

Project 2

Team Name: idk

Amr Shurman 100996742

Jacob Martin 101003643

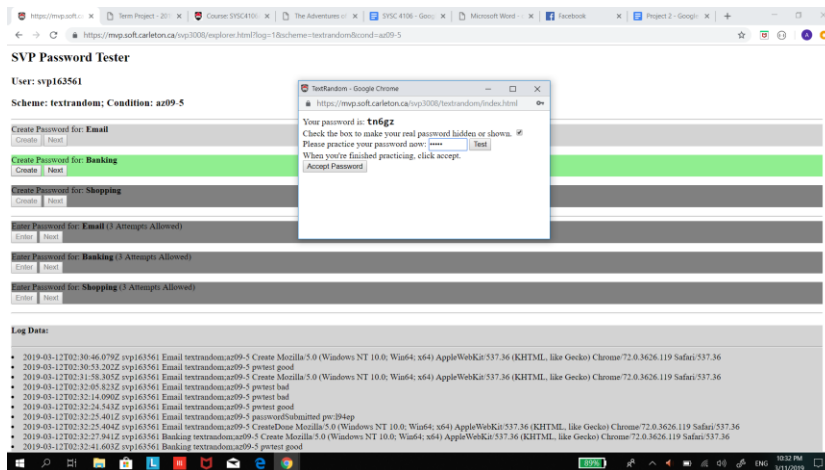
Marcio Paulo 100998559

Eto-Oluwa Segun 100985208

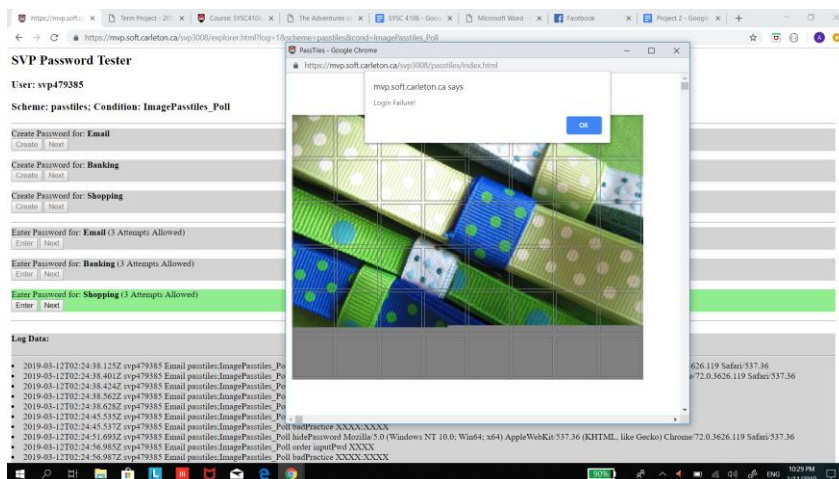
Comp 3008

Section 1.1)

Both TEXT21 and IMAGE21 schemes shared the same kind of interface which seems to work well when it comes to the testing functionalities. We can productively practice our password, as we are able to hide the password and also unhide it when we are practicing. This serves to stimulate our memory and help us in terms of memorization. When it comes to passwords, it seems like both schemes are completely random pieces of information. We are provided with random spots of pictures to remember for IMAGE21, which most likely are non-memorable spots. For TEXT21, we are given random letters and numbers that have no meaning whatsoever, making it pretty unmemorable as well. However, when it comes to security, these schemes both prove to be ideal as they are very hard to guess or memorize off first glance, making them both very secure schemes. We had a much easier time memorizing the text passwords than the image ones. However, we also came to the realization that the TEXT21 passwords tend to get forgotten about after we move to the next password. This issue is not as prominent when it comes to IMAGE21, however, it does take us longer for us to memorize the image password. We also found both systems to be very bland and un-interactive. It is difficult to get the user to remember passwords when the user is confused and overwhelmed by the password, yet alone when they are uninterested at all. The data generated from the passwords also lack any relatability or meaning since they are complete random gibberish. We also thought it was much easier and faster for us to enter our passwords using the TEXT21 system, since the user can login in a matter of seconds, sometimes without even thinking about the password. However, IMAGE21 passwords seem to need more effort and time in order to complete. Also, when we have mastered the IMAGE21 password and the TEXT21 passwords, we noticed that we got less failed logins when using the IMAGE21 scheme. However, this information doesn't mean much since it takes us longer time to master the IMAGE21 passwords. All in all, we think the TEXT21 is slightly superior to the IMAGE21 scheme. The only thing that we noticed the IMAGE21 scheme might be better at is the fact that its passwords take a longer time to be forgotten about .



