COMP3008 Project 2
Quantitative Usability Evaluation

Team Name: COMP3008

Team Member:

SongJin (100955149)

XinPeng Jiang (100926864)

SiRui Zeng (100958822)

Zi Jin (100941677)

Part1:

1.1

In text21:

-Use recall to do the memory retrieval.

-Assigned Text Password (AST).

-Use less time to memorize.

-Shorter memory time compare to graphic recognition.

-Need to write down

-Random generated passwords, barely encoding information can be used by users to recall it.

In Imagept21:

-Use recognition to do the memory retrieval.

-Image Passtile(IPT)

-Not clear, sometimes not sure which one I have already clicked.

-Need more time to memorize the locations of tiles (compare to text password).

-No enough features in images that could help user memorize positions. (encoding information).

-Longer memory time compare to text password.

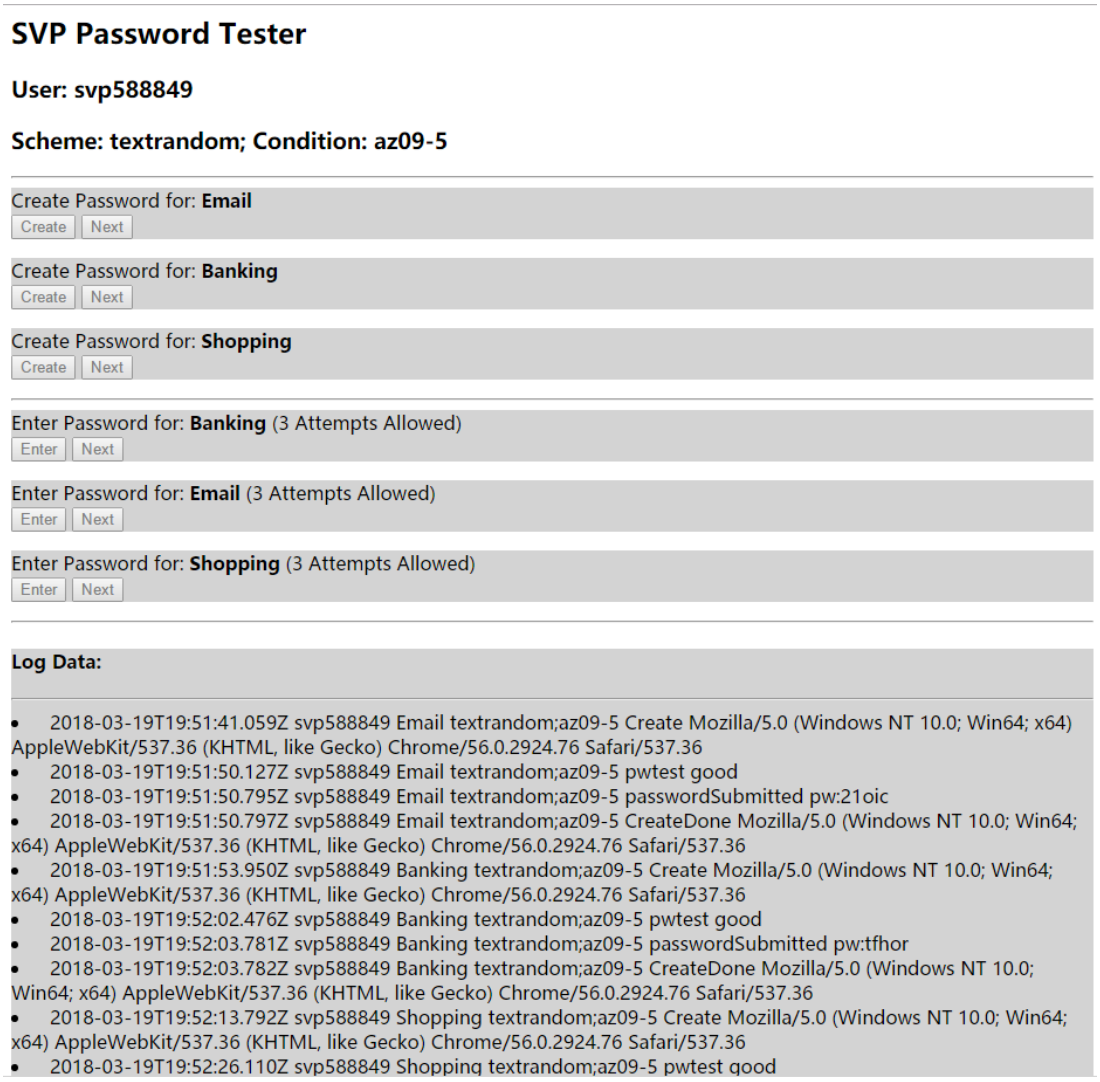
In general, text21 is assign text password, users have to recall the password, which is more complex to remember than recognition password. It is hard to memorize and easy to forget text21 password. Users need to write the password on the paper to help memorize.

Image Passtile provides an entire image to help recognize the password. Although this password scheme is superior than assigned text password, it is still different to use.

Image password is convenient to use when there are many obvious features in the image. It utilizes users' cognition rather than recalling memory. However, in Imagept21, many images do not own obvious features, which users just memorize blurred locations.

Additionally, when users enter password by clicking on tiles, they do not get any feedback about the tile location is correct or not.

TEXT21



- 2018-03-19T19:52:27.077Z svp588849 Shopping textrandom;az09-5 passwordSubmitted pw:neqo8
- 2018-03-19T19:52:27.078Z svp588849 Shopping textrandom;az09-5 CreateDone Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:52:30.753Z svp588849 Banking textrandom;az09-5 Enter Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:52:35.777Z svp588849 Banking textrandom;az09-5 EnterSuccess Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:52:38.515Z svp588849 Email textrandom;az09-5 Enter Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:52:57.993Z svp588849 Email textrandom;az09-5 EnterFailure Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:53:00.207Z svp588849 Email textrandom;az09-5 Enter Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:53:06.373Z svp588849 Email textrandom;az09-5 EnterSuccess Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:53:08.386Z svp588849 Shopping textrandom;az09-5 Enter Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:53:19.110Z svp588849 Shopping textrandom;az09-5 EnterSuccess Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36

Imagept21

SVP Password Tester

User: svp324175

Scheme: passtiles; Condition: ImagePasstiles_Poll

Create Password for: **Email**
Create Next

Create Password for: **Banking**
Create Next

Create Password for: **Shopping**
Create Next

Enter Password for: **Shopping** (3 Attempts Allowed)
Enter Next

Enter Password for: **Banking** (3 Attempts Allowed)
Enter Next

Enter Password for: **Email** (3 Attempts Allowed)
Enter Next

Log Data:

- 2018-03-19T19:56:01.478Z svp324175 Email passtiles;ImagePasstiles_Poll Create Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:56:01.665Z svp324175 Email passtiles;ImagePasstiles_Poll PassTilesStart Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:56:01.671Z svp324175 Email passtiles;ImagePasstiles_Poll picChange boats_s.jpg
- 2018-03-19T19:56:01.749Z svp324175 Email passtiles;ImagePasstiles_Poll picAccept boats_s.jpg
- 2018-03-19T19:56:01.787Z svp324175 Email passtiles;ImagePasstiles_Poll Password XXXX
- 2018-03-19T19:56:10.910Z svp324175 Email passtiles;ImagePasstiles_Poll order inputPwd XXXX
- 2018-03-19T19:56:10.912Z svp324175 Email passtiles;ImagePasstiles_Poll goodPractice E3F2F5H1H3:XXXX
- 2018-03-19T19:56:33.392Z svp324175 Email passtiles;ImagePasstiles_Poll Create Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:56:33.665Z svp324175 Email passtiles;ImagePasstiles_Poll PassTilesStart Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:56:33.671Z svp324175 Email passtiles;ImagePasstiles_Poll picChange psychadelic.jpg

- 2018-03-19T19:56:33.728Z svp324175 Email passtiles;ImagePasstiles_Poll picAccept psychadelic.jpg
- 2018-03-19T19:56:33.760Z svp324175 Email passtiles;ImagePasstiles_Poll Password XXXX
- 2018-03-19T19:56:46.115Z svp324175 Email passtiles;ImagePasstiles_Poll order inputPwd XXXX
- 2018-03-19T19:56:46.117Z svp324175 Email passtiles;ImagePasstiles_Poll goodPractice A2B6D4E4G3:XXXX
- 2018-03-19T19:56:50.474Z svp324175 Email passtiles;ImagePasstiles_Poll setPasswordData psychadelic.jpg:XXXX
- 2018-03-19T19:56:50.475Z svp324175 Email passtiles;ImagePasstiles_Poll PwdDisplay Begin
- 2018-03-19T19:56:50.476Z svp324175 Email passtiles;ImagePasstiles_Poll PwdDisplay XXXX
- 2018-03-19T19:56:50.477Z svp324175 Email passtiles;ImagePasstiles_Poll Password XXXX
- 2018-03-19T19:56:50.481Z svp324175 Email passtiles;ImagePasstiles_Poll CreateDone Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:56:52.328Z svp324175 Banking passtiles;ImagePasstiles_Poll Create Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:56:52.476Z svp324175 Banking passtiles;ImagePasstiles_Poll PassTilesStart Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:56:52.483Z svp324175 Banking passtiles;ImagePasstiles_Poll picChange museepicasso.jpg
- 2018-03-19T19:56:52.554Z svp324175 Banking passtiles;ImagePasstiles_Poll picAccept museepicasso.jpg
- 2018-03-19T19:56:52.590Z svp324175 Banking passtiles;ImagePasstiles_Poll Password XXXX
- 2018-03-19T19:56:59.057Z svp324175 Banking passtiles;ImagePasstiles_Poll order inputPwd XXXX
- 2018-03-19T19:56:59.059Z svp324175 Banking passtiles;ImagePasstiles_Poll goodPractice C3D6E2E6F6:XXXX
- 2018-03-19T19:57:10.015Z svp324175 Banking passtiles;ImagePasstiles_Poll Create Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:57:10.140Z svp324175 Banking passtiles;ImagePasstiles_Poll PassTilesStart Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:57:10.144Z svp324175 Banking passtiles;ImagePasstiles_Poll picChange lilipad_flower_pd.jpg
- 2018-03-19T19:57:10.205Z svp324175 Banking passtiles;ImagePasstiles_Poll picAccept lilipad_flower_pd.jpg
- 2018-03-19T19:57:10.240Z svp324175 Banking passtiles;ImagePasstiles_Poll Password XXXX
- 2018-03-19T19:57:16.241Z svp324175 Banking passtiles;ImagePasstiles_Poll order inputPwd XXXX
- 2018-03-19T19:57:16.243Z svp324175 Banking passtiles;ImagePasstiles_Poll goodPractice D3E2F4G3G4:XXXX
- 2018-03-19T19:57:22.155Z svp324175 Banking passtiles;ImagePasstiles_Poll setPasswordData lilipad_flower_pd.jpg:XXXX

