, it is necessary to bring into existence the ideal authentication system to the text-based authentication supporting dual mode configuration through which users can access to Internet accounts either from desktop computers or from mobile devices optionally in user-friendly and secure way, respectively.

As being a viable alternative to traditional text-based passwords, graphical passwords have gained significant attention in academic research in the last 15 years [11]. From practical point of view, maybe the most successful graphical password example is Android Lock Pattern (ALP) which comes pre-installed in most of Android smartphones and is presumably the most widely deployed one. As its name implies, Android Lock Pattern (ALP) is mainly used to lock (unlock) smart-phones. Security and usability requirements for remote access (over the Internet) are very different than the ones present in local operation while locking/unlocking a phone. We identify two main differences as follows:

1. ALP provides a theoretical password space of 18 or 19 bits [11], [12]. Recent research estimates a partial guessing entropy of only 9.10 bits. This may provide adequate level of security for its intended purposes especially with a policy enforcing maximum number of false trials. On the other hand, although there is not a consensus among security researchers for the minimum security requirements for web authentication, there is no doubt that ALP in its present form offers much less than required.

2. Even though touchscreen devices are becoming widely deployed by most

of Internet users, use of a desktop or a laptop computer with an old-fashioned monitor is still common. Previous research suggested that an authentication scheme designed for touch screen devices such as ALP is likely not accommodate users alternating between desktops and touch screen devices, well [13].

In this thesis, we propose a new knowledge-based authentication method called charPattern targeting web applications by a careful adaptation of ALP addressing the aforementioned differences and thus challenges. We also conduct a hybrid lab and web study to compare the usability of charPattern with text passwords and gridWordX [6]; a recent multiword password proposal answering the research challenge arising from the evolution of Internet access devices [13].

The rest of the thesis is organized as follows: Section 2 overviews the related work. In section 3, the proposed system, charPattern, is presented. The user study and its results are introduced in section 4. Section5 presents the discussion related to the collected data and also includes limitations and the security analysis.In section 6, the conclusion is presented. Final sections of the thesis cover references, the collected raw data and overview statistical tests used during the analysis.

2. RELATED WORK

The important key concept in authentication is secure sharing of as called the “Secret” between a user and a server (device) during initialization of a communication session. The “Secret” can be one of these three following kinds [14]: “something you know” such as passwords, “something you have” such as “cards” and “something you are” such as biometrics. Generally, every authentication scheme is designed according to these three kinds of principles. When the scheme holds two security factors it is called two-factor authentication and on the other hand, it is called multi-factor authentication while it includes more than three kinds of the “Secret”. In the following subsections, similar to charPattern authentication techniques are presented in brief.

2.1 Graphical Authentication

Having improved since 1996 when it was first proposed by Greg Blonder [1], where he introduced the graphical password using a single image letting users click (choosing by a mouse) on some regions of it (see Figure 2.1) as a graphical password , the graphical authentication is becoming widely used in accessing to Internet accounts helping users to easily memorize and utilize their Internet passwords. Despite good usability characteristics of graphical authentications, they have not replaced the traditional text authentication at all just becoming a part of two-factor authentication together with the text-based one or chosen as yet another authentication scheme (YAAS) [15].

Graphical passwords are based on using of images as a graphical password to improve memorability for users [16], [11]. When users first authenticate, they need to choose a region (or multiple regions) on a particular image (by Blonder [1]) or choose one image among a definite set of images which is used as a graphical password for accessing to Internet accounts. The level of memorability of the

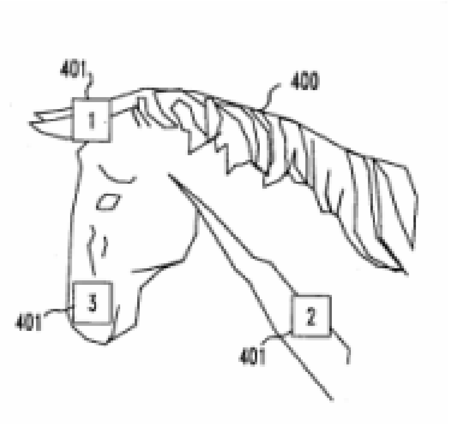


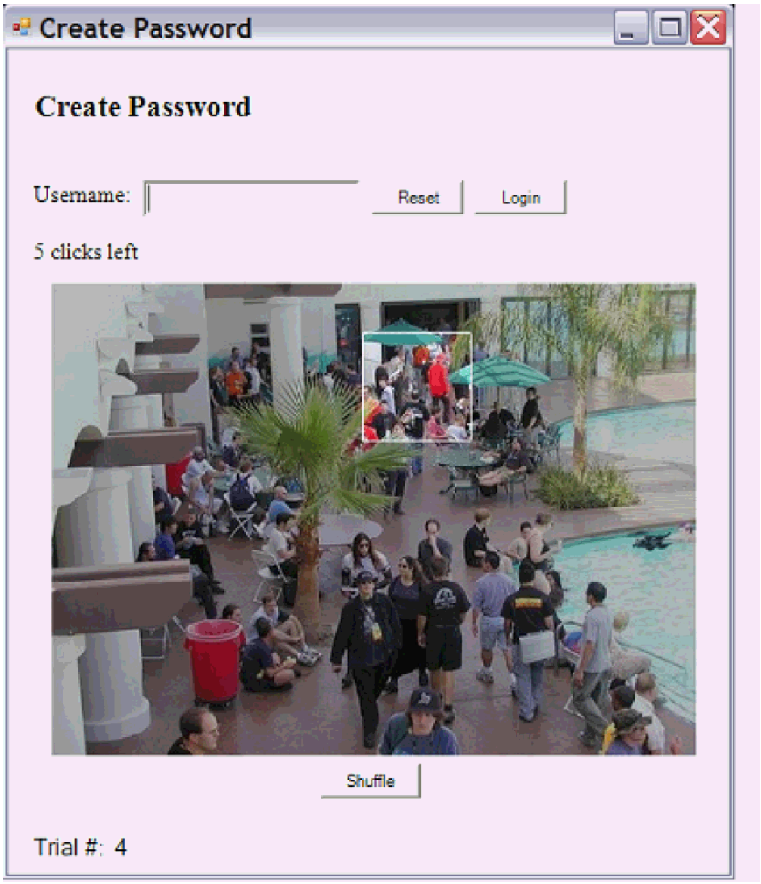
Figure 2.1: The Graphical password firstly proposed by Blonder [1].

chosen region on the image or a chosen image depends on a semantic meaning of that region or the chosen image thus in abstract regions/images there tend to be low memorability. In this research, dividing the image into multiple regions (cells, grids) is also suggested. Dividing into cells has some useful points: users can easily utilize (memorize, enter) making use of recognition memory, the system avoids selecting of hotspots by users, it gives flexibility of implementation just identifying each cell with a unique rather than processing with a whole image(sending, image recognition, hashing of images).

During choosing a password region, users are likely to click particular regions called hotspots that are easily defined by cued recall. While this feature provides good memorability, on the other hand, such a guessability property is exposed to guessing attacks .

Persuasive Cued Click Points (PCCP) schema is the one of solutions to guessing attacks on the graphical authentication [11]. As observed in Figure 2.2, a main idea of PCCP is to divide the image into small multiple cells suggesting random cells as chosen regions automatically and perform shuffle until users do not accept randomly chosen cells as graphical passwords.

Graphical Passwords on Mobile Devices based on the recognition of



Create Password

Create Password

Username:

5 clicks left

Trial #: 4

Figure 2.2: The Login Screen of Persuasive Cued Click Points (PCCP).

photographs in the context of mobile devices were investigated by Dunphy et al. [17]. Schaub et al. explore the design space of graphical passwords on smart phones by implementing five different graphical password schemes on one smartphone platform [18]. They perform usability experiments and analyze shoulder surfing success rates. They consider two levels of theoretical password strength (14-bits and 42-bits) but does not analyze practical password space.

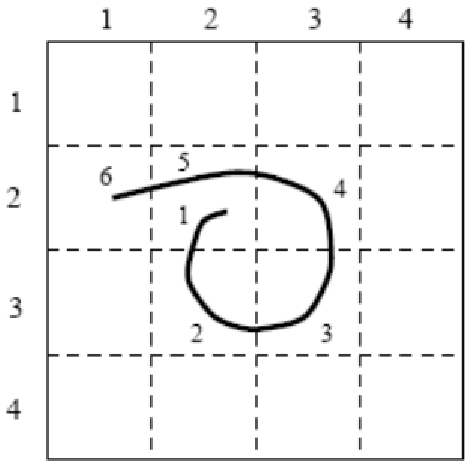


Figure 2.3: Draw-A-Secret (DAS).

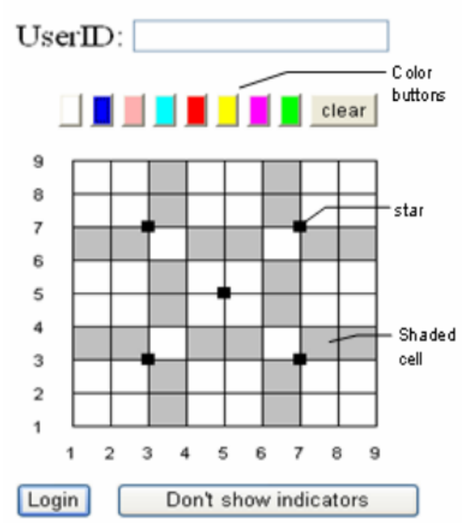
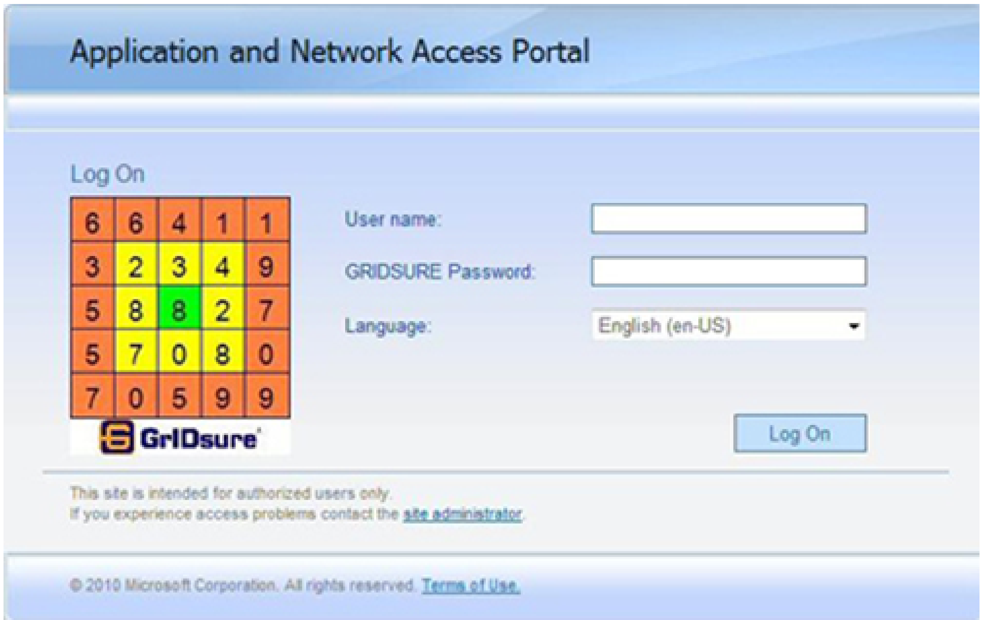


Figure 2.4: Pass-Go Main Login Interface.