Practicing text passwords



Entering Image passwords

Section 1.3)

The log data for each password scheme was collected by reading in each file and then dividing it by scheme and user. Each file when loaded would read each line in the file one at a time, breaking them apart based on the commas in the line. These lines would then be sorted into a data structure called a “Record” that could store the data for the time, user ID, password scheme, site ID, mode used, and event message.

Each record would then have their user ID checked to find the user that the record belonged to in the program’s records. If the user for the record wasn’t found, then a new user would be created with the new user ID. The record would then have its event field checked to see if it matched “start”, “enter”, or “login” as these are the only events that matter for the data that we were

gathering. In the case of the “start” and “enter” events, the current record would be stored in the user’s data as the last start event record. For the “login” records, the program would get the users last stored start event record (as described for the “start” and “enter” records) and use the time of that record and the time of the “login” record to find the amount of time the user took to login. From the “login” record, we also got whether the login was a success from the event message field where it would contain either “success” or “failure”. The type of password scheme that was in use is also obtained from the “login” record, all of which is then stored in the users data which then sorts and stores the data on the login time, fail/success rate of that user for each password scheme that it is given.

When all the records from the csv files are loaded and sorted into the appropriate users and schemes, the program then goes through all the users that have been found, and then goes through all the schemes that user used. The programs then gets all the data for each user and scheme and writes them out to a new csv file with the rows of “user ID”, “password scheme”, “total logins”, “successful logins”, “failed logins”, “average successful login time”, and “average failed login time”. This would result in a csv file with all the required data sorted and averaged into usable fields that could then be imported and displayed in R.

PSeudoCode

```
file = readFile(Filename)
```

```
for (row in file):
```

```
    record = readRecord(row)
```

```
    if (record.event == "start" or record.event == "enter"):
```

```
        users[record.userID].setStartRecord(record)
```

```
    else if (record.event == "login"):
```

```
        startRecord = users[record.userID].getStartRecord()
```

```
        deltaTime = record.time - startRecord.time
```

```
        loginAttempt = new LoginAttempt(deltaTime, record.scheme, record.data)
```

```
        users[record.userID].addLoginAttempt(loginAttempt)
```

```

outputFile = writeFile(outputFileName)
for (user in users):
    outputFile.write(user.data)