- 2018-03-19T19:57:22.157Z svp324175 Banking passtiles;ImagePasstiles_Poll PwdDisplay Begin
- 2018-03-19T19:57:22.158Z svp324175 Banking passtiles;ImagePasstiles_Poll PwdDisplay XXXX
- 2018-03-19T19:57:22.159Z svp324175 Banking passtiles;ImagePasstiles_Poll Password XXXX
- 2018-03-19T19:57:22.163Z svp324175 Banking passtiles;ImagePasstiles_Poll CreateDone Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:57:24.267Z svp324175 Shopping passtiles;ImagePasstiles_Poll Create Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:57:24.407Z svp324175 Shopping passtiles;ImagePasstiles_Poll PassTilesStart Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:57:24.414Z svp324175 Shopping passtiles;ImagePasstiles_Poll picChange zebracrossing.jpg
- 2018-03-19T19:57:24.488Z svp324175 Shopping passtiles;ImagePasstiles_Poll picAccept zebracrossing.jpg
- 2018-03-19T19:57:24.521Z svp324175 Shopping passtiles;ImagePasstiles_Poll Password XXXX
- 2018-03-19T19:57:32.456Z svp324175 Shopping passtiles;ImagePasstiles_Poll Create Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:57:32.623Z svp324175 Shopping passtiles;ImagePasstiles_Poll PassTilesStart Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:57:32.629Z svp324175 Shopping passtiles;ImagePasstiles_Poll picChange veggies.jpg
- 2018-03-19T19:57:32.691Z svp324175 Shopping passtiles;ImagePasstiles_Poll picAccept veggies.jpg
- 2018-03-19T19:57:32.723Z svp324175 Shopping passtiles;ImagePasstiles_Poll Password XXXX
- 2018-03-19T19:57:38.032Z svp324175 Shopping passtiles;ImagePasstiles_Poll order inputPwd XXXX
- 2018-03-19T19:57:38.034Z svp324175 Shopping passtiles;ImagePasstiles_Poll goodPractice B1C2D2F5G2:XXXX
- 2018-03-19T19:57:40.890Z svp324175 Shopping passtiles;ImagePasstiles_Poll setPasswordData veggies.jpg:XXXX
- 2018-03-19T19:57:40.891Z svp324175 Shopping passtiles;ImagePasstiles_Poll PwdDisplay Begin
- 2018-03-19T19:57:40.892Z svp324175 Shopping passtiles;ImagePasstiles_Poll PwdDisplay XXXX
- 2018-03-19T19:57:40.893Z svp324175 Shopping passtiles;ImagePasstiles_Poll Password XXXX
- 2018-03-19T19:57:40.896Z svp324175 Shopping passtiles;ImagePasstiles_Poll CreateDone Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:57:43.024Z svp324175 Shopping passtiles;ImagePasstiles_Poll Enter Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:57:43.168Z svp324175 Shopping passtiles;ImagePasstiles_Poll PassTilesStart Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:57:55.874Z svp324175 Shopping passtiles;ImagePasstiles_Poll order inputPwd XXXX
- 2018-03-19T19:57:55.876Z svp324175 Shopping passtiles;ImagePasstiles_Poll badLogin XXXX:XXXX
- 2018-03-19T19:57:57.482Z svp324175 Shopping passtiles;ImagePasstiles_Poll EnterFailure Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:57:58.955Z svp324175 Shopping passtiles;ImagePasstiles_Poll Enter Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:57:59.090Z svp324175 Shopping passtiles;ImagePasstiles_Poll PassTilesStart Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36

- 2018-03-19T19:58:06.552Z svp324175 Shopping passtiles;ImagePasstiles_Poll order inputPwd XXXX
- 2018-03-19T19:58:06.554Z svp324175 Shopping passtiles;ImagePasstiles_Poll badLogin XXXX:XXXX
- 2018-03-19T19:58:07.550Z svp324175 Shopping passtiles;ImagePasstiles_Poll EnterSuccess Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:58:09.461Z svp324175 Banking passtiles;ImagePasstiles_Poll Enter Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:58:09.596Z svp324175 Banking passtiles;ImagePasstiles_Poll PassTilesStart Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:58:25.823Z svp324175 Banking passtiles;ImagePasstiles_Poll order inputPwd XXXX
- 2018-03-19T19:58:25.825Z svp324175 Banking passtiles;ImagePasstiles_Poll badLogin XXXX:XXXX
- 2018-03-19T19:58:26.907Z svp324175 Banking passtiles;ImagePasstiles_Poll EnterSuccess Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:58:29.538Z svp324175 Email passtiles;ImagePasstiles_Poll Enter Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:58:29.675Z svp324175 Email passtiles;ImagePasstiles_Poll PassTilesStart Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:58:42.446Z svp324175 Email passtiles;ImagePasstiles_Poll order inputPwd XXXX
- 2018-03-19T19:58:42.448Z svp324175 Email passtiles;ImagePasstiles_Poll badLogin XXXX:XXXX
- 2018-03-19T19:58:43.467Z svp324175 Email passtiles;ImagePasstiles_Poll EnterFailure Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:58:44.405Z svp324175 Email passtiles;ImagePasstiles_Poll Enter Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:58:44.546Z svp324175 Email passtiles;ImagePasstiles_Poll PassTilesStart Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36
- 2018-03-19T19:58:53.769Z svp324175 Email passtiles;ImagePasstiles_Poll order inputPwd XXXX
- 2018-03-19T19:58:53.771Z svp324175 Email passtiles;ImagePasstiles_Poll badLogin XXXX:XXXX
- 2018-03-19T19:58:54.629Z svp324175 Email passtiles;ImagePasstiles_Poll EnterSuccess Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36

1.2

In this part of the project, we developed a program the uses three loops to go through a dataset and extract useful data for father use. The first loop loops through all different UID and ensures the current UID. The second loop loops through current UID and gets the Total number of login, number of successful logins and number of unsuccessful logins. The third loop loops through the current UID and output a data set with information on current UID, Total number of login, number of successful logins and number of unsuccessful logins, the password scheme of current login, if the current login successful or not, and the time took on current login.

Pseudocode:

While not all user ids are processed{

Get current UID

while still at current UID{

If the action is login and the result is fail

add to fail count and total count

if the action is login and the result success

add to success count and total count

}

while in the same UID{

every time there is a login

get the password scheme

get if fail or success

get time

output current data with UID Total count, Total successful, Total unsuccessful, password scheme, fail or success and time

}

Go to next UID

}

Source code:

```
library(data.table)

#get data
dt = data.table(image21.)
dt[1620,V2]
nrow(dt)
```

```
#initial helpers and counters
lastf<-data.frame()
Totalfail<-0
Totalsuccess<-0

i<-2
o<-2
q<-1



#see the number of unique userid
adt<-unique(dt$V2)
length(adt)



#while there are more unprocessed id
while (q <= length(adt)){
  #set current uid

  uid<-dt[i,V2]
  Totalfail<-0
  Totalsuccess<-0
  Totallogin <-0

  #while it is still the current uid

  while (dt[i,V2] == dt[i-1,V2]){
    #if the action is login and the result is fail add to fail count and total count
```

```
  if(dt[i,V7]=="failure"&& dt[i,V6]=="login")
  {

    Totalfail = Totalfail + 1
    Totallogin = Totallogin +1
  }
  #if the action is login  and the result success add to fail count and total success count
  if(dt[i,V7]=="success"&& dt[i,V6]=="login")
  {
    Totalsuccess = Totalsuccess + 1
    Totallogin = Totallogin +1
  }

  i=i+1
  if(i>nrow(dt)){break}
}

#while in the same password scheme
while (dt[o,V2] == dt[o-1,V2]){
#every time there is a login
if(dt[o,V6]=="login"){

#get the password scheme
Passwordscheme <- dt[o,V4]

#get if fail or success
SorF<-dt[o,V7]
```

```
  j<-o

  #get time by subtract the time on the nearest start statement
  while(dt[j,V7] != "start"){ j=j-1;}
  time<- as.numeric(as.POSIXct(dt[o,V1])-as.POSIXct(dt[j,V1]))



  #set and merge the data
  newf<-data.frame(uid,Passwordscheme,Totallogin,Totalsuccess,Totalfail,SorF,time)
  thenewf<- rbind(lastf, newf)

  lastf<-thenewf
  }

  o=o+1
  if(o>nrow(dt)){break}
  }
 i=i+1
 q=q+1
 o=o+1
}
```

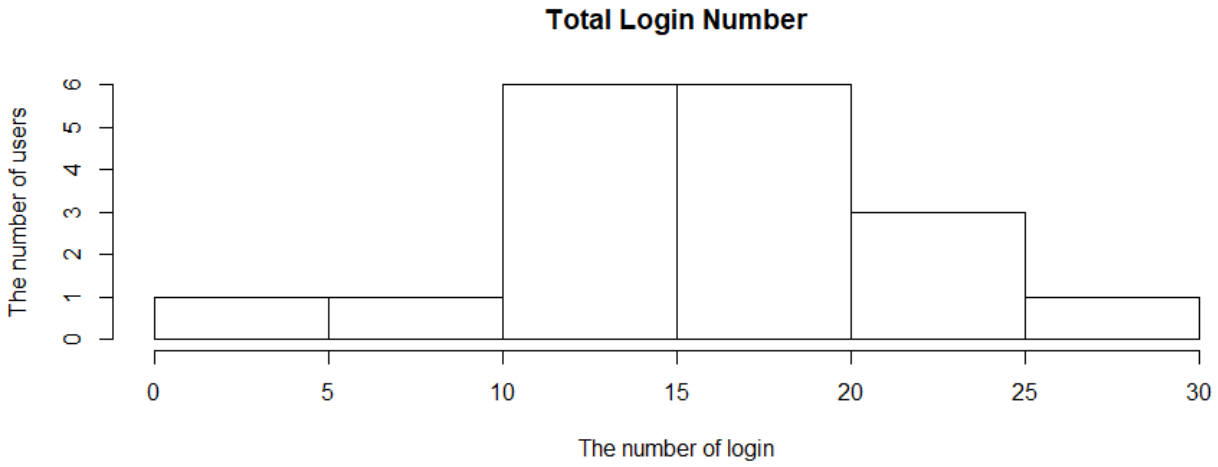
1.3

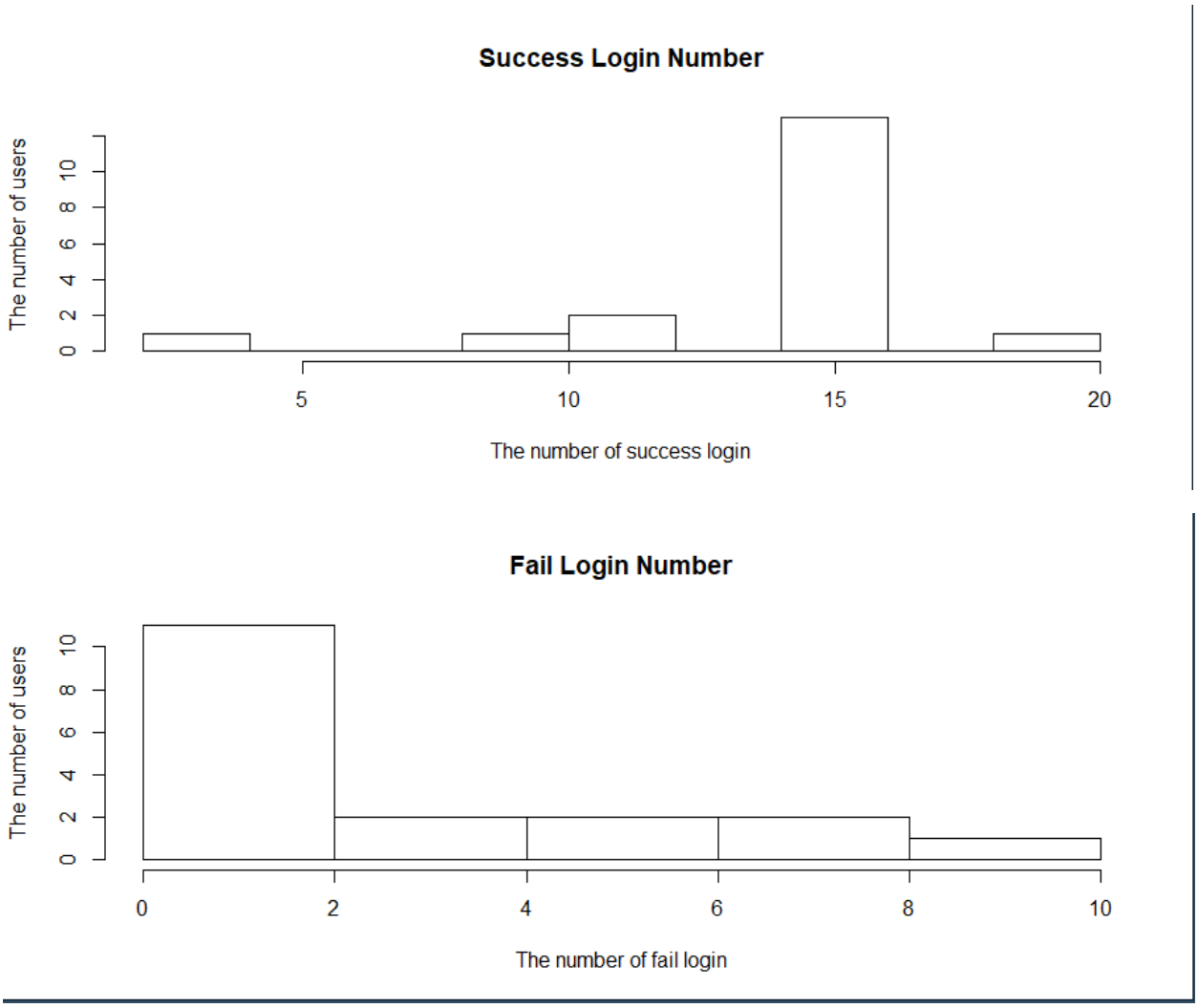
Text21:

Descriptive statistics:

Text21 Descriptive Statistics			
	Mean	**SD**	**Median**
Total-Login	16.61	4.9	16
Total-Success	14.05	3.438	15
Total-Fail	2.56	3.329	1
Success-Time	1.89	1.844	1.5
Fail-Time	0.44	0.922	0

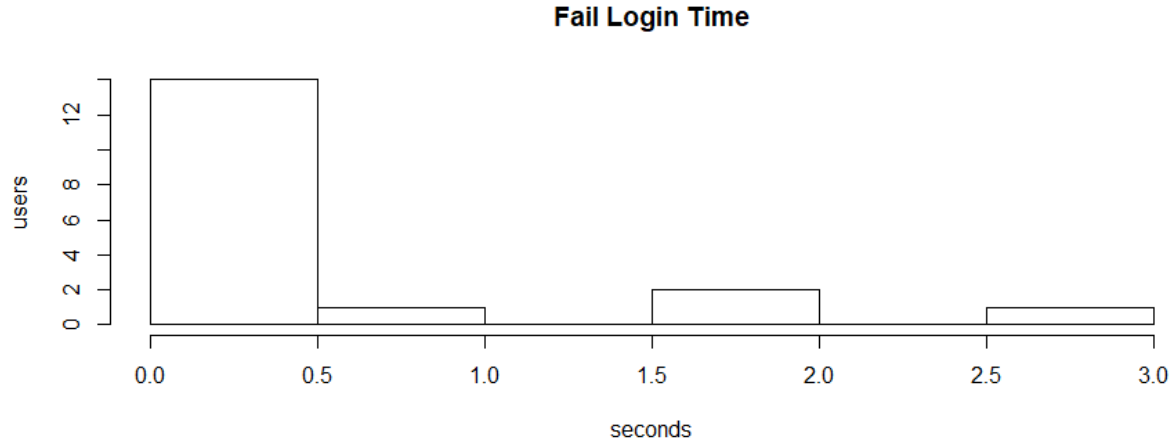
Histograms for the number of logins (per user, total, successful, and unsuccessful):

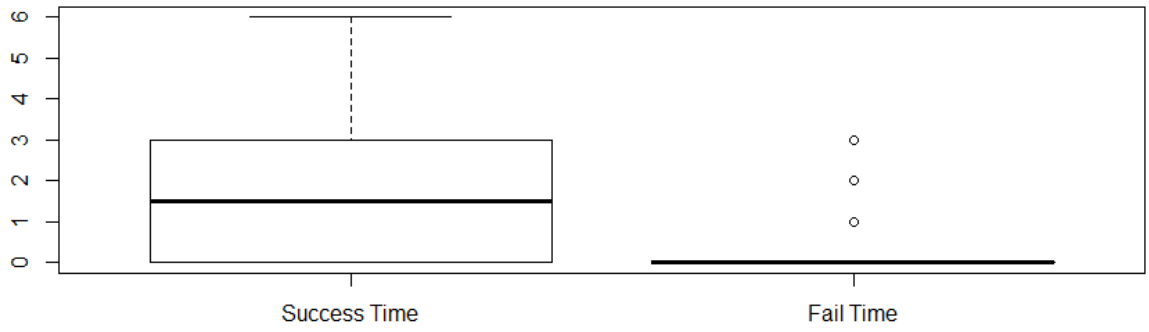



Success Login Number
The number of users
0
2
4
6
8
10
5
10
15
20
The number of success login

Fail Login Number
The number of users
0
2
4
6
8
10
0
2
4
6
8
10
The number of fail login

Histograms and boxplots for the login time per user, successful, and unsuccessful:





Interpretation:

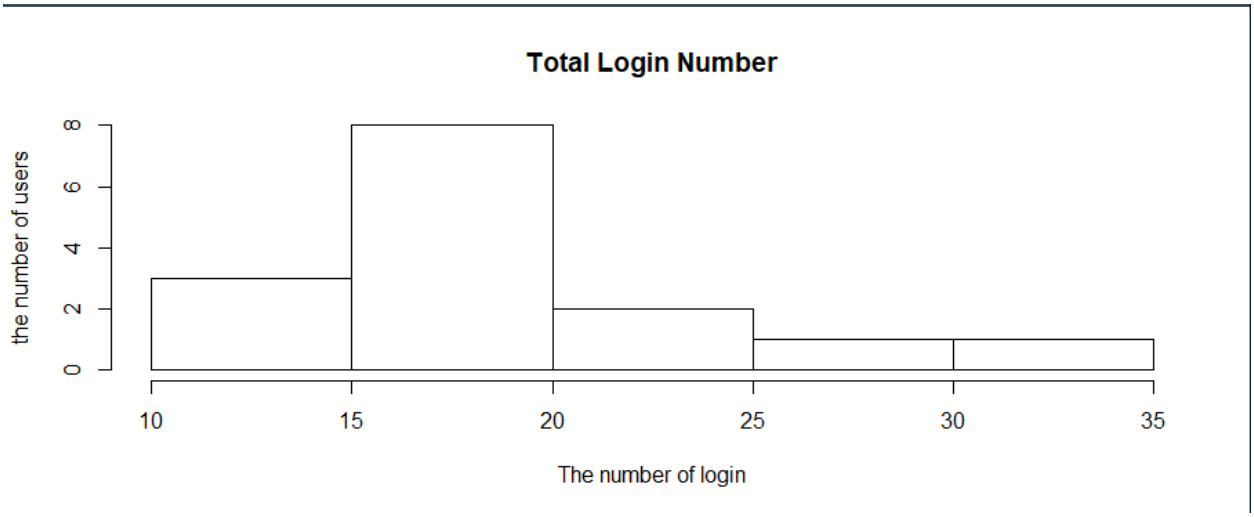
Descriptive statistics table shows the statistic data for the number of login (per user, total, successful and unsuccessful) and login time (successful and unsuccessful). In mean data: users login about 16 times (about 14 times success and around 2 times fail). The high successful login rate indicates the Text21 password is reliable. Average successful login time is 1.89s, which also means users can recall the password in short time. From histogram, we can find the similar result. The grams show, apparently, the password is reliable to login.

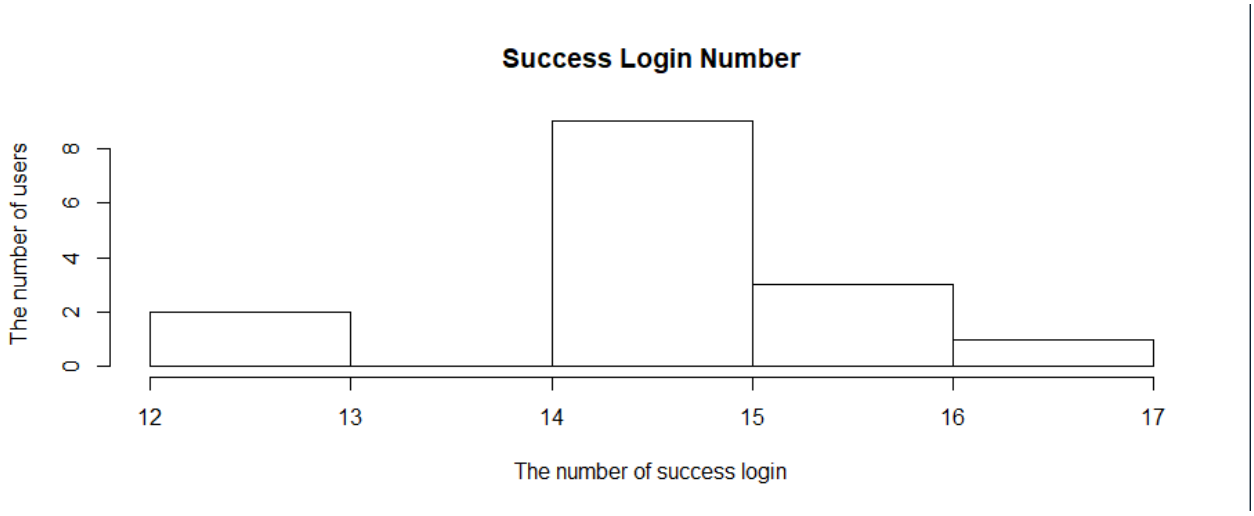
Imagept21:

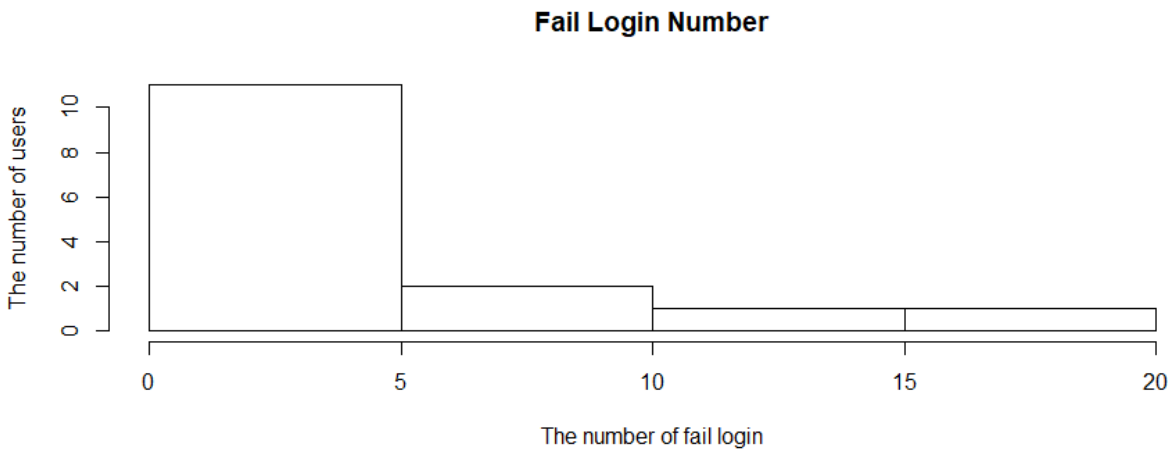
Descriptive statistics:

Imagept21 Descriptive Statistics			
	Mean	SD	Median
Total-Login	19.4	5.235	18
Total-Success	14.93	1.335	15
Total-Fail	4.47	4.438	3
Success-Time	4.07	2.154	4
Fail-Time	1.27	1.831	1