2.2 Pattern-based Authentication

Actually, pattern-based authentication can be accepted as a kind of the graphical authentication. The key point of classification is a way of memorizing graphical passwords. Graphical passwords could be grouped based on how they are memorized: recall-based, cued-recall and recognition-based schemes. As a matter of fact, pattern-based authentication is included to recal-based graphical authentication [19]. The one of pioneers suggesting recall-based graphical authentication is Draw-A-Secret (DAS) schema (see Figure 2.3) by Jermyn et al. [20].

Pass-Go [21] (see Figure 2.4), inspired by an old Chinese game, is a recall-based scheme where passwords are drawn by using 9 x 9 grid's intersection points rather than cells in order to draw diagonals and increase a password entropy with the same grid space. Here, to choose desired intersection correctly without any burden, error tolerance mechanism is used that balances easy selection and not tapping on other intersection points. Unlike other graphical passwords, Pass-Go lets users to draw discrete patterns on the same grid space and use 9 different



Application and Network Access Portal

Log On

6	6	4	1	1
3	2	3	4	9
5	8	8	2	7
5	7	0	8	0
7	0	5	9	9

User name:

GRIDSURE Password:

Language: English (en-US)

This site is intended for authorized users only.
If you experience access problems contact the site administrator.

© 2010 Microsoft Corporation. All rights reserved. Terms of Use.

Figure 2.5: Main Interface of OTP GridSure.

colors to increase password entropy which reaches extremely large space of 374 bits.

Gridsure [22] is also a grid-based authentication system which specifically uses a 5 x 5, 6 x 6 and 7 x 7 grids as an alternative to one-time PIN system (see Figure 2.5). The grid is populated with different random digits, thus a user who memorizes her pattern could enter a different PIN occupied by the pattern in each login. A similar one-time password scheme is PassPattern system [23].

PassPattern System (PPS) is another way of the Internet authentication based on a challenge-response system. Using N x N matrix of characters, PPS is designed with the idea of gaining higher memorability of patterns created by secret characters over memorizing memorizing texts, images or image regions. In PPS, recognition-based scheme is played a greater role than recall-based one just requiring to memorize initial pattern organized by secret characters. As presented in Figure 2.6, the user has to memorize the pattern and when the is getting authenticated she has to type characters (characters are arranged in random order in each login)corresponding to the secret pattern. PPS provides

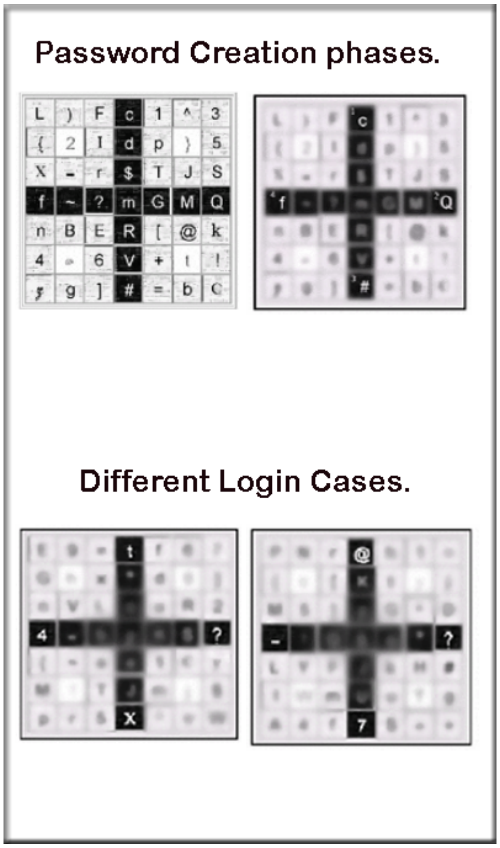


Figure 2.6: PassPattern(PPS) Interfaces.

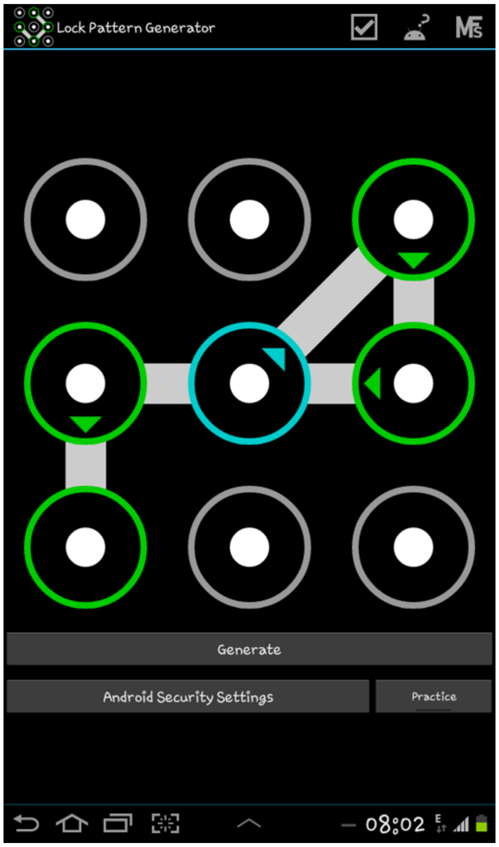


Figure 2.7: Android Lock Pattern Interface.

good resistance to shoulder-surfing attack without high workload on user-side.

Android Lock Pattern(ALP) could be considered as a variation of the Pass-Go scheme by using nine points arranged in a 3x3 grid [11], [12] as presented in Figure 2.7. By setting the minimum number of points that should be chosen as four, the number of possible patterns is 389.112 giving an approximate security of 19 bits. However, this is just a theoretical maximum value. Uelenbeck et al. shows that in practice only a partial guessing entropy of 9.1 bits is achieved which is around the same security level of 3-digits random PINs [12]. Given the popularity of ALP, it is of no surprise to see that the idea is ported to other platforms as well. For instance Eusing Maze Lock 3.1 is such a free product for Windows platforms [24].

2.3 Multiword Passwords

Multiword method was arisen as a hybrid authentication combining main features of traditional text passwords and graphical passwords [25]. The main goal of this method is to improve memorability and usability of strong text passwords both on desktop computers and on input-limited devices. In other words, graphical features are used to increase typing speed and recall rates. Besides using graphical features, the voice-entry of passwords is proposed in Fastword [25].

gridWordX, improved version of gridWord [13], is hybrid knowledge-based authentication schema, which supports elements of text and graphical passwords improving memorability of passwords and faster managing (entering, editing, resetting) them [6]. In gridWordX, in order to conduct usability study, traditional text-based authentication (see Figure 3.1(a)) was also implemented with the minimum of eight-character requirement which corresponds to 18 bits. GridWordX (see Figure 3.1(b)) uses as password objects 104 concrete words which are then utilized as a part of a password consisting of three words. The words are arranged in 8 x 13 (8 rows, 13 columns) 2D grid with one to one mapping. Besides of 2D grid of words, the interface also includes three combo boxes with autocomplete property for each words of the password in order to dual mode authentication (either by typing or touching over the words). Here, three-word-length password is selected yielding about 20 bits of password entropy. GridWordX is designed trying to eliminate weak points of text passwords regarding to usability in managing Internet passwords both from desktop computers and mobile devices [6].

3. PROPOSED SYSTEM

The proposed system in this research, charPattern (see Figure 3.1(c)), is expected to become an alternative way to earlier designed and evaluated hybrid authentication systems, such as gridWord [13] and gridWordX [6]. The proposed schema, charPattern, gives privilege to drawing a pattern over so called dot-characters (dot-character is a dot which contains one unique character) intending to obtain better usability evaluation than of traditional text password. Thus, supporting both of typing and drawing a pattern modes simultaneously, charPattern is expected to leverage password memorability, easily managing passwords from both of desktop computers and mobile devices.

3.1 Design Features

The approach of mixing alphanumeric passwords with drawing a pattern in authentication is arisen from the growing tendency of users who use ALP in locking their Android devices. We present each of main differences of charPattern and ALP presented in the following way (see Table 3.1):

1. Designing 35 dots in charPattern is due to obtaining 20 bits of password entropy. The system can withstand against online attacks according to the NIST standard [26] and in order to equalize to the password entropy of gridWordX and traditional text password authentication used in gridWordX [6]. On the other hand, less number of dots gives ALP advantage in terms of simplicity and memorability of the pattern.

2. We design charPattern as 5 x 7 dot-matrix so as to arrange 35 dots in a rectangular form. We need to notice that having N x N size as in ALP, such a dot-matrix is likely to increase memorability of passwords than having different row and column sizes as in charPattern.

3. In charPattern, each of the dot is mapped to a unique alphanumeric character. We choose 10 numeric digits and 25 lowercase letters (all letters in English alphabet except the letter “z”) to have 35 characters in total. This gives the opportunity to map each pattern to a text password composed of four characters. Users are free to enter their passwords either by drawing the pattern or by typing the password. For instance, the pattern seen in Figure 3.2 could also be entered by typing the password “ha5v”.

4. charPattern password consists of four dots giving a password space over one million (35 x 34 x 33 x 32 = 1256640 $\cong 2^{20}$) which could withstand against online attacks if passwords are chosen uniformly and lockout rules are in use [27], [28]. In addition, we assume that four is the minimum number of dots to create meaningful patterns (like rectangles, diamonds etc.).

5. To be able to draw a pattern with any of 4 dots (not only consecutive dots) within 35 dots, we use pausing for 150 ms to select a dot which neither affect login time nor it expand error rates. In other words, it is possible to skip those dots not to be selected by drawing a pattern without pausing over them. Although pausing on dots is only 150 ms, it may increase error rates when the user does not get accustomed to dealing with charPattern's rules. In this case, for him/her charPattern may seem to be tedious. Actually, 150ms of pausing on each dot of the charPattern password affects security especially being prone to shoulder surfing attack. However, we measure charPattern mainly in terms of usability.

6. A main difference may be the advantage of charPattern over ALP in the sense that it provides dual-mode authentication which helps to remove the restriction of using dot-pattern only on touchpad devices.

7. Owing to the previous property, charPattern can also be used on desktop computers. This property gives the priority to charPattern to be used as the Internet authentication, too.

8. Theoretical password space could not be reached in practice with user-chosen passwords since users are more likely to select a password among hotspots, a more popular subset. However, with persuasive technology proposed first with Persuasive Cued Click Points (PCCP) method , hotspots could be avoided. The basic idea is to suggest users a randomly generated password while they are creating their account. While users are allowed to ask for a new suggestion as much as they wanted, this significantly slow the password creation process. Hence a secure password selection becomes “a path of least resistance”. In a sense, use of persuasive technology could be regarded as balancing the tradeoff between system generated passwords and user chosen passwords regarding usability and security properties. In charPattern, we borrow this technique to suggest users a randomly generated pattern password composed of four dot-characters.

charPattern is the knowledge-based authentication system that gives users the chance of entering their passwords either by drawing a pattern, by typing a text or by mixed way to make text passwords easily memorable and easily utilizable.