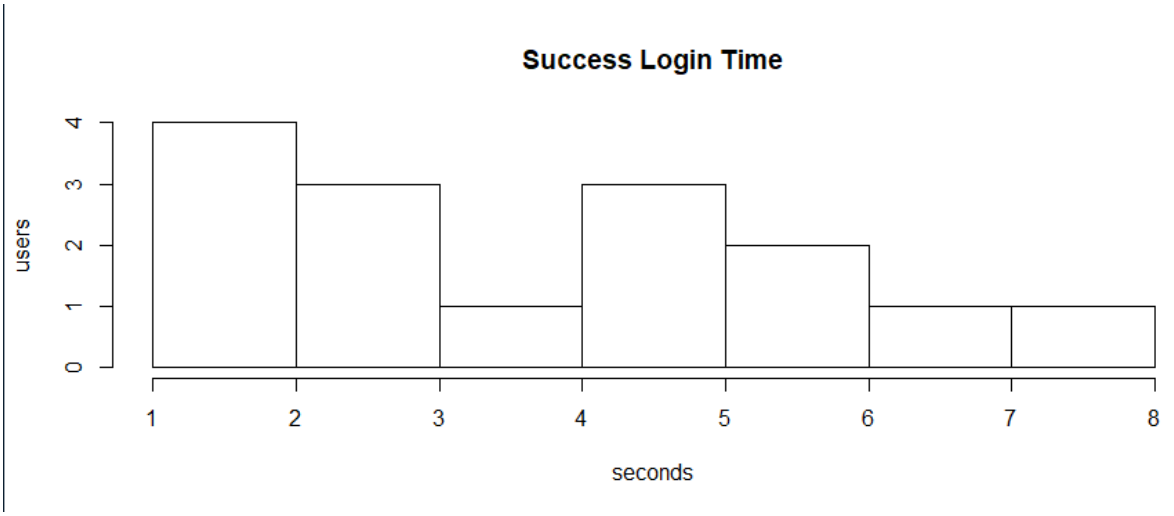
Histograms for the number of logins (per user, total, successful, and unsuccessful):

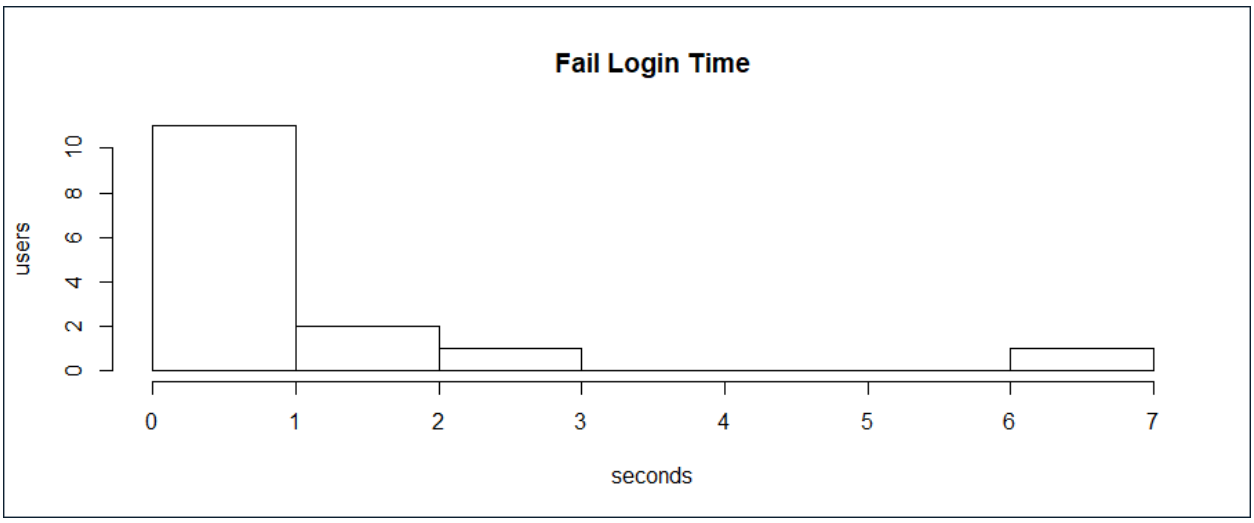


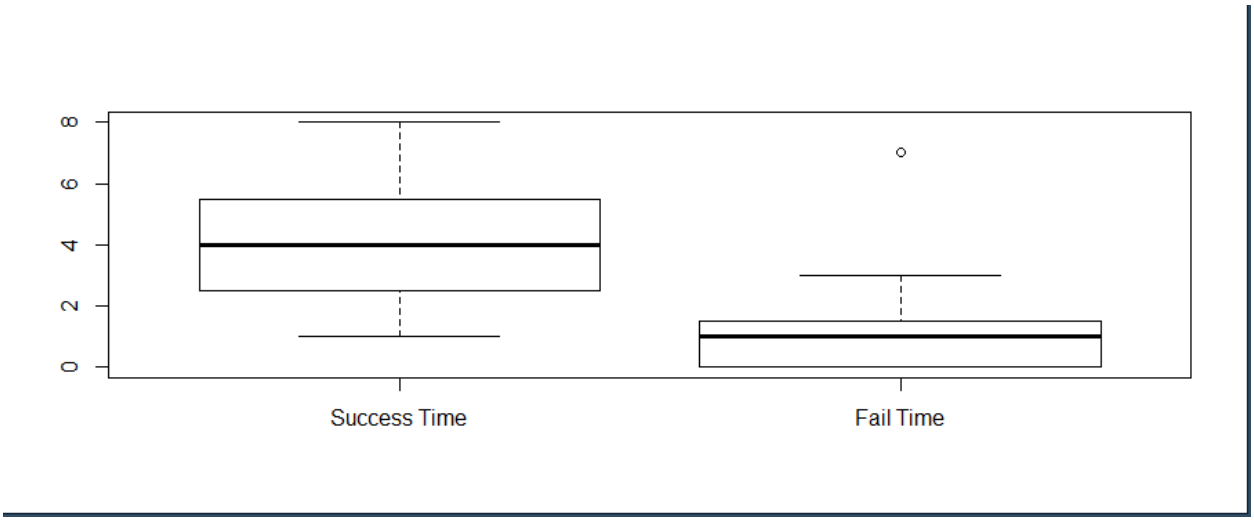




Histograms and boxplots for the login time per user, successful, and unsuccessful:







Interpretation:

From the descriptive statistic table, we can find the average number of login is around 19 times. About 15 times are successful. The successful rate is approx. 77%. That's a nice performance. While, the successful login time is about 4 seconds. It means users need to spend more time on recalling the password. The Imagept21 password scheme, is not efficient as Text21. From the histograms and boxplot diagram we also can get similar result.

Discussion:

The goal of this study is to compare usability and memorability of Text21 and Imagept21 this two kinds of password schemes. The statistic data shows that users are able to remember Text21 password better than Imagept21 password.

First of all, from the average number of successful login times, in two descriptive statistic tables, we find users login successfully 14.05 times(Text21) and 14.93 times(Imagept21). The two elements are not significantly different. However, user login with Text21 password 16.61 times averagely, which is less than login with Imagept21 password 19.4. The successful login rate of Text21 is higher than the rate of Imagept21. The comparison shows Text21 owns better usability. The result is more obvious through comparison of median total the number of successful login times and total login times. Secondly, based on average successful login time, Text21 password is 1.89 seconds and Imagept21 password is 4.07 seconds, Text21 is easily recalled by users. Text21 also owns better memorability to users. We also can find really different from median data of successful login time (Text21 is 1.5 seconds and Imagept21 is 4 seconds). Next, Imagept21 is OPT, Text21 is AST. From the histograms of successful login time we find there is significant differences in login times between the two passwords conditions. A majority part of users used less one second to login with Text21 password. While, with Imagept21 password, we can realize users spend more time on login. Histograms of the distributions of successful login time for every of the two conditions suggested that the distributions are approximately normal.

Overall, the Text21 owns better usability and memorability through comparison of average number of successful login times and costing time to successful login. With current condition, we cannot obtain disadvantage of Text21. Probably, we can get different result in more various comparison.

Part2:
2.1

Four password systems we have discussed：

5 characters password:

-First 3 positions: a-z (26 possibilities).

-Last 2 positions: 0-9 (10 possibilities).

-Password space: 26 * 26 * 26 * 10 * 10 = 1,757,600.

-Advantages: all lowercase, easy to remember compare to mix with lowercase & uppercase.

-Disadvantages: password space is not complex enough.

4 characters password:

-A-Z, a-z, {!, @,#,$,%,^,&,*,(,)} (62 possibilities).

-0-9 (10 possibilities).

-Password space: 62 * 62 *62*10 = 2,383,280.

-Advantages: Smaller password space, short length makes it easy to remember.

-Disadvantages: symbols probably make users confused.

Choose 6 images for users as their pass images.

-Choose 4 images (out of 6) in 48 (6 * 8) images.

-Pass, password space is not a constant.

1024 words (This is our new password scheme in this project)

-Random 2 words combine with a ‘2’ or ‘4’

-Password space: 1024 * 1024 * 2 = 2,097,152. (Perfect)

-Advantages: Easy to remember (for users who is good at English).

-Disadvantages:

1, The new password scheme is not friendly to non-native speakers of English.

2, Users have to spend more time on entering the password.

Explain our new password scheme：

The name of our new password scheme is 2WordsPassword. As above mentioned, our team has talked about designing a new password system. Initially, after brainstorming, we figure out 4 ways to generate passwords. Finally, 2WordsPassword won the competition, which consist of 2 random English words(noun) and 1. We created a English words libaray which includes 1,024 words(noun), which come from random word generator website. Every time, this system generates a new password, which randomly combines 2 words from database randomly and a number ‘2’ or ‘4’.

Such as: “dog2cat”, “room4city”, “key2door”.

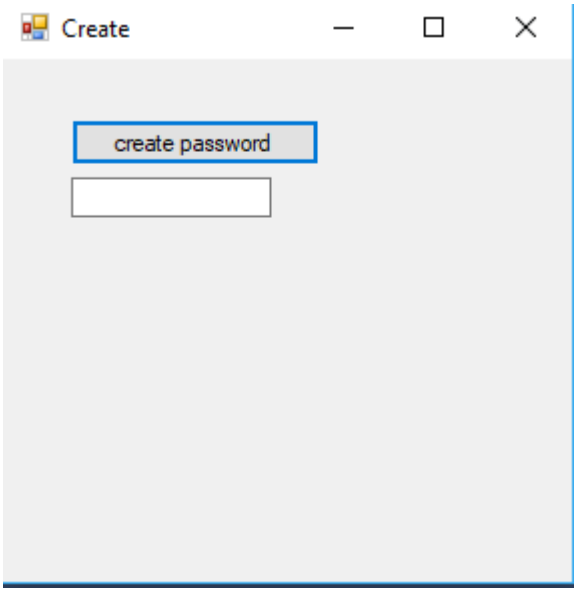
How we think it might have good usability:

In this system, our idea is to make a simple “password sentence”, that’s why we use ‘2’ or ‘4’ to combine two English words. Number ‘2’ and ‘4’ sound like ‘to’ and ‘, which make the password readable. For example ‘room4city’ can be read as ‘room for city’. Although the sentence means nothing, it could help users to memorize by developing cognition.