The proposed system is implemented for both of desktop computers and mobile devices, separately. We describe detailed implementations of Web and mobile applications separately in the following subsections.

3.2 Implementation of Mobile Application

The mobile application is developed on Android SDK platform with 17 API. Like other two authentication methods (text password, gridWordX), charPattern on the mobile device is implemented as a standalone full-screen Android application (see Figure 3.1(c)) which consists of 3 consecutive phases (see Figures 3.2) as in gridWordX [6]. The phases’ specifications of text password and gridWordX are not changed while those of charPattern are designed as follows:

Table 3.1: ALP vs. charPattern.

	Subject of Comparison	**ALP**	**charPattern**
1	# of dots	9	35
2	Dot-matrix size	3x3	5x7
3	Dot interface	only dot	with a unique character
4	Password-length(dot)	[2,9]	4
5	# of possible passwords	389112	1256640
6	Max. password entropy(bit)	17	20
7	Dot selection way	every dot in a path	150 ms pausing on a dot to be selected
8	Dual mode	NO	YES (typing)
9	Compatibility with PC	NO	YES
10	Creating a password	user-selecting	using persuasive technique

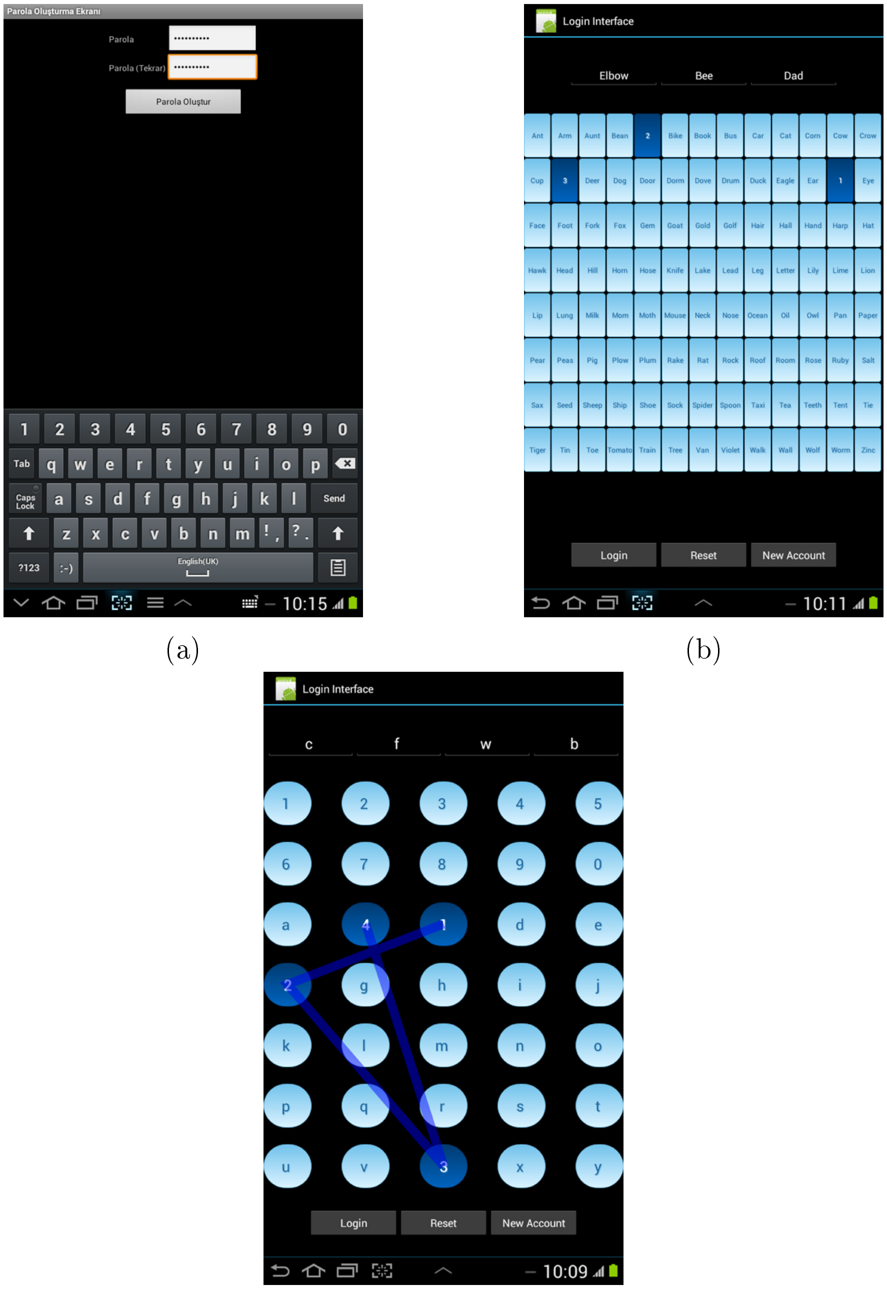
Password Creation & Confirmation phase is designed for creation and confirmation username and password (see Figure 3.2(b)). Initial interface includes 3 textfields (for name, surname, and username) and "create username" button. After creating username, Password Creation interface appears where on the top, 4 textfields (not editable) are located and below of them 35 dots are arranged as a 7x5 (7 rows and 5 columns) 2D dot-matrix (matrix consisting of dot-characters). Each dot includes one unique character (characters are arranged with the order of numbers followed by lowercase letters alphabetically) every of which is not visible in this phase. On the bottom of the interface, 3 buttons, "Accept Password", "Shuffle" and "Go to main page", are also arranged. When "Shuffle" is touched the system automatically suggests random-generated four-dot-character passwords (hence we also call it just charPattern password) in order to prevent users choosing hotspots [23]. Random generating occurs with drawing a pattern between four-dot-characters and typing corresponding characters on four textfields with corresponding order. Users are free to repeat touching on "Shuffle" button until they like either four characters and/or the pattern between four dot-characters. After accepting the charPattern password touching on "Accept Password", Password Creation is supplanted with Password Confirmation interface. In this interface, objects and their arrangement are almost same with those on the previous interface with some differences. The main difference is that here, dot-characters are touchable and characters on dot-characters are visible for users. Users need to draw a pattern connecting 4 dot-characters accepted on the previous step. Significant difference of drawing a pattern on charPattern from that on ALP is that it does not take every dots liying on the pattern due to a four-dot restriction. We conducted a pre-experimental laboratory study with 10 participants and defined appropriate waiting time for choosing a dot of 100 ms which neither affects login time nor increase login error rate. Above the matrix of dots, four textfields accepting exactly one character each are arranged for four characters of charPattern password. The goal of designing in such a way is that when users are typing characters on textfields, the system automatically selects corresponding dot-characters and draws a pattern between them, respectively, and vice versa, when users are drawing a pattern (swiping) connecting four dot-characters from 2D dot matrix, the system automatically makes typing those characters constructing the pattern, on textfields, respectively.

MRT, Mental Rotation Test, is occured after successful confirmation. MRT is implemented so as to remove users' short term memory avoiding users' temporary remembering passwords.

Login Phase (see Figure 3.2(c))with same interface as on Password Confirmation appears after completing MRT. Users need to redraw accepted on creation & confirmation phase, charPattern passwords in order to perform login and terminate the last phase of the mobile application.

3.3 Implementation of Web Application

We also developed charPattern Web application for desktop computers (see Figure 3.3) using PHP, html, Javascript especially widely using Kinetic Javascript library with version 5. As DBMS, the serverless system Sqlite version 3 is used for both of Web and mobile applications. Consisting of two interfaces (in first interface for performing login by username and the second for completing login via charPattern), Web application allow users to perform login from any of desktop computer connected to the Internet. Here, in order to provide consistency, we locate 35 dot-characters in same order as in the mobile application. Unlike in the mobile application, in Web application, drawing a pattern between four dot-characters occurs by clicking four corresponding dot-characters. As an additional feature, here, is that after three unsuccessful login, users are asked to send their charPattern password via email using SMTP protocol.



(a)

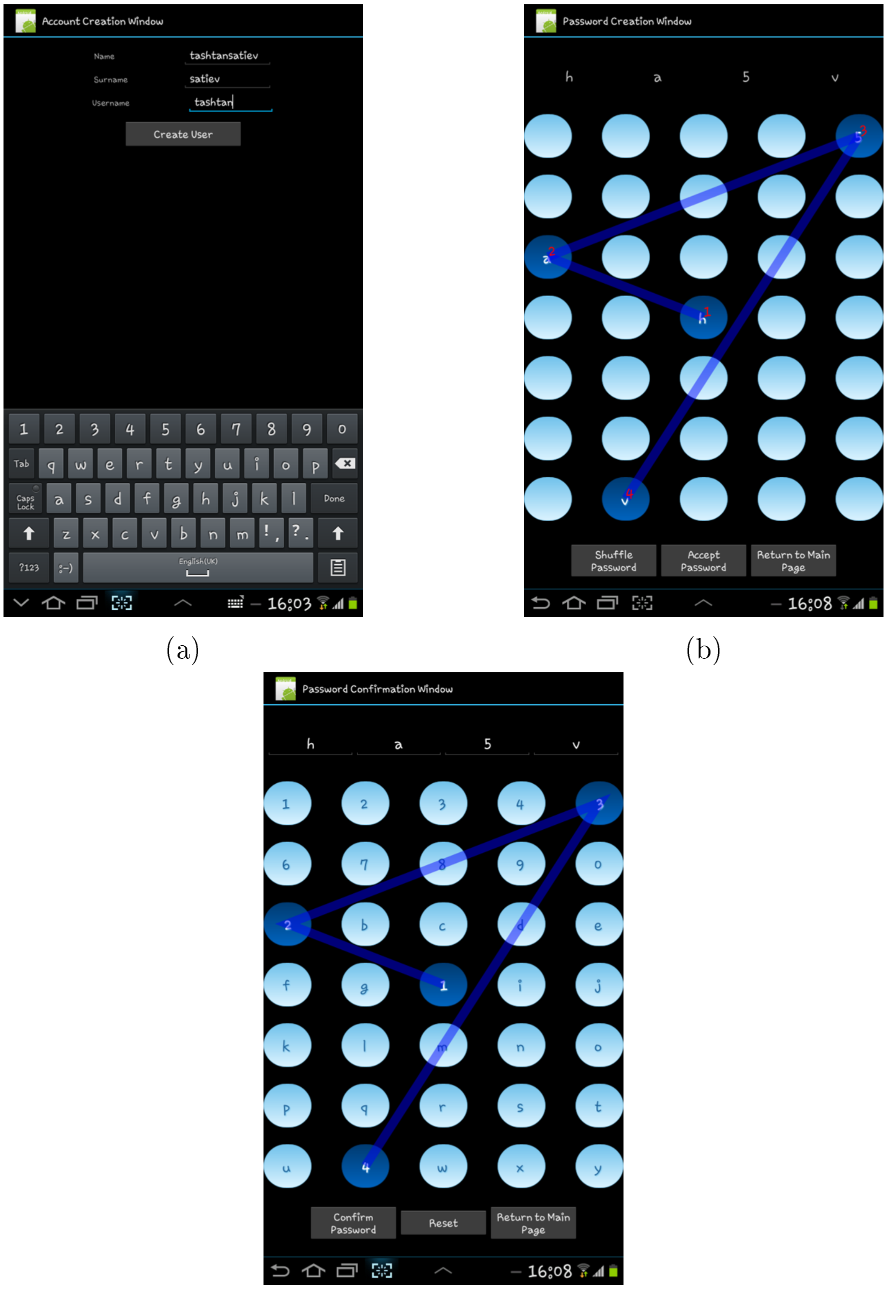
Ant	Arm	Aunt	Bean	2	Bike	Book	Bus	Car	Cat	Corn	Cow	Crow
Cup	3	Deer	Dog	Door	Dorm	Dove	Drum	Duck	Eagle	Ear	1	Eye
Face	Foot	Fork	Fox	Gem	Goat	Gold	Golf	Hair	Hall	Hand	Harp	Hat
Hawk	Head	Hill	Horn	Hose	Knife	Lake	Lead	Leg	Letter	Lily	Lime	Lion
Lip	Lung	Milk	Mom	Moth	Mouse	Neck	Nose	Ocean	Oil	Owl	Pan	Paper
Pear	Peas	Pig	Plow	Plum	Rake	Rat	Rock	Roof	Room	Rose	Ruby	Salt
Sax	Seed	Sheep	Ship	Shoe	Sock	Spider	Spoon	Taxi	Tea	Teeth	Tent	Tie
Tiger	Tin	Toe	Tomato	Train	Tree	Van	Violet	Walk	Wall	Wolf	Worm	Zinc

(b)

1	2	3	4	5
6	7	8	9	0
a	4	1	d	e
2	g	h	i	j
k	l	m	n	o
p	q	r	s	t
u	v	3	x	y

(c)

Figure 3.1: Login Interfaces of three authentication methods on a mobile device: (a) Text password, (b) gridWordX, (c) charPattern.



Account Creation Window

Name: tashtansatiev

Surname: satiev

Username: tashtan

(a)

Password Creation Window

h a 5 v

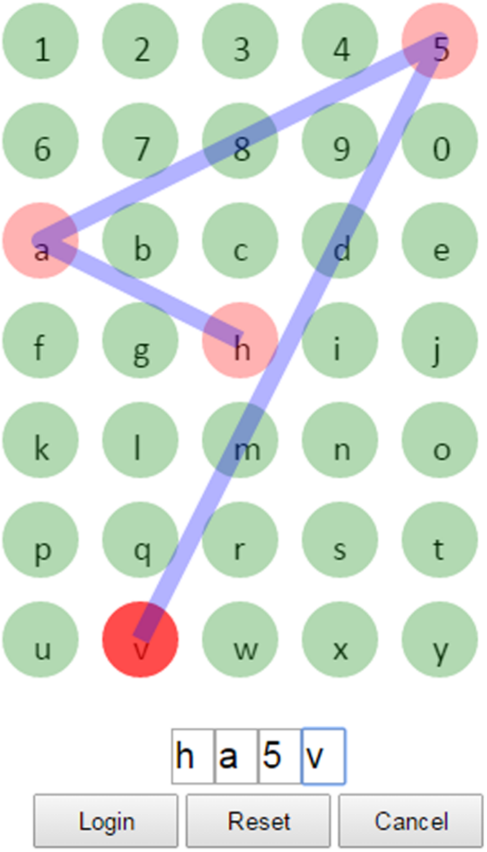
(b)

Password Confirmation Window

h a 5 v

(c)

Figure 3.2: Key Interfaces of charPattern on the Android Application: (a) Account Creation, (b) Password Creation, (c) Login Interface.



1	2	3	4	5
6	7	8	9	0
a	b	c	d	e
f	g	h	i	j
k	l	m	n	o
p	q	r	s	t
u	v	w	x	y

h a 5 v

Figure 3.3: Login Interface of charPattern Web Application.

4. USER STUDY AND ANALYSIS

In this research, we conduct the user study over traditional text password, gridWordX and charPattern so as to measure and compare usability evaluation of charPattern with those of text password and gridWordX. We try to correspond each authentication technique with regard to password entropy, number of interfaces and devices on which users perform login via these methods. Before the user study, we defined our hypotheses as follows:

1. Login process with charPattern takes shorter time than via text-based authentication on mobile devices.
2. Login process with charPattern takes shorter time than via griWordX on mobile devices.
3. Login process with charPattern takes comparable time with those on text passwords on desktop computers having physical keyboard.
4. Login process with charPattern takes comparable time with those of gridWordX on desktop computers having physical keyboard.

In the user study, 25 computer-engineering students (17 males and 8 females) from TOBB ETU university, the ages of which are ranged between 19 and 28, participated. We note that every participant is familiar with performing the Internet login on desktop computers and mobile devices by typing a text, drawing a pattern and (or) by clicking.

4.1 Sessions of the Study

The user study has a within-subjects design and consists of four sessions, intervals of which are between 4 and 7 days (why the intervals are not fixed is revealed in next chapters). In the first session, each participant is invited to the lab and asked to create an account by entering a username and creating a password on a mobile device. A password is created for all three systems; text password authentication, gridWordX and charPattern hence each participant has three passwords in total. Then, participants also perform login on the mobile device by created username and password after solving a mental rotation test (MRT) to remove users' short term memory. We employ counterbalancing between password methods to handle order effects.

In the second and third sessions, the participants just perform login on own desktop computers remotely by their username-password pairs created in the first session (with all three systems).

In the last session, the participants are re-invited to the lab and asked to perform a second login on the mobile device with their username-password pairs created in the first session (again via all three systems).

4.2 Pre-experimental Instruction

Before the first session, a brief presentation about the user study was provided which included generalized oral instruction and demonstrative authentication via three techniques (particularly, demonstrative authentication via charPattern is clarified later on) for the participants. The oral instruction covered following criteria:

- We emphasize that our aim is evaluating authentication methods they perform login, but not experimenting participants themselves.
- We ask participants to create text passwords which consists of at least eight characters.
- We ask them not to use a password they use in real life as the text password

they create for the study.

- The participants should not take a note of their created passwords in any form(writing down, taking a photo etc.).
- The participants are asked to treat their passwords as a real passwords rather than just experimental as they have to use them in future sessions, again.

4.3 Lab Study

As participants perform login on the mobile device in the first and the last sessions, it regarded as the lab study. Consisting of two sessions, the lab study is carried out in the laboratory environment for each participant individually taking advantage of each one's own behavior and perception. Before the beginning, the demonstrative authentication, which included creation & confirmation and login steps of each method, was conducted. In demo part, apart from text-based and gridWordX authentication, following kinds of charPattern specifications as a methodology were also shown:

- ∗ How to generate charPattern password touching on shuffle button.
- ∗ When drawing a pattern, the participants should make pause over each dot-character they wish to select without taking off the fingers and they should drag fingers a bit fast while drawing a pattern from one dot-character to another avoiding making selection of incorrect dot-characters.
- ∗ Participants can touch on reset button or just redraw a pattern in case if they want reset the last drawn pattern.

In the lab study, as the experimental mobile device, we strictly used only Sumsung Tab2 7 inch tablet with Android SDK API 17 which has 600x1024 resolution and

170 ppi pixel density trying to conduct the study under same conditions. We supposed that the participants' own mobile devices or other models may affect results of the study due to different size, performance and software platforms.

The first session of the lab study was conducted within three days since our schedule was flexible with regard to participants' university courses and the study was held individually with each participant. After three weeks (during this time the web study was held) the second session of the lab study was conducted with same period as those of the first session. Unlike in the first session, in this one, the participants just performed login on the mobile device (Android mobile app used in the first session is re-implemented providing only its login interface) with all three authentications methods. The participants filled out a post-task questionnaire after the second login performed during their second visit to the lab.

4.4 Web Study

As second and third sessions were conducted over the Web, we considered it as a web study. The web study was held to compare usability of charPattern with traditional text password and gridWordX on desktop computers. The first session of the Web study was scheduled after one week of the Web study's first session. Conducted with the period of one week, in both sessions of the web study the participants performed login via each of three authentication methods from web browsers with username-password pairs created by themselves in the first session of the lab study, respectively. We asked participants not to use their touch-screen devices in the web study. But we did not ask anything particular regarding mouse use. The users were free to use a keyboard or a mouse (applicable only with gridWordX and charPattern) to enter their passwords. In the web study, users were allowed to ask for their passwords through email if they decided they could not recall their passwords after three unsuccessful trials.

4.5 Results

The data from the user study are collected according to following kinds:

Timing and Number of Attempts. For direct comparison of test results, times for creation and confirmation and login times of each schema are collected. In fact, times for creation & confirmation are obtained in the first session of lab study(when the password is created and confirmed). On the other hand, login times are obtained in each of four sessions when the participants performed login. The number of attempts until the correct login are kept in order to calculate success rates of each participant (success rates are calculated as the the ratio of attempts performed no more than three times to the number of overall trials) when she performs login via each method. Each time measuring begins with the appearance of the interface and ends with touching on "Confirm Password" ("Login") button.

Number of Shuffles. We remind that shuffle is occurred (see Design and Implementation) during changing a random-generated password (in gridWordX and charPattern)

Modes of Input. Modes of input in each login are collected in gridWordX and charPattern so as to observe the participants prefer either typing, drawing (clicking) or mixed mode. In addition, we examine the effect of modes to success rates.

Questionnaire. After the final session of the study the participants were asked a couple of questions (in details about the questions we reveal in the next chapter) to observe the participants' behaviors and perceptions related to charPattern.

Table 4.1: Friedman Test Results for Lab Study

Method Name	Mean Ranks			Test Results	
	First Login	Last Login		First Login	Second Login
text password	2.93	2.84	Chi-Square	31.76	26.64
gridWordX	1.56	1.64	df	2	2
charPattern	1.52	1.52	Asymp.Sig.	0.00000	0.00000

4.6 Collected Data Analysis

Here, we give statistical analysis of above mentioned data sets. By default, we find analysis meaningful with the condition that p value is less than 0.05.

Confirmation and Login Times, Success Rates. We take total time of times for creation and confirmation for each schema (see Figure 4.1). Likewise, total values of login times during the lab study (see Figure 4.2) (we mention that consisting of two sections, the lab study was conducted on the mobile device and login was performed in both sessions) and those of login times during the Web study (see Figure 4.3) (the Web study was conducted on desktop computers through Web in two sessions being performed login in each of them) of every participant for each methods are examined for conducting statistical measurements.

Analyzing data of total login times of each of three schemata on the mobile device (lab study) we obtain high significant difference between three datasets applying non-parametric k-related sample-test Friedman to three datasets in each of two sessions, separately as shown in Table 4.1. Likewise, Table 4.2 presents results of how non-parametric k-related sample-test Friedman is applied for analyzing login times of text password, gridWordX and charPattern together in the Web study. Here, we find no significant difference though charPattern has shorter login time than of text password and gridWordX.