Calculate password space:

The password space in this system is 1,024 * 2 * 1,024 = 2,097,152 (21 bits)

2.2



This is the password creation window

…

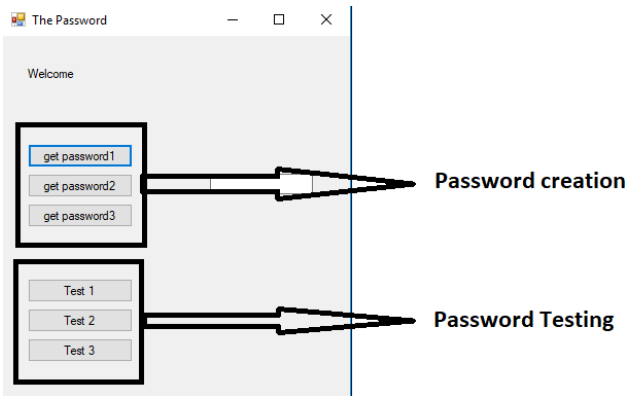
This is the part of the code that relates to password creation

```
  //get words from data base
      string[] getwords(string filename)
      {

          var fullPath =
System.IO.Path.GetDirectoryName(System.Reflection.Assembly.GetExecutingAssembly().Location);
          var fullFileName = System.IO.Path.Combine(fullPath, filename);

          string[] words = System.IO.File.ReadAllLines(fullFileName);



          //MessageBox.Show(words[5]);

          return words;
      }

      //gentrate password
      string getpassword(string[] x, string[] y)
      {
          string password;
```

```
        //random number genrator
        Random rnd = new Random();

        // random index = random word
        int rand1 = rnd.Next(1, 1025);
        int rand2 = rnd.Next(1, 1025);

        // random between 1 and 2 , if 2 the middle number is 2 else, the middle number is 4
        int rand3 = rnd.Next(1, 3);
        // MessageBox.Show(rand3.ToString());
        string number;
        if (rand3 == 2)
            number = "2";
        else
            number = "4";

        password = x[rand1] + number + y[rand2];
        // MessageBox.Show(password);
        return password;
    }
```

2.3

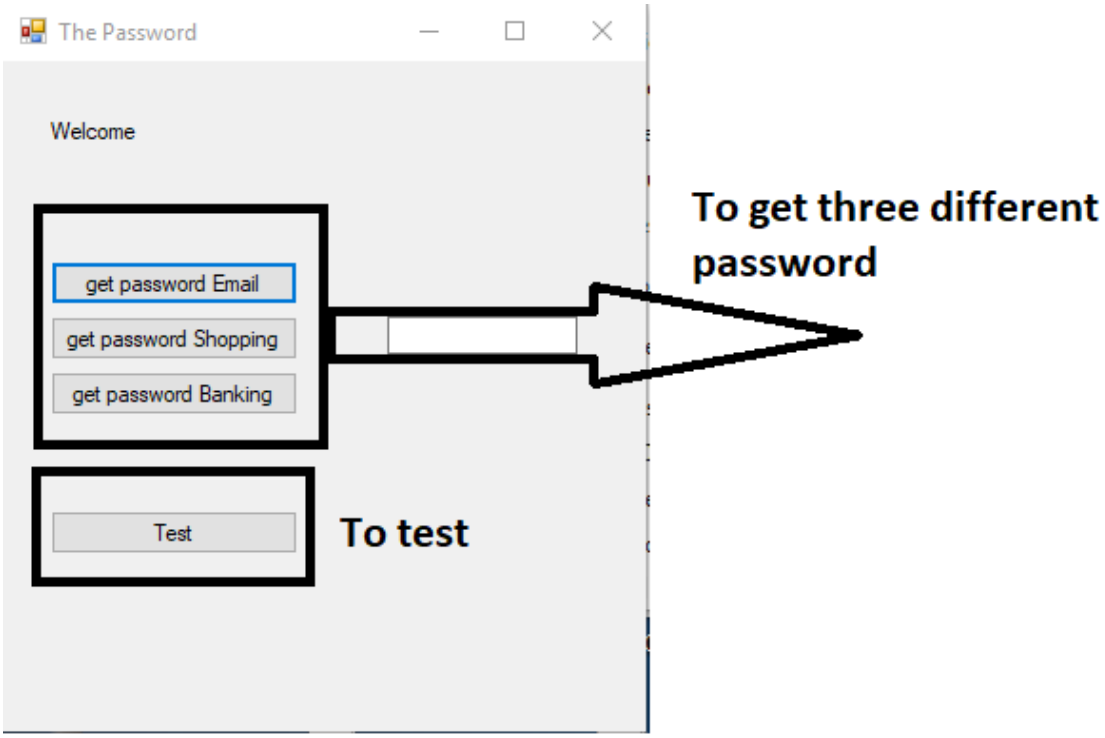
Version used on data gathering

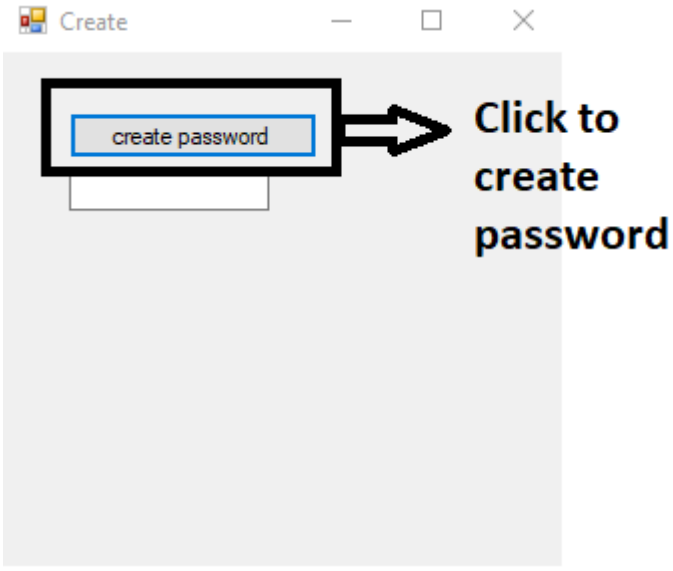


This is the welcome screen of the program The Get password button allows the user to create password

The Test button allows the user to test password

Definitive version

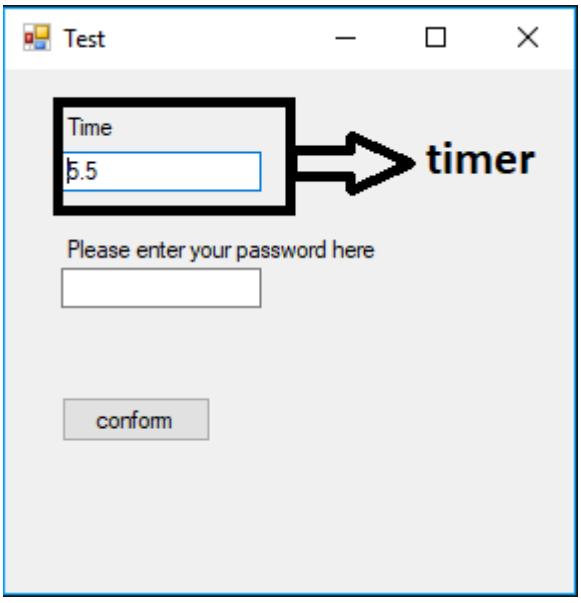




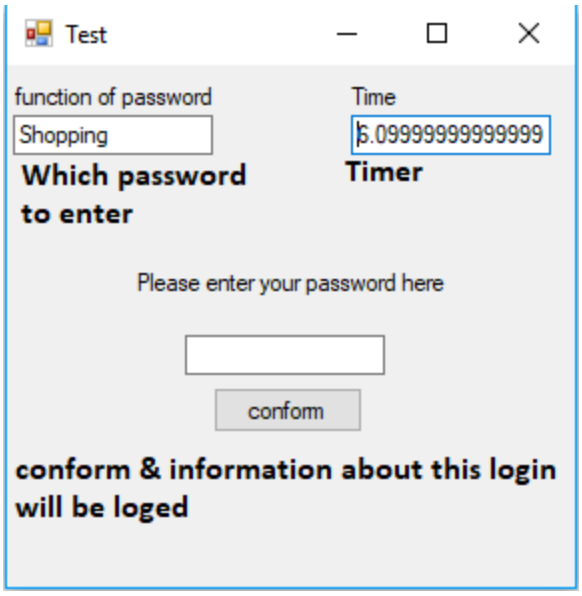
This is the password creation screen of the program

Once the Create password is clicked, the password will show on the box below

Version used on data gathering



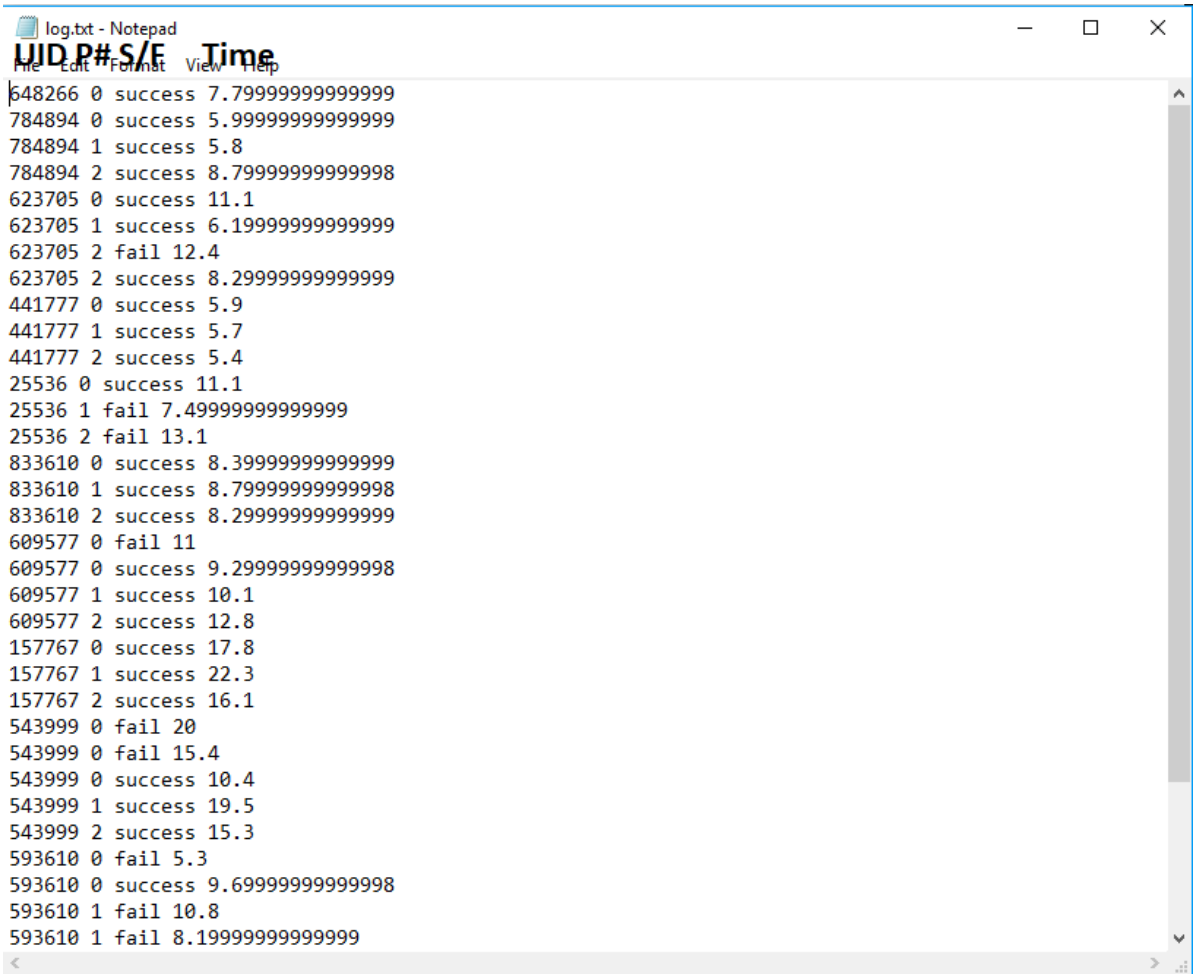
Final Version



This is the password testing screen of the program

The timer will start once the user enters this testing screen

After a password is entered and the conform button is clicked. First a success or failure message log will appear and then the require data including time, successful/failure, will be save into the log file.



Above is the log data from each password entry.

From left to right, the data is categorized in UID P# S/E Time.

```
125269 0 success 17.8351631 Shopping suc
482852 Banking fail 1.7
482852 Banking fail 1.6
482852 Shopping fail 1.7
343962 Banking fail 23.2000000000001
```

New log, replaced 0,1,2 with Email, Shopping and Banking.

2.4

Questionnaire:

After using the new password scheme, please read the following carefully and make your choices.

'1' : Strongly disagree

'2' : Disagree

'3' : OK

'4' : Agree

'5' : Strongly agree

Section A: **Our password scheme compare to normal user-chosen text passwords.**

A1. **It was easy to remember the passwords provided to me.**

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A2. **It took me a long time to enter my password using this password scheme.**

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A3. The two English words in password scheme are easy to remember.

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A4. I would use this password scheme to log into my social media accounts.

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A5. I thought the password scheme was easy to use.