Table 4.3 represents success rates (for calculation of success rates see previous

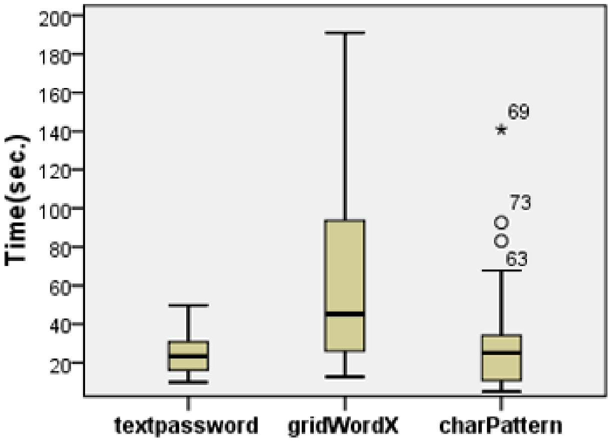


Figure 4.1: Creation & Confirmation times.

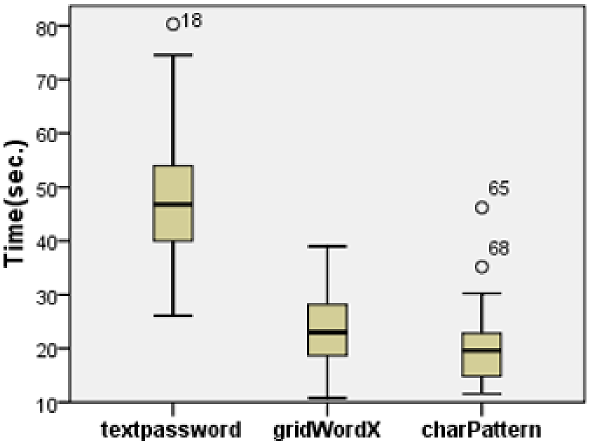


Figure 4.2: Login times in lab study.

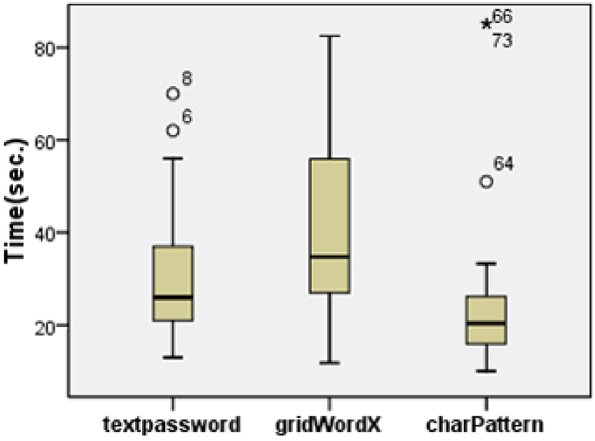


Figure 4.3: Login times in web study.

Table 4.2: Friedman Test Results for Web Study

Method Name	Mean Ranks			Test Results	
	First Login	Last Login		First Login	Second Login
text password	1.92	2.16	Chi-Square	4.16	2.96
gridWordX	2.32	2.12	df	2	2
charPattern	1.76	1.72	Asymp.Sig.	0.125	0.228

Table 4.3: Login Success Rates

	Create & Confirm	Login Sessions			
		First	Second	Third	Fourth
text password	25/25	25/25	24/25	25/25	25/25
Success Rates	100.00 %	100%	96%	100%	100%
gridWordX	23/25	25/25	17/25	23/25	25/25
Success Rates	92%	100%	68%	92%	100%
charPattern	25/25	24/25	16/25	24/25	25/25
Success Rates	100%	96%	64%	96%	100%

subsection) of text password, gridWordX and charPattern with regard to creation & confirmation and each login process. We apply non-parametric k-related sample-test Friedman to calculate success rates and obtain no significant difference.

Shuffles. We remind that shuffle feature exists only on gridWordX and charPattern (see Design and Implementation). As represented in Table 4.4, shuffle count of charPattern is less than of gridWordX, but applying the paired-sample Wilcoxon test, we obtain no significant difference between them.

Table 4.4: Shuffle Results of gridWordX and charPattern

	N	Mean	Std. Dev	Min	Max
gridWordX	25	4.60	7.984	0	36
charPattern	25	1.56	1.981	0	7

To examine data of shuffles, the number of participants in gridWordX utilizing more than 5 shuffles is 5, whereas in charPattern it equals to 1. In Table 4.5 (row with number 1 belongs to gridWordX, number 2 to charPattern), how low and high numbers of shuffles in gridWordX and charPattern may influence on success rates is presented.

Table 4.5: Effects of Shuffles on Success Rates for gridWordX and charPattern

	# of Shuffles	# of Trials	Confirm and Login Success Rates				
			Conf.	1st	2nd	3rd	4th
1	Low:<6	20 (80%)	95%	100%	70%	90%	100%
	High:>5	5 (20%)	80%	100%	60%	100%	100%
2	Low:<6	24 (96%)	100%	95.8%	62.5%	96.8%	100%
	High:>5	1 (4%)	100%	100%	100%	100%	100%

Input Modes in gridWordX and charPattern. We remind that participants can use as input modes of typing, drawing or hybrid mode in charPattern while in gridWordX, clicking is used instead of drawing. Distribution of the participants under these three input modes is shown in table 4.6.

Table 4.6: Frequency of Input Modes in charPattern and GridWordX

		Create & Confirm	Logins			
			wk 1	wk 2	wk 3	wk 4
gridWordX	clicking	25	24	23	23	25
	typing	0	0	1	0	0
	hybrid	0	1	1	2	0
charPattern	drawing	25	25	22	24	25
	typing	0	0	2	1	0
	hybrid	0	0	1	0	0

User Perception. In the questionnaire, we included in total of ten questions regarding to charPattern: eight questions are answered according to 10-point Likert-scale (1 is disagreement, 10 is strong agreement), one choice question and one yes/no question . As represented in Table 4.7, we witness for the positive opinion of the participants to charPattern and especially highest rates in that that performing login both on desktop and mobile devices was easy via charPattern. Even though the participants had been notified not using their real passwords as text passwords in the study, 10 participants used same passwords they use currently or had used before. Related to the question 9, answers of

Table 4.7: The Questionnaire Results.

	Question	Mean
Q1	Using pattern makes charPattern easily memorable.	8.56
Q2	Distances between dots were NOT critique in drawing a pattern.	6.76
Q3	I easily created a password in charPattern.	8.68
Q4	Login using charPattern was easy on a desktop computer.	9.48
Q5	Login using charPattern was easy on a mobile device.	9.08
Q6	I liked charPattern as much as a text password.	8.04
Q7	charPattern is at least as secure as a text password.	7.72
Q8	The password I entered was similar to the one I used previously.	6.72
Q9	Do you continuously use ALP? a. I do not use.,b. I used in the past c. I use it currently	a-3 b-16 c-6
Q10	Does an increased number of dots in charPattern than of Google make charPattern unusable? Yes/No	Yes-8 No-17

the participants for alternatives a, b, c are 3, 16, 6, respectively, which is said that almost every participant is aware of ALP. For the last question of the questionnaire 8 participants answered positively in contrast to 17 participants who think that having more dots (35 dots) than traditional ALP is not unusable.

5. DISCUSSION

Before the user study, we conjectured that users would spend less time to login with charPattern on a mobile device because drawing a pattern is much natural than typing on a virtual keyboard (as in text passwords) or touching on cells in a grid (as in gridWordX). According to test results shown in Table 4.1, charPattern is faster than text password and gridWordX with respect to login times on the mobile device which supports our first two hypotheses (see Hypotheses and User Study), simultaneously. Here, we can see the effect of drawing over touching and typing.

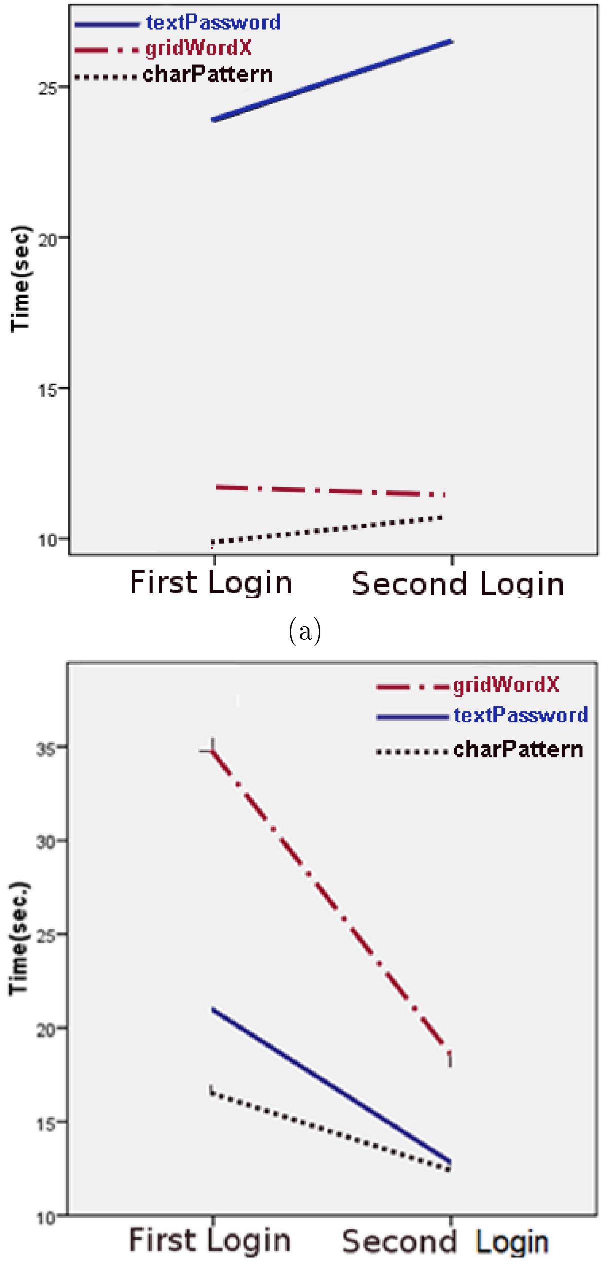
When comparing login times of text password, gridWordX and charPattern in the Web study by Friedman test, there is no significant difference (see Table 4.2). On the other hand, observing not high differences between obtained asymptotic significance for both sessions of the Web study (for the first and last login, asymptotic significances are equal to 0.125, 0.228, respectively as shown in Table 4.2) and p value of 0.05, we apply the paired-sample Wilcoxon test to the login times of charPattern together with those of text password and gridWordX separately for each session and we find charPattern faster than gridWordX with regard to login times with marginal significant differences (asymptotic significance in the first and last sessions are 0.045 and 0.069, respectively) which controverts hypothesis 4. On the other hand, applying Wilcoxon test to login times of charPattern and text password we obtain not significant difference which supports hypothesis 3, where charPattern takes login times comparable those of text password. Before the user study, we conjectured that on a machine without a touchscreen the advantage of charPattern regarding login times is lost because drawing the pattern on the screen is no longer possible. But we thought charPattern still yields comparable login times with the other methods since users have the chance to try other modes of input *i.e.*, by typing. After the user study, we see that the expected result is observed due to a reason not we have foreseen. In the user study, users still prefer drawing the pattern over typing the password but this time with a mouse or a touchpad. Since drawing a pattern with a mouse or a touchpad is not as comfortable as drawing it on the screen, the login times turned out to be as expected. However, by observing text passwords of the participants, we notice that ten passwords consist of consecutive digits, or phone numbers or just names concatenated with birth years of the participants.

It is necessary to point out that 6 participants sent us email after the first session of the Web study (conducted on desktop computers) that they erroneously tried to login via charPattern by drugging a mouse instead of just clicking dots during drawing a pattern (We remind that during the pre-experimental instruction demonstrative authentication via three methods were shown on the mobile device but not on the desktop computer) which provoked login time on desktop computers. To reveal this impact on login times, we examine success rates of three methods with single attempt presented in Table 5.1 and observe that success rates of the first login on the desktop computer via charPattern is 52%.

Table 5.1: Login Success Rates with Single Attempt

	Create &	Login Sessions			
	Confirm	1st	2nd	3rd	4th
text password	25/25	20/25	22/25	23/25	22/25
Success Rates	100%	80%	88%	92%	88%
gridWordX	19/25	21/25	15/25	20/25	23/25
Success Rates	76%	84%	60%	80%	92%
charPattern	20/25	22/25	13/25	21/25	23/25
Success Rates	80%	88%	52%	84%	92%

As seen in Figure 5.1(a), there exist slight slopes from the second login times to the first login with all three methods on the mobile device which presents that the login time in the second login on the mobile device takes longer that the one in the first login for all three methods. This results suggest that although we applied a MRT test, users were more comfortable in entering their passwords just after they created it. In addition, for charPattern, most likely, it is due to the fact that the last login on the mobile device was conducted after 3 weeks as the first session



(a)

(b)

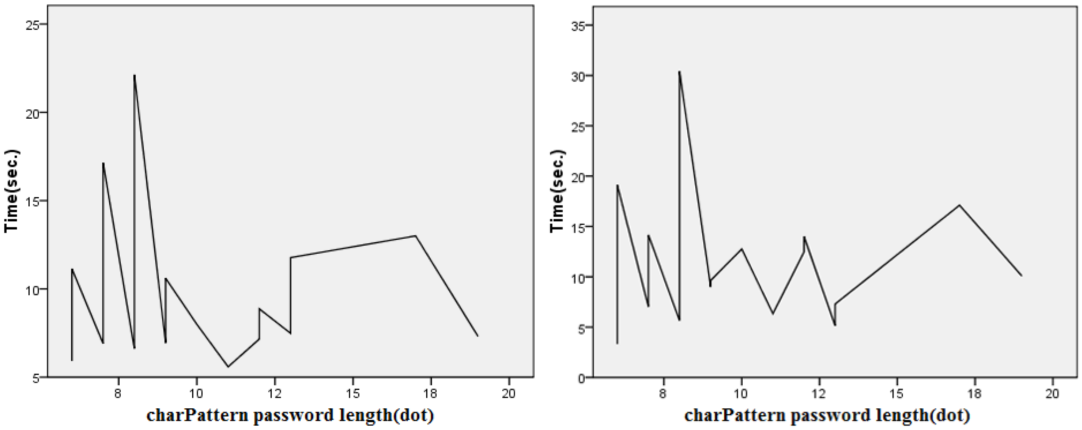
Figure 5.1: Means of Login Times of three methods on Web and Lab Studies: (a) Login Times on the Mobile Device, (b) Login Times on Desktop Computers.

was finished which affects the participants in reusing their passwords and dealing with a new system (selecting definite dots and drawing a pattern between them correctly). On the other hand, in Figure 5.1(b), we observe reverse slope between subsequent login times in the Web study with all three methods which shows that login times in the last session were shorter than of first session for all three methods. Here, the participants' consecutive performing login via charPattern on desktop computers within a week should be taken into the consideration. The important point here is that in the lab study the difference between login times of charPattern and text passwords holds for both logins (on the other hand, the difference between gridWordX and charPattern drops significantly).

Unlike distribution of kinds of input modes among the participants in gridWordX , where percentages of the total numbers of hybrid and typing modes used during performing login within two sessions on the mobile device and on desktop computers separately are 15.15% and 12.12%, respectively. In this research, they are 2% and 8% on gridWordX, 0% and 8% on charPattern as presented in Table VI. First of all, it can be explained as a users' growing trend towards using touch-pad devices. Consequently, it can be also possible that after performing login on the mobile device by touching or drawing, many of the participants opted to login via gridWordX and charPattern by clicking than typing on desktop computers even though typing text passwords on desktop computers is traditional. In addition, opting to draw than type is based on look and feel principle.

The survey results show (see Table 4.7) that users find charPattern easy-to-use both on desktops and mobile devices. It is surprising to see that users find charPattern easier to use than text passwords more on desktop machines than mobile devices (although the difference is not significant).

Furthermore, in the study, we examine either long distances between 4 selected dot-characters in the pattern of charPattern affect usability of the system on mobile devices. To reveal this, we asked the question in the questionnaire regarding to being long of distances between dot-characters (see Table 4.7, question 2) and also tried to prove it examining obtained dataset. By behavior of



(a) (b)

Figure 5.2: Correlation between Login Times on the mobile device via charPattern and charPattern password-lenghts in Euclidean distance ((a) First Session, (b) Second Session).

the participants, being long of distances between dot-characters in charPattern is not critique (where mean of notes for the second question of the questionnaire is 6.76 which is greater than 5). However, due to the limitation of the number, kinds of participants and etc. the obtained result may not suffice for strong deduction. Using data of selected dots from dataset, lengths of patterns in the charPattern password of each participant are calculated. It is done by summarizing Euclidean distance of selected dot-characters between first and second, second and third, and third and last with regard to dot-length (The maximum and minimum of charPattern password lengths can be 27 and 3, respectively). We examine the correlation between found distances of charPattern and login times of the participants, respectively, in the lab study (on the mobile device) as presented in Figure 5.2(a) and 5.2(b), and do not observe any ascending noticeable trend. It means that distances between dot-characters do not significantly affect login times.

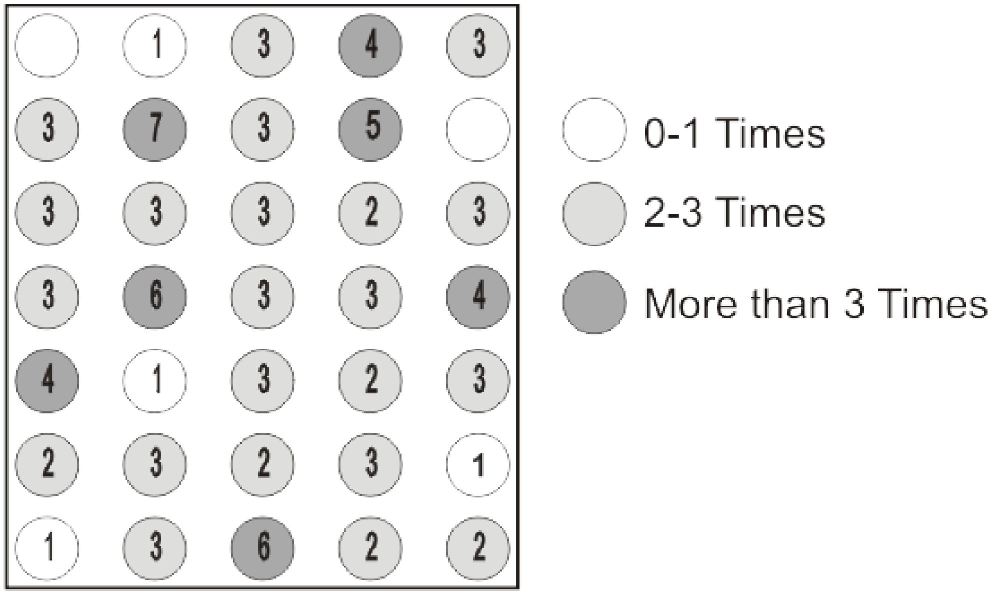
5.1 Limitations

We tried to conduct the user study taking into account of a number of limitations. The one of noticeable limitations is with regard to the focus group. First of all, the participants were not from different audiences but they were all computer engineering students which affected the login times and answers to questionnaire. Secondly, the number of participants was 25 which did not suffice for making sharp analysis. The following limitation is technical limitaion. In other words, in the study, the restricted number of devices were used in processing login. To exemplify, in the lab study we used only one 7 inch tablet device trying to make equal conditions for participants. The last of significant limitations is time restriction. We conducted the study within a month which were short for better analyzing memorability of charPattern.

5.2 Security Analysis

We mentioned that the password entropy of charPattern is 20 bits which can safeguard against online attacks with lockout rules. In charPattern, we mitigate guessing and dictionary attacks by disallowing user-chosen passwords and suggesting users randomly generated passwords. On the other hand, hotspots are still could weak points of charPattern (hitting the "Shuffle" button until an easy-to-guess password is suggested.) with regard to security [13] which can be prone to shoulder surfing [29] and guessing attacks. As the hotspots in charPattern, dots located on the edges of dot-matrix especially on the corner parts are assumed. While, patterns like rectangles, diamonds dots of which are located very closely or located on the edges, can weaken the charPattern password. In this section, we tried to estimate these two weaknesses by the methods used in previous researches [13], [6].

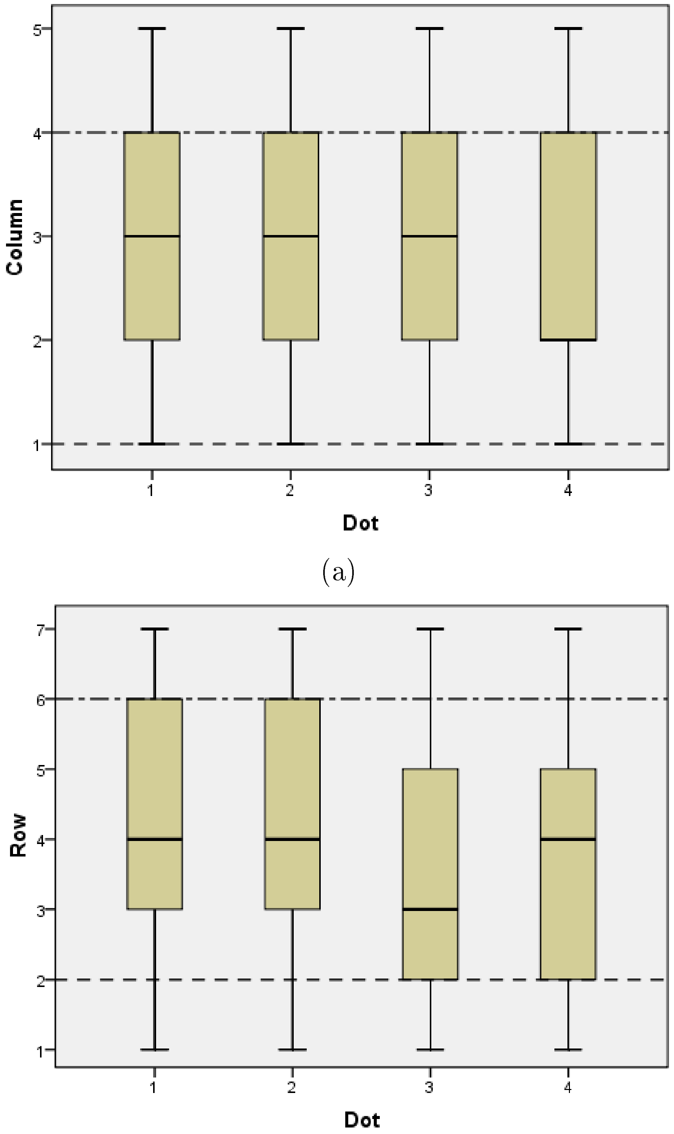
We remind that as in the previous graphical authentication systems [13], [6],



	1	3	4	3
3	7	3	5	
3	3	3	2	3
3	6	3	3	4
4	1	3	2	3
2	3	2	3	1
1	3	6	2	2

Figure 5.3: Frequency of Selected Dots in charPattern.