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A6. I used some memory techniques to help me remember my new passwords.

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A7. It was difficult to remember the passwords provided to me.

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A8. I trust this password scheme to protect my accounts.

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A9. Using common words in password scheme is necessary in this new system.

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

A10. I would like to use this system rather than normal user-chosen text passwords.

1 ☐
2 ☐
3 ☐
4 ☐
5 ☐

You have reached the end of survey, thank you!

Link:

https://hotsoft.carleton.ca/comp3008limesurvey/index.php/333397?lang=en

account: comp3008t22

password: comp3008

2.5

Carleton UNIVERSITY
Canada's Capital University

Carleton University, School of Computer Science
COMP3008: Human-Computer Interaction, Winter, 2018

Interaction Design Project User Consent Form

Instructor: Prof. Robert Biddle
Office: HP5169, Tel. Ext. 6317, Email: robert.biddle@carleton.ca

COMP3008 Student Names:

Sirui Zeng Zi Jin Xiaopeng Jiang Song Jin

Note: This project was reviewed by the Carleton University Research Ethics Board (CUREB-B), which provided clearance to carry out the research: (Clearance #105985).

If you have any ethical concerns with the study, please contact Dr. Andy Adler, Chair, Carleton University Research Ethics Board-B (by phone at 613-520-2600 ext. 4085 or via email at ethics@carleton.ca

Study Purpose: This project is to enable students in COMP3008 to experience working with potential users to better understand testing of software using quantitative measures and analysis. Working with potential users is considered best practice in the design of interactive computer systems, and is identified in international standards such as ISO 9241-210:2010 — Human-centred design for interactive systems. Part of the process is first obtaining informed consent from prospective participants, and that is the reason for this form.

Study Procedure: In the project, the proposed system is a kind of password system, where users will be asked to use the system, remember some random passwords, and then try to use them to simulate login to a system. At no time will you be asked for any of your real passwords on any real systems. You will also be asked to fill out a questionnaire about your perceptions of the software and related issues.

Risks, Benefits, Compensation: We are not aware of any risks associated with this study. The benefits are that COMP3008 students gain experience in this aspect of Human Computer Interaction Design, and that you may gain some insight about the processes involved. There will be no financial compensation for your participation in the study.

Consent and Withdrawal: We require your consent before you can participate in the student, which you may indicate by signing your initials in the space provided below. You may choose to withdraw from the study at any time and without explanation, in which case any collected data will be discarded.

Anonymity and Confidentiality: The study involves gaining better general understanding of how students plan their degree programs, but does not involve asking you any specific personal information, nor any specific details of your degree or courses. We do not record or even ask your full name. We will not record or divulge any personal information about you.

By signing with your initials below, you consent to participate in the study.

Initials: Date:

	Agreement	Initials	Date
623705	I consent to particpate.	XF	2017- - 04/03
	I consent to particpate.	ZH	2017- - 03. Apr.
	I consent to particpate.	QM	2017- - 03. Apr
	I consent to particpate.	WY	2017- - 04/03
784594	I consent to particpate.	TG	2017- - 04/03
	I consent to particpate.	RZ	2017- - 4.3
441777	I consent to particpate.	CM	2017- - 4.3
25536	I consent to particpate.	RY	2017- - 4.3
833616	I consent to particpate.	DN	2017- - 4/3
604577	I consent to particpate.	M	2017- - 4/3
157767	I consent to particpate.	T.C.	2017- - 4.3
☆ 583994	I consent to particpate.		2017- - 4.3
593610	I consent to particpate.	YH	2017- - 4.3
	I consent to particpate.	E.W.	2017- - 4.3
	I consent to particpate.		2017- -
	I consent to particpate.		2017- -
	I consent to particpate.		2017- -
	I consent to particpate.		2017- -
	I consent to particpate.		2017- -
	I consent to particpate.		2017- -
	I consent to particpate.		2017- -
	I consent to particpate.		2017- -
	I consent to particpate.		2017- -
	I consent to particpate.		2017- -

2.6

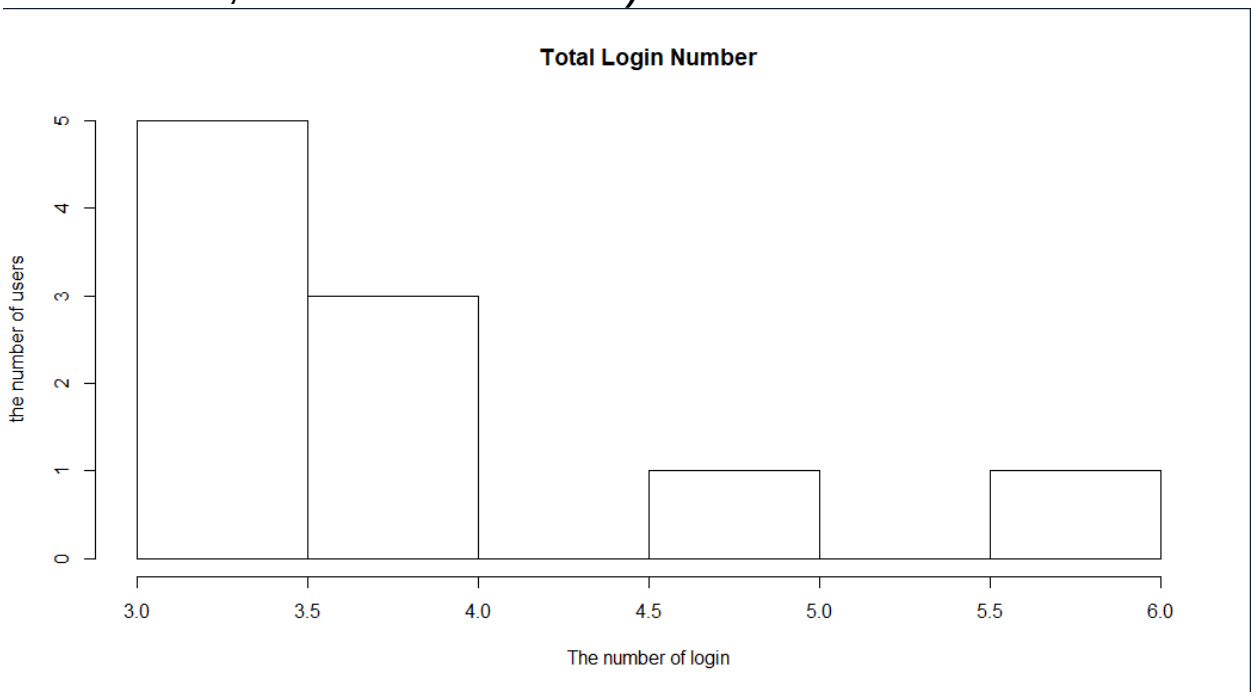
2.6.1The name of new password scheme is

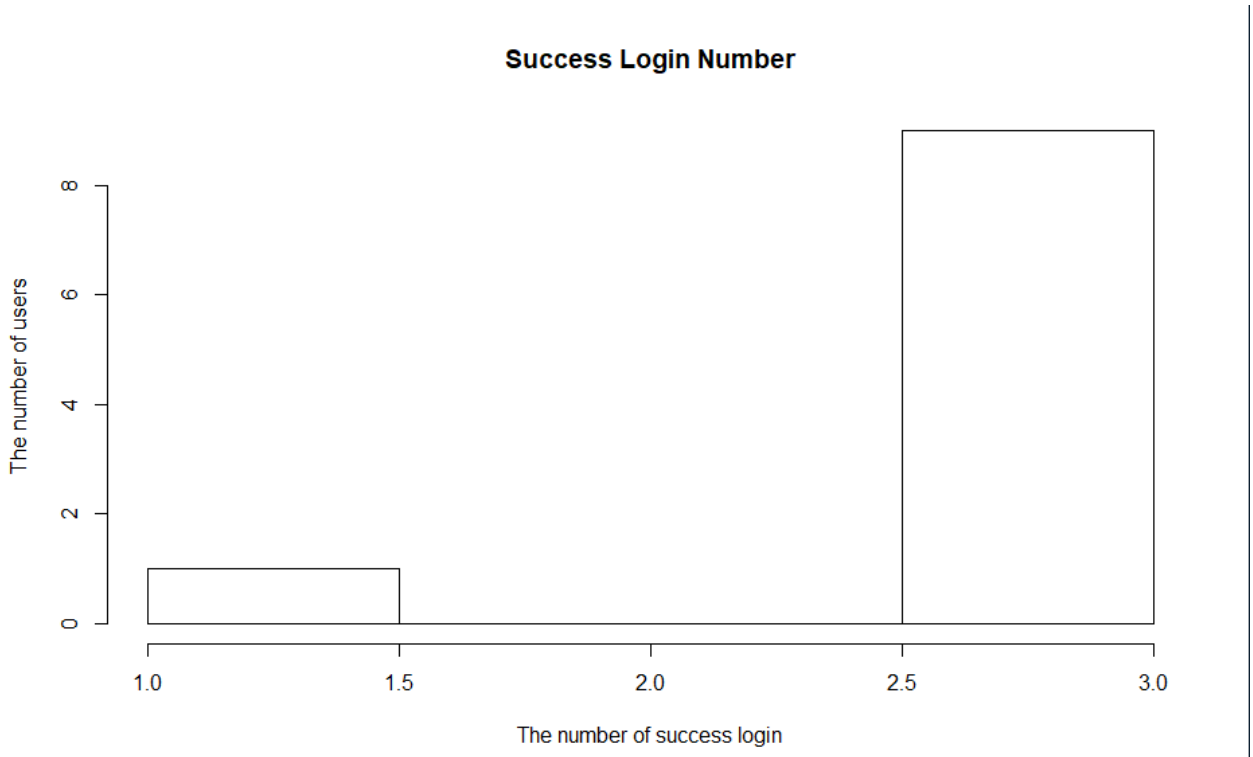
2WordsPassword.The name will be used in following.

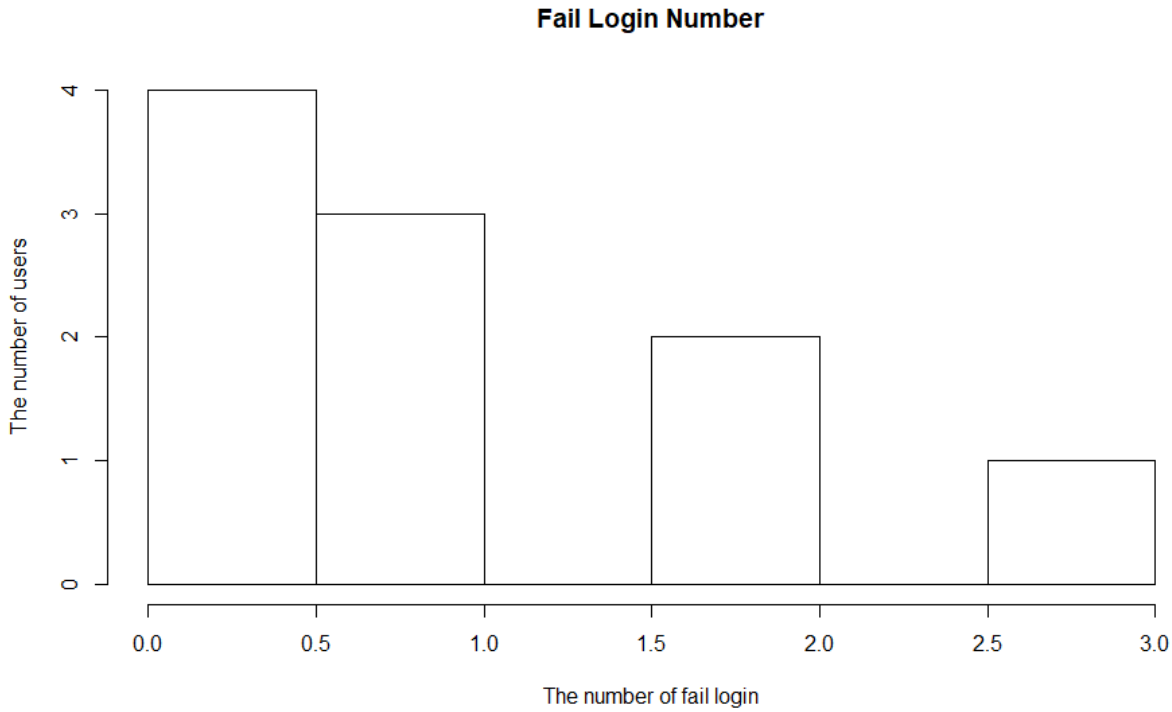
2.6.2Descriptive statistics:

2WordsPassword Descriptive Statistic			
	Mean	SD	Median
Total-Login	3.8	1.033	3.5
Total-Successful	2.8	0.63	3
Total-Fail	1	1.05	1
Successful-Time	30.71	13.61	28.9
Fail-Time	11.23	12.28	9.8

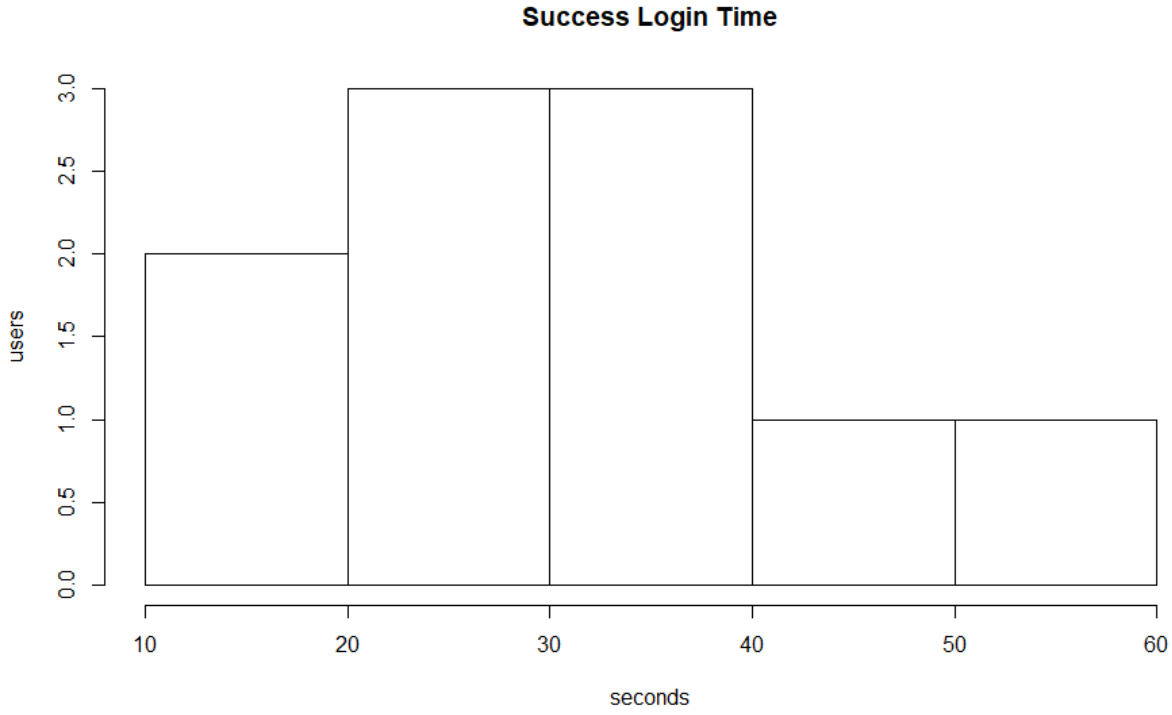
2.6.3Histograms for the number of logins (per user, total, successful, and unsuccessful):

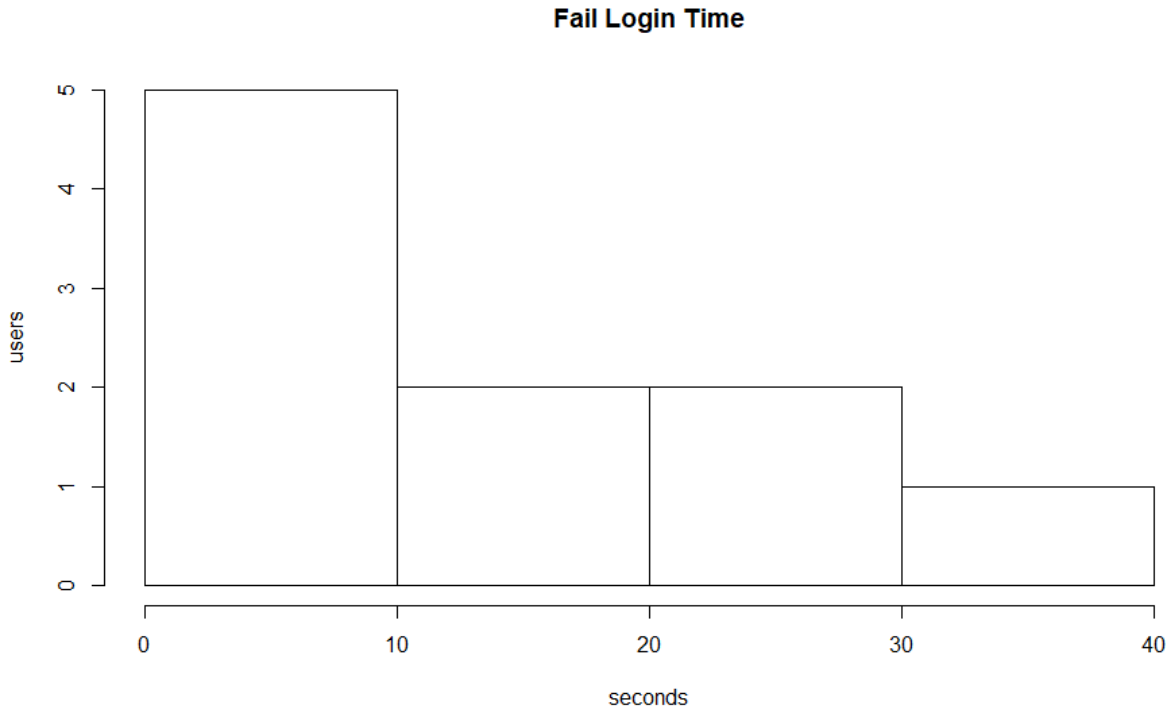


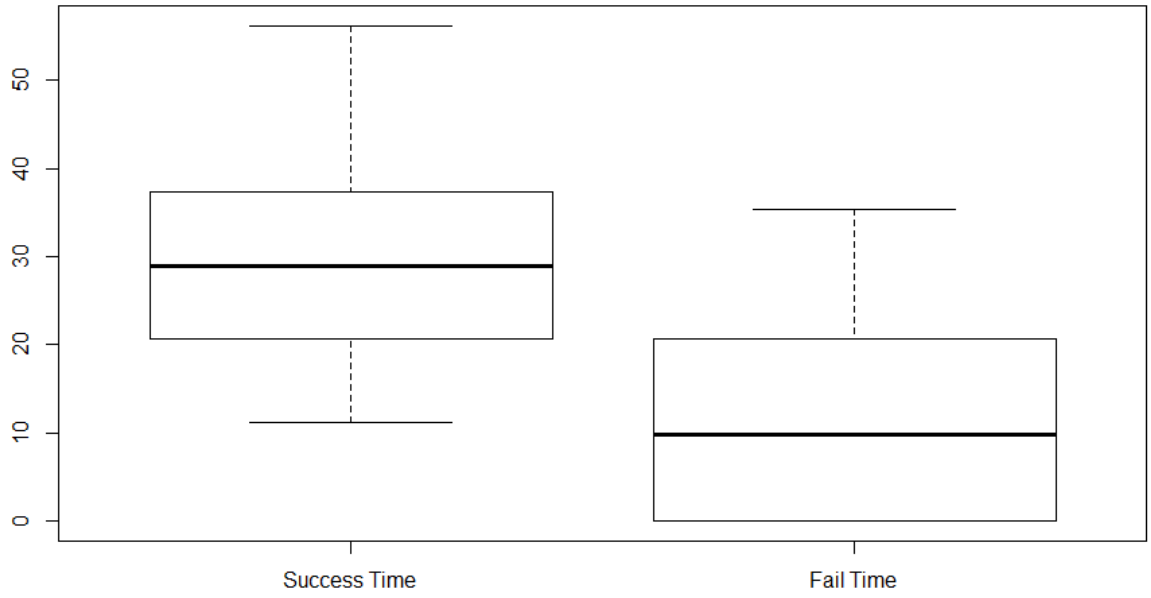

Success Login Number
The number of users
0
2
4
6
8
1.0
1.5
2.0
2.5
3.0
The number of success login


Fail Login Number
The number of users
0
1
2
3
4
0.0
0.5
1.0
1.5
2.0
2.5
3.0
The number of fail login

2.6.4Histograms and boxplots for the login time per user, successful, and unsuccessful:







2.6.5Using inferential statistics to determine whether the results are statistically significant.

$$t = \frac{\text{statistic - hypothesized value}}{\text{estimate standard error of the statistic}}$$

Statistic = $M_{Text21} – M_{2WordsPassword}$

Hypothesized value = N (Text21) – N (2WordsPassword)

Estimate standard error of the statistic = $S_{M_{Text21} - M_{2WordsPassword}}$

$$б_{M_{Text21} - M_{2WordsPassword}} = \sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}$$

$$(S_{M_{Text21} - M_{2WordsPassword}})^2 = б_{M_{Text21} - M_{2WordsPassword}}$$

Based on above formula we can calculate get t. We can get following result after two tailed t test.

1, Comparison of the number of total login between Text21 and 2WordsPassword.

	AST	AST
	2WordsPassword_totalLogin	Text21_totalLogin
Mean	3.8	16.61
SD	1.033	4.9
N	10	18
t	8.1026	
df	26	
standard error of difference	1.581	
p	p < 0.0001	

Because of two-tailed p < 0.0001, by conventional criteria, this difference is considered to be extremely statistically significant.

2, Comparison of the number of total successful login between Text21 and 2WordsPassword.

	AST	AST
	2WordsPassword_totalSuccess	Text21_totalSuccess
Mean	2.8	14.05
SD	0.63	3.438
N	10	18
t	10.1704	
df	26	
standard error of difference	1.106	
p	p<0.0001	

Because of two-tailed p < 0.0001, by conventional criteria, this difference is considered to be extremely statistically significant.

3, Comparison of the number of total unsuccessful login between Text21 and 2WordsPassword.

	AST	AST
	2WordsPassword_totalFail	Text21_totalFail
Mean	1	2.56
SD	1.05	3.329
N	10	18
t	1.4321	
df	26	
standard error of difference	1.089	
p	p = 0.1640 > 0.0001	

Because of two-tailed p = 0.1640 > 0.0001, by conventional criteria, this difference is considered to be not extremely statistically significant.

4, Comparison of successful login time between Text21 and 2WordsPassword.

	AST	AST
	2WordsPassword_sucessfulTime	Text21_successfulTime
Mean	30.71	1.89
SD	13.61	1.844
N	10	18
t	8.9713	
df	26	
standard error of difference	3.212	
p	p < 0.0001	

Because of two-tailed p < 0.0001, by conventional criteria, this difference is considered to be extremely statistically significant.

5, Comparison of unsuccessful login time between Text21 and 2WordsPassword.

	AST	AST
	2WordsPassword_failTime	Text21_failTime
Mean	11.23	0.44
SD	12.28	0.922
N	10	18
t	3.7666	
df	26	
standard error of difference	2.865	
p	p = 0.0009 > 0.0001	

Because of two-tailed p = 0.0009 > 0.0001, by conventional criteria, this difference is considered to be not extremely statistically significant.

2.6.6Interpret the results of our testing and survey and assess our findings.