[30], here also users can change randomly-generated passwords by touching the "shuffle" button until appearing the best fit charPattern password for users. On the other hand, using "shuffle" button, users are likely select hotspots. Figure 5.3 presents the frequency table of dots selected by the participants where 17.14% were selected 0-1 times, 62.86% were 2-3 times and 20% of dots were selected more than 3 times. Here, we need to notice that two dot-characters (characters "1" and "0") were never selected, while the dot-character with a character of "7" was selected 7 times. To understand whether this particular distribution is different than a random distribution, we generate simulated data consisting of 100 datasets each of which has 25 pairs of (x, y) elements where x ranges from 1 to 5 and y ranges from 1 to 7 corresponding to the size of data in our user study charPattern. Figures 5.4(a) and 5.4(b) present box-plots of distributions of selected dots with horizontal lines representing maximum and minimum medians of simulated datasets. Here, as observed, median values of selected dot-characters are between maximum and minimum medians of simulated datasets. Then, we calculate rough estimate values of password entropy for the collected dataset together with random datasets using the formula H(X) defined in [13]. Our



(a)

(b)

Figure 5.4: Distribution of dots in Cartesian System where horizontal lines denote maximum and minimum medians of simulated datasets ((a) Dot Arrangements by Columns, (b) Dot Arrangements by Rows).

rough estimate password entropy of collected dataset is between maximum and minimum entropy values of simulated datasets. Since each random dataset represents a chance to include the observed data, with 99% probability, the user study dataset is a dataset occurred by chance. This analysis gives an evidence that hotspots does not skew the password distribution for charPattern. The one of main advantages of charPattern with regard to security is that as in other dotPattern authentication systems, charPattern passwords are not stored on any devices used and anywhere on the Internet [31]. On the other hand, patterns are prone to such attacks as dictionary, shoulder-surfing and smudge attacks [32]. Although patterns like rectangles, diamonds can leverage memorability of charPattern password (We do not know specific goals, but 3 participants used charPattern passwords with crossed-line patterns), this case may reduce the password entropy making security trade-off to usability.

6. CONCLUSION

In spite of usability problems of traditional text passwords especially on mobile devices, text passwords are still in use for device and Internet authentications owing to its simplicity and familiarity. Alternative authentication techniques to the traditional text-based authentication such as password managers, graphical passwords, biometric passwords which have better usability features than of text passwords are being established. However, some of these new techniques are not workable on desktop computers with respect to hardware requirements, others of them have their own security deficiencies.

As Android Lock Pattern has successfully demonstrated, drawing a pattern-password is preferred over typing a password or a PIN by many users for locking/unlocking their touchscreen devices. However, lock patterns could not be used over the Internet directly for remote user authentication due to different security and usability requirements. In this thesis, we introduce charPattern, a new pattern-based authentication method which increases password space to adequate levels (i) by increasing number of possible patterns by careful addition of more dots, (ii) by using persuasive technology to avoid hotspot passwords (more popular patterns). To accommodating users who alternately login from devices with and without full physical keyboards, the new scheme improves on the idea of Android Lock Pattern by introducing a second mode of input by enabling users to type the characters corresponding the dots forming their pattern-password.

In this research, we implement charPattern, the dual-mode authentication system supporting both of drawing and typing, in which users can draw pattern along 2D dot-matrix where unique characters are arranged on each of those 35 dots in order to easily memorize charPattern passwords or just type characters which are on dots.

To make a usability evaluation, we conduct the user study on mobile devices and desktop computers comparing charPattern's timing and success rates with those of traditional text password and gridWordX [6]. The study results shows that charPattern has shorter login times than text password and gridWordX on the mobile device and also charPattern is faster regarding to login process than gridWordX on desktop computers, while it has comparable login times with text password on desktop computers. In addition, most users prefer to enter charPattern passwords by drawing the pattern rather than by typing via keyboard even on desktop machines, which leads to login times comparable to those of text passwords on desktops. Based on user study findings, we conclude that charPattern is a promising alternative to text passwords for those who access same sites from both of mobile devices and desktops.

REFERENCES

[1] G.E. Blonder. Graphical password, September 24 1996. US Patent 5,559,961.

[2] J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: empirical results. *Security Privacy, IEEE*, 2(5):25–31, Sept 2004.

[3] Eiji Hayashi and Jason Hong. A diary study of password usage in daily life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, pages 2627–2630, New York, NY, USA, 2011. ACM.

[4] J. Alex Halderman, Brent Waters, and Edward W. Felten. A convenient method for securely managing passwords. In *Proceedings of the 14th International Conference on World Wide Web*, WWW '05, pages 471–479, New York, NY, USA, 2005. ACM.

[5] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun. ACM*, 42(12):40–46, December 1999.

[6] Ugur Cil and Kemal Bicakci. gridwordx: Design, implementation, and usability evaluation of an authentication scheme supporting both desktops and mobile devices. *Workshop on Mobile Security Technologies (MoSTâĂŹ13)*, 2013.

[7] Rui Zhao and Chuan Yue. All your browser-saved passwords could belong to us: A security analysis and a cloud-based new design. In *Proceedings of the Third ACM Conference on Data and Application Security and Privacy*, CODASPY '13, pages 333–340, New York, NY, USA, 2013. ACM.

[8] Sonia Chiasson, P. C. van Oorschot, and Robert Biddle. A usability study and critique of two password managers. In *Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15*, USENIX-SS'06, Berkeley, CA, USA, 2006. USENIX Association.

[9] Emanuel von Zezschwitz, Paul Dunphy, and Alexander De Luca. Patterns in the wild: A field study of the usability of pattern and pin-based authentication on mobile devices. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, MobileHCI '13, pages 261–270, New York, NY, USA, 2013. ACM.

[10] Shari Trewin, Cal Swart, Larry Koved, Jacquelyn Martino, Kapil Singh, and Shay Ben-David. Biometric authentication on a mobile device: A study of user effort, error and task disruption. In *Proceedings of the 28th Annual Computer Security Applications Conference*, ACSAC '12, pages 159–168, New York, NY, USA, 2012. ACM.

[11] Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Comput. Surv.*, 44(4):19:1–19:41, September 2012.

[12] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. Quantifying the security of graphical passwords: The case of android unlock patterns. In *Proceedings of the 2013 ACM Conference on Computer and Communications Security*, CCS '13, pages 161–172, New York, NY, USA, 2013. ACM.

[13] Kemal Bicakci and Paul C. van Oorschot. A multi-word password proposal (gridword) and exploring questions about science in security research and usable security evaluation. In *Proceedings of the 2011 Workshop on New Security Paradigms Workshop*, NSPW '11, pages 25–36, New York, NY, USA, 2011. ACM.

[14] L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, Dec 2003.

[15] Cormac Herley and Paul van Oorschot. A research agenda acknowledging the persistence of passwords. *IEEE Security and Privacy*, 10(1):28–36, January 2012.

[16] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Authentication using graphical passwords: Effects of tolerance and image choice. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, SOUPS '05, pages 1–12, New York, NY, USA, 2005. ACM.

[17] Paul Dunphy, Andreas P. Heiner, and N. Asokan. A closer look at recognition-based graphical passwords on mobile devices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 3:1–3:12, New York, NY, USA, 2010. ACM.

[18] Florian Schaub, Marcel Walch, Bastian Könings, and Michael Weber. Exploring the design space of graphical passwords on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 11:1–11:14, New York, NY, USA, 2013. ACM.

[19] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. *Int. J. Hum.-Comput. Stud.*, 63(1-2):128–152, July 2005.

[20] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. The design and analysis of graphical passwords. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, SSYM'99, pages 1–1, Berkeley, CA, USA, 1999. USENIX Association.

[21] Hai Tao and Carlisle Adams. Pass-go: A proposal to improve the usability of graphical passwords. *International Journal of Network Security*, 7(2):273–292, 2008.

[22] Sacha Brostoff, Philip Inglesant, and M. Angela Sasse. Evaluating the usability and security of a graphical one-time pin system. In *Proceedings*

of the 24th BCS Interaction Specialist Group Conference, BCS '10, pages 88–97, Swinton, UK, UK, 2010. British Computer Society.

[23] T. Rakesh Kumar and S. V. Raghavan. Passpattern system (pps): A pattern-based user authentication scheme. In *Proceedings of the 7th International IFIP-TC6 Networking Conference on AdHoc and Sensor Networks, Wireless Networks, Next Generation Internet*, NETWORKING'08, pages 162–169, Berlin, Heidelberg, 2008. Springer-Verlag.

[24] Eusing Maze Lock 3.1. www.bit.ly/maze203, 2014.

[25] Markus Jakobsson and Ruj Akavipat. Rethinking passwords to adapt to constrained keyboards. In *Proceedings of Mobile Security Technologies*, 2012.

[26] William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, Emad A. Nabbus, U.S. Department of Commerce, National Institute of Standards, and Technology. *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology - Special Publication 800-63-1.* CreateSpace Independent Publishing Platform, USA, 2012.

[27] Dinei Florêncio, Cormac Herley, and Baris Coskun. Do strong web passwords accomplish anything? In *Proceedings of the 2Nd USENIX Workshop on Hot Topics in Security*, HOTSEC'07, pages 10:1–10:6, Berkeley, CA, USA, 2007. USENIX Association.

[28] Dinei Florêncio, Cormac Herley, and Paul C. van Oorschot. An administrator's guide to internet password research. In *28th Large Installation System Administration Conference (LISA14)*, Seattle, WA, November 2014. USENIX Association.

[29] Arash Habibi Lashkari, Samaneh Farmand, Omar Bin Zakaria, and Rosli Saleh. Shoulder surfing attack in graphical password authentication. *CoRR*, abs/0912.0951, 2009.

[30] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P.C. Van Oorschot. Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *Dependable and Secure Computing, IEEE Transactions on*, 9(2):222–235, March 2012.

[31] DotPass Security Discussion. www.lostminds.com/content/, 2014.

[32] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. Smudge attacks on smartphone touch screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies*, WOOT'10, pages 1–7, Berkeley, CA, USA, 2010. USENIX Association.

APPENDIX

A. DATA

Table A.1: Login Times of Three Methods in The Lab Study Sessions (in the table, text-text Password, grid-gridWordX, char-charPattern).

	Session1(sec.)			Session2(sec.)			Average(sec.)		
	text	grid	char	text	grid	char	text	grid	char
1	20.427	10.179	11.77	19.583	6.915	6.814	20	8	9
2	10.105	6.824	7.497	16.005	16.214	6.994	13	11	7
3	23.049	11.983	10.145	30.933	17.329	10.012	26	14	10
4	19.758	7.772	10.568	27.047	31.197	8.99	23	19	9
5	16.066	14.491	7.481	19.923	8.611	7.299	17	11	7
6	24.603	6.628	11.140	79.863	13.261	19.127	52	9	15
7	17.947	7.602	6.170	17.097	21.002	11.645	17	14	8
8	24.678	9.014	9.703	25.951	7.097	5.140	25	8	7
9	20.767	14.293	7.790	19.996	14.998	9.669	20	14	8
10	29.527	14.567	5.912	15.628	12.198	5.656	22	13	5
11	31.331	7.211	7.988	22.666	10.314	12.756	27	8	10
12	50.162	16.160	6.621	24.388	6.284	5.665	37	11	6
13	18.436	8.961	6.902	21.545	9.851	14.156	19	9	10
14	19.026	27.814	8.869	23.062	9.202	14.006	21	18	11
15	35.463	12.296	15.796	15.860	9.715	30.413	25	11	23
16	22.114	6.365	14.246	25.712	22.085	10.727	23	14	12
17	26.915	14.182	17.149	43.395	9.234	7.035	35	11	12
18	19.625	16.084	22.134	60.685	8.317	13.031	40	12	17
19	19.426	9.244	6.937	25.055	6.537	9.630	22	7	8
20	24.083	18.739	7.163	29.25	9.462	12.456	26	14	9
21	14.997	6.807	5.589	15.404	6.037	6.342	15	6	5
22	15.438	5.144	8.646	24.453	5.633	3.325	19	5	5
23	48.372	10.693	13.001	25.372	7.973	17.111	36	9	15
24	30.610	18.339	7.312	19.856	8.773	10.084	25	13	8
25	13.102	11.655	10.608	13.329	7.471	9.276	13	9	9

Table A.2: Login Times of Three Methods in The Web Study Sessions (denoted in the table: text-text Password, grid-gridWordX, char-charPattern).

	Session2(sec.)			Session3(sec.)			Average(sec.)		
	text	grid	char	text	grid	char	text	grid	char
1	11	23.291	7.534	8	7.235	6.908	9	15	7
2	7	39.610	10.670	13	12.94	5.681	10	26	8
3	9	13.175	6.514	7	23.750	12.820	8	18	9
4	10	16.077	62.380	26	10.910	33.910	18	13	48
5	12	10.079	13.620	10	4.574	6.782	11	7	10
6	38	13.501	8.506	24	21.230	11.700	31	17	10
7	10	10.236	5.499	21	5.536	7.192	15	7	6
8	58	43.387	15.460	12	33.220	10.740	35	38	13
9	13	14.862	5.239	13	12.560	19.190	13	13	12
10	14	165.850	19.230	9	8.773	5.923	11	87	12
11	82	14.782	8.330	13	21.470	6.734	47	18	7
12	13	42.168	21.540	19	13.300	4.952	16	27	13
13	10	35.942	11.380	6	66.030	6.260	8	50	8
14	16	29.760	22.100	21	21.310	28.900	18	25	25
15	16	34.923	7.599	10	47.550	13.300	13	41	10
16	46	20.098	34.850	10	8.310	50.280	28	14	42
17	11	41.231	8.554	2	17.130	5.358	6	29	6
18	7	32.522	9.695	14	34.700	8.029	10	33	8
19	44	16.536	8.100	8	39.380	7.836	26	27	7
20	14	16.368	26.460	11	15.690	6.804	12	16	16
21	17	5.835	4.245	14	5.984	5.813	15	5	5
22	6	19.771	20.570	13	7.319	5.050	9	13	12
23	11	14.217	51.200	10	7.505	33.900	10	10	42
24	42	8.876	14.600	9	12.520	9.453	25	10	12
25	10	8.150	8.621	14	5.827	7.313	12	6	7

Table A.3: Times to Create Passwords with Three Methods.

	textPassword (sec.)	gridWordX (sec.)	charPattern (sec.)
1	19.52	102.83	67.84
2	36.72	55.77	18.20
3	16.34	129.28	9.40
4	15.69	43.70	9.75
5	15.23	21.44	10.84
6	25.12	28.53	12.73
7	13.89	36.07	14.93
8	30.71	191.03	28.42
9	30.71	46.90	17.06
10	16.18	21.37	25.46
11	35.12	115.63	8.21
12	23.26	93.70	25.19
13	17.27	55.19	83.09
14	31.27	96.60	34.15
15	9.90	21.11	42.80
16	20.46	30.88	25.10
17	24.56	45.20	30.36
18	35.29	59.75	37.78
19	14.27	24.25	140.90
20	34.55	31.41	30.38
21	10.56	18.16	6.48
22	16.19	26.00	5.07
23	24.64	188.42	92.66
24	49.63	12.72	7.77
25	24.79	64.23	21.84

Table A.4: The Number of Attempts until Successful Login with All Three Methods in The Web Study(in the table, text-textPassword, grid-gridWordX, char-charPattern).

	Session 2			Session 3		
	text	grid	char	text	grid	char
1	1	1	1	1	1	1
2	1	1	1	1	1	1
3	1	2	1	1	1	1
4	1	1	2	1	1	1
5	1	1	1	1	2	1
6	2	1	1	1	1	1
7	1	1	1	1	1	1
8	2	1	1	1	1	1
9	1	1	1	1	1	1
10	1	4	1	2	1	1
11	1	1	1	1	1	1
12	1	2	1	2	1	1
13	1	1	1	1	1	1
14	1	1	1	1	1	1
15	1	1	1	2	1	2
16	1	1	1	1	1	3
17	1	2	1	1	1	4
18	1	3	1	1	1	2
19	1	1	1	1	1	1
20	1	1	3	1	2	1
21	1	1	1	1	1	1
22	1	1	2	1	1	3
23	1	1	1	2	2	1
24	1	1	1	2	3	1
25	1	1	1	1	1	1

Table A.5: Shuffle Counts in gridWordX and charPattern.

	gridWordX	charPattern
1	5	1
2	4	3
3	6	0
4	1	3
5	0	0
6	6	0
7	0	0
8	0	1
9	1	2
10	0	5
11	0	0
12	16	1
13	0	3
14	18	0
15	0	7
16	4	1
17	3	5
18	4	0
19	1	1
20	2	0
21	3	0
22	0	0
23	3	4
24	2	0
25	36	2

Table A.6: The Answers to The Questionnaire.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
1	10	10	10	10	10	10	10	10	a	no
2	10	8	10	10	10	7	4	7	c	no
3	8	9	10	10	10	9	10	0	b	no
4	8	3	10	8	9	8	10	5	b	yes
5	10	1	9	10	8	8	9	8	b	no
6	9	8	9	9	9	10	2	2	b	no
7	10	9	10	10	10	10	10	10	a	no
8	10	7	9	10	9	10	8	5	b	yes
9	8	8	9	10	10	5	2	9	c	yes
10	10	10	10	10	10	5	1	7	b	no
11	8	2	7	10	7	9	8	1	c	no
12	8	9	9	9	9	8	10	10	b	yes
13	8	9	7	10	10	5	10	10	b	no
14	8	5	6	10	7	7	10	9	b	no
15	8	7	9	10	10	7	9	8	b	yes
16	5	9	6	6	7	5	8	10	c	yes
17	10	10	10	10	9	10	10	10	c	no
18	8	3	8	10	9	7	10	3	b	yes
19	9	9	8	10	10	9	8	7	b	no
20	6	2	6	10	9	10	6	0	a	yes
21	8	5	8	5	8	9	7	5	b	no
22	10	10	10	10	10	10	10	10	b	no
23	10	2	10	10	9	9	9	9	b	no
24	5	5	7	10	10	9	10	5	b	no
25	10	9	10	10	8	5	2	8	c	no

B. STATISTICAL TESTS

B.1 The Friedman Test

Friedman Test is a non-parametric statistical test evaluating the difference between several related samples. Being alternative to Repeated measures analysis of variances, non-parametric k-related sample test Friedman is used in case of the condition that same parameter has been measured under different conditions on the same subjects. The test involves ranking the datasets (the number of samples tests) then it takes of averages of rankings on each column.

To exemplify, in this thesis, the test is applied to compare login times of text passwords, gridWordX and charPattern on the mobile device. Actually, our data is three-related sample. The login times of tree authentication methods on the mobile device and their ranking are presented in Table B.1. With p value less than 0.05, we can see from mean ranks in Table B.1, that login by charPattern on the mobile device takes shorter time than of tex passwords and gridWordX.

B.2 The Wilcoxon signed-rank Test

The Wilcoxon signed-rank test applies to two-sample designs involving repeated measures. The logic behind the Wilcoxon test is quite simple ranking the data to each of two conditions. In the test, most of the high ranks belong to one condition and most of low ranks belong to other one if there occurs a systematic condition between the two conditions. On the other hand, in case if two conditions are similar, high and low ranks are distributed fairly.

We applied the paired-sample Wilcoxon test when we compare login times of charPattern and gridWordX in the first and second sessions of the Web study (see

Table B.1: Average login times of text passwords, gridWordX and charPattern in the lab study(in the table, donated: text-taxtPassword, grid-gridWordX, char-charPattern).

	Average(sec.)			Ranking by Friedman		
	text	grid	char	text	grid	char
1	9	15	7	2	3	1
2	10	26	8	2	3	1
3	8	18	9	1	3	2
4	18	13	48	2	1	3
5	11	7	10	3	1	2
6	31	17	10	3	2	1
7	15	7	6	3	2	1
8	35	38	13	2	3	1
9	13	13	12	2	2	1
10	11	87	12	1	3	2
11	47	18	7	3	2	1
12	16	27	13	2	3	1
13	8	50	8	1	2	1
14	18	25	25	1	2	2
15	13	41	10	2	3	1
16	28	14	42	2	1	3
17	6	29	6	1	2	1
18	10	33	8	2	3	1
19	26	27	7	2	3	1
20	12	16	16	1	2	2
21	15	5	5	2	1	1
22	9	13	12	1	3	2
23	10	10	42	1	1	2
24	25	10	12	3	1	2
25	12	6	7	3	1	2
	Mean of Ranks			1.92	2.12	1.52

Table A.2) and find that charPattern has shorter login time than of gridWordX marginal significance (asymptotic significance for the first and second sessions of the Web study is p=0.045 and p=0.069, respectively).

CURRICULUM VITAE

Personal Information

Surname, Name	:	SATİEV, Tashtanbek
Citizenship	:	KYRGYZSTAN
Date and Place of Birth	:	23.07.1986 KYRGYZSTAN
Marital Status	:	Married
Telephone	:	(90) 5073735405
e-mail	:	satievtashtan@gmail.com

Education

Level	**Training Unit**	**Graduation Date**
Master Degree	TOBB Universitry of Economics and Technology	2015
Bachelor Degree	Kyrgyz National University	2009

Job Experience

Year	**Place**	**Duty**
2009-2014	TOBB University of Economics and Technology	Scholarship Student

Foreign Language

Turkish (Perfect)
Russian (Perfect

Publications

- K. Bicakci, **T. Satiev** "charPattern: Rethinking Android Lock Pattern to Adapt to Remote Authentication", *Passwords 14 International Conference on Passwords*, 8-10 December 2014, Trondheim, Norway (in Post-Proceeding Process).