In this survey, there were 11 participants testing 2WordsPassword. Because one of them left before finishing the entire testing, we drop off his data. Therefore, the sample size is 10.

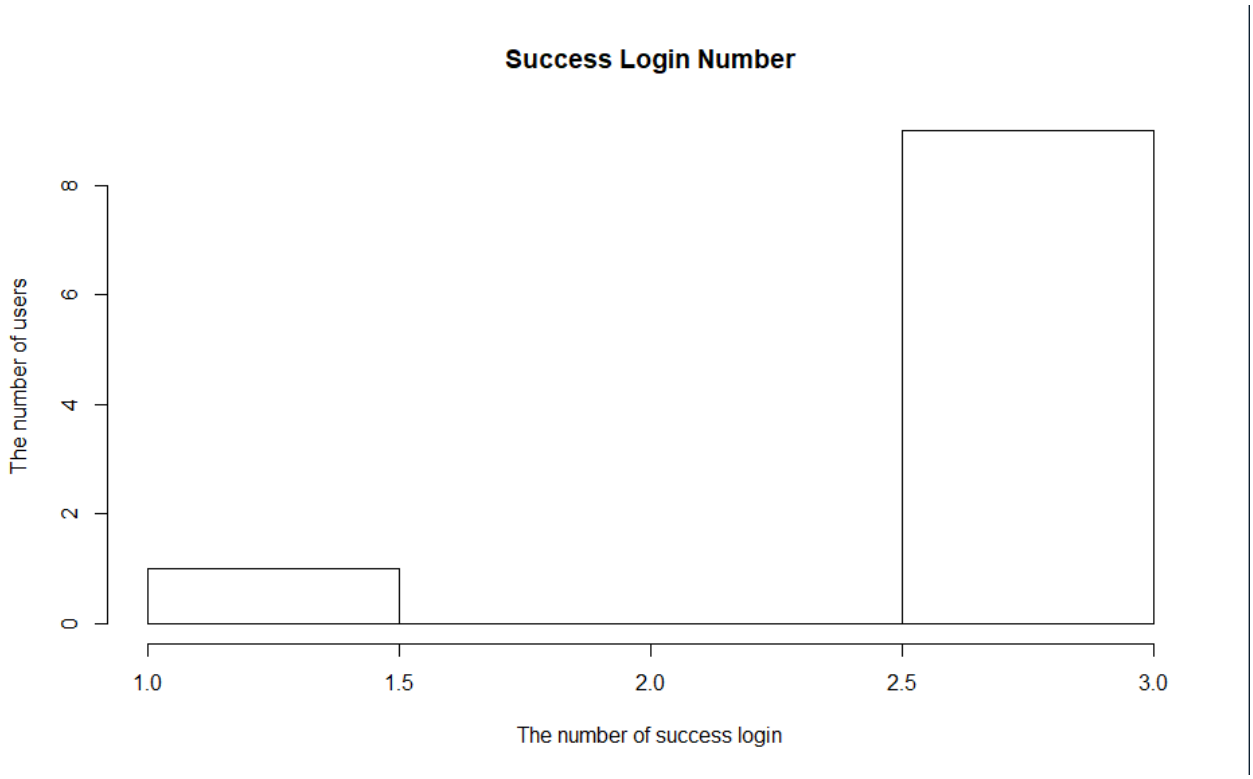
2WordsPassword Descriptive Statistic			
	Mean	SD	Median
Total-Login	3.8	1.033	3.5
Total-Successful	2.8	0.63	3
Total-Fail	1	1.05	1
Successful-Time	30.71	13.61	28.9
Fail-Time	11.23	12.28	9.8

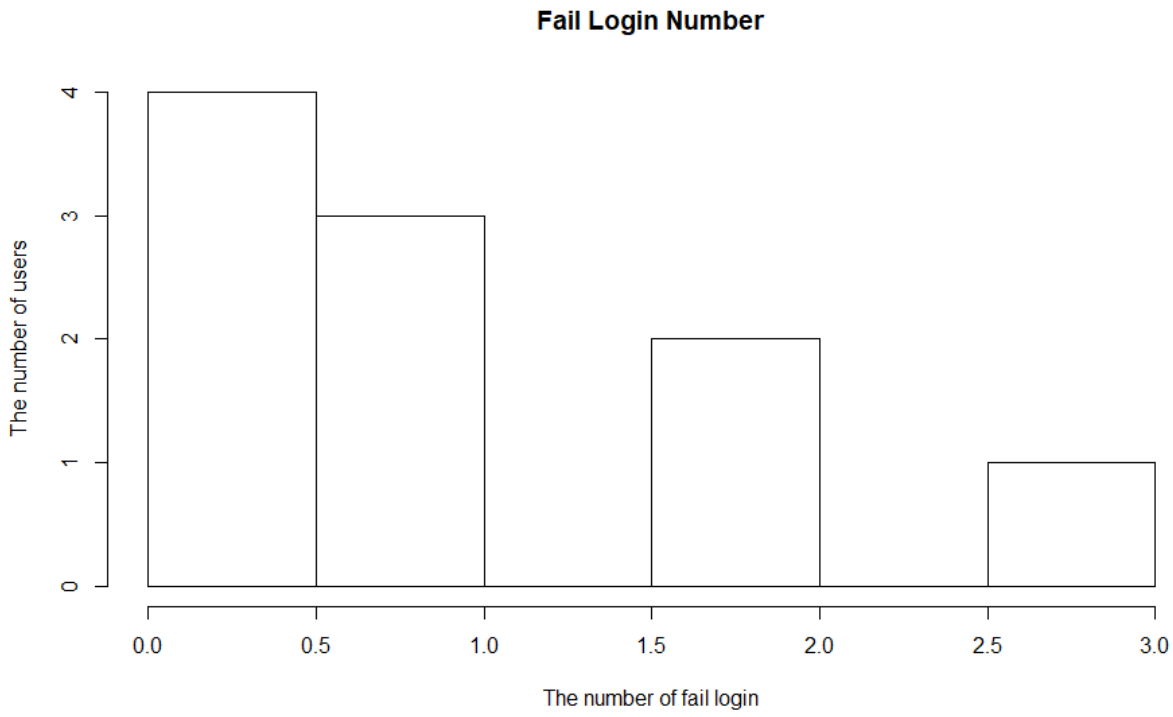
From above table we can find average number of login is 3.8 times.

2.8 times, in these 3.8 times, are successful. The rest is failed. Successful login rate is high around 74%. Median data also (total login 3.5 times, success 3 times) indicates high successful login rate. These data prove 2WordsPassword is convenient to use.

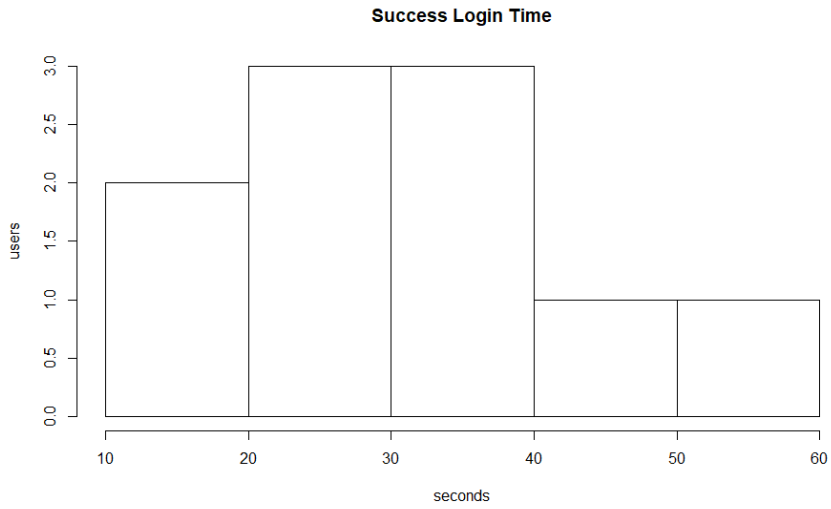
For login time, mean of successful time （30.71 seconds）is much higher than mean of unsuccessful time （11.23 seconds）. It shows 2WordsPassword is reliable to use.

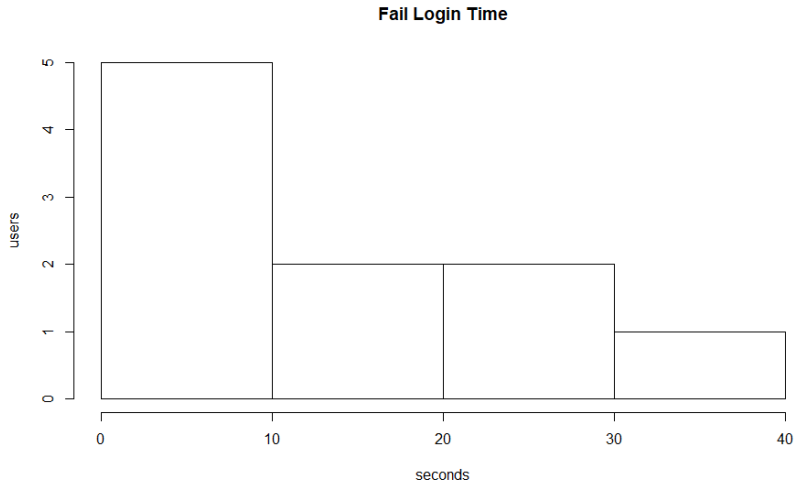
While, drawback of long login time is also obvious. Overall, from above table, 2WordsPassword own wonderful performance on the usability and memorability.





We find the number of successful login is much higher than the number of unsuccessful login, through above two histograms.





The two histograms show that successful login time is higher than unsuccessful login time. By the two histograms we find user spend too much time on login, although almost every time login is successful.

2.6.7. Discussion (Text21 VS 2WordsPassword)

2WordsPassword Descriptive Statistic			
	Mean	SD	Median
Total-Login	3.8	1.033	3.5
Total-Successful	2.8	0.63	3
Total-Fail	1	1.05	1
Successful-Time	30.71	13.61	28.9
Fail-Time	11.23	12.28	9.8

Text21 Descriptive Statistics			
	Mean	**SD**	**Median**
Total-Login	16.61	4.9	16
Total-Success	14.05	3.438	15
Total-Fail	2.56	3.329	1
Success-Time	1.89	1.844	1.5
Fail-Time	0.44	0.922	0

These two kinds of password scheme are both AST (Assigned Text Passwords).

The successful login rate of Text21 is 85%(the mean number of total successful login is 14.05, the mean number of total login is 16.61)

The successful login rate of 2WordsPassword is 74%(the mean number of total successful login is 2.8, the mean number of total login is 3.8)

The successful login rate of Text21 is much higher than 2WordsPassword.

We also get similarly result after calculating the successful rate through median data.

From login successful time view, we can find compared with Text21(1.89 seconds) users will spend much more time (30.71 seconds) on 2WordsPassword to login.

2.6.8 Conclusion

The two passwords scheme are both wonderful password. They all own good performance on the usability and memorability. After survey, the result support our initial predication, which 2WordsPassword is too long and not friendly to non-native speakers.

First of all, 2WordsPassword is too long. 2WordsPassword consist of two random English words and a number, which comes “2” or “4”. Compared with Text21, the length of 2WordsPassword is much longer. That’s why user spend more time on entering password. From this view, in our opinion, users will not choose 2WordsPassword as their normal password.

Secondly, 2WordsPassword is not convenient for non-native speakers of English. For native speakers, they can remember the passwords easily because it’s mother language. However, for others, the two new English words are a challenge to remember. The non-native speakers have to recite several times or a few days to remember. This limits application of 2WordsPassword. In our view, non-native speakers of English will not prefer to choose 2WordsPassword as their normal password.

Overall, 2WordsPassword is a good password scheme. While, compared with Text21, 2WordsPassword is not good enough to widely used. In our opinion, users will not choose 2WordsPassword as their normal password. If have chance, we will continue developing this password scheme to make it more efficient.

Finally, thanks for TA’s helping. Have a nice vacation!