```

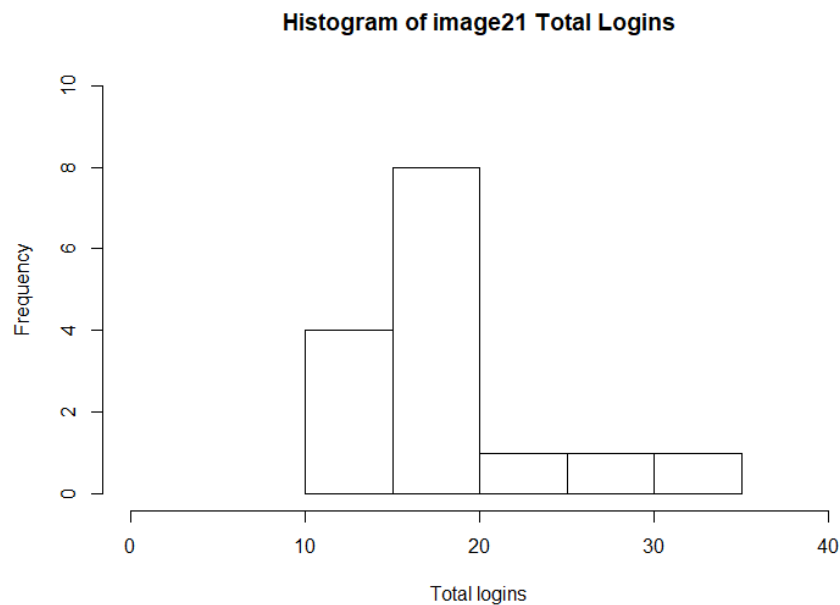
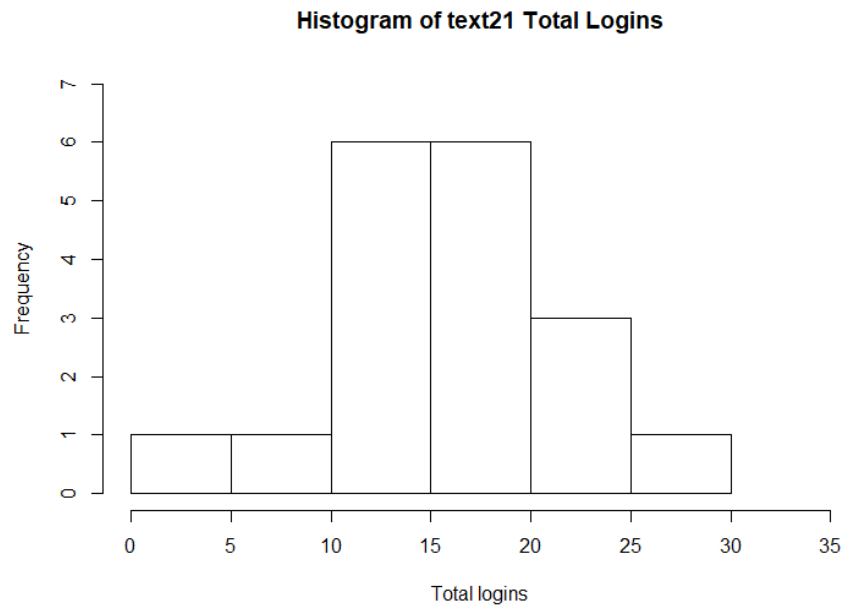
Section 1.4)

	Text21	Image21
Mean for Total Login	16.61111	19.13333
Mean for Successful Login	14.05556	14.73333
Mean for Failed login	2.55556	4.4
Median for total login	16	18
Median for successful login	15	15
Median for Failed login	1	3
Standard deviation for Total login	4.900647	5.289702
Standard deviation for Successful login	3.438061	1.387015
Standard deviation for Failed login	3.329409	4.436859
Mean for successful login time	9951.056 ms	17132.53 ms
Mean for failed login time	6017.333 ms	18405.07 ms
Median for successful login time	9063 ms	14184 ms
Median for failed login time	5500 ms	15666 ms
Standard deviation for successful login time	4244.465 ms	7570.872 ms
Standard deviation for failed login time	6896.467 ms	14101.44 ms

According to the data collected. We notice that the participants had more login failures in the image21 scheme than they did in the text21 scheme when looking at the means. (Text21 being 2.555556, and Image21 being 4.4) However, to ensure that this conclusion is true, we decided to run probabilities on the mean values. We will also apply the same procedure to the other factors as well. According to our data, we have a total login mean of 16.61111 for text21, while image21 has a 19.13333 total mean. According to our data, this means that text21 has a 15.4 % login failure rate ($2.555556 / 16.61111$) while Image21 has a 23 % failure rate ($4.4 / 19.13333$). We also notice that the standard deviation for failed Login is larger for image21(4.436859) than that of text21(3.329409), meaning that the average variation around the failed login mean for image21 is larger than that of text21. This means that the mean for the failed logins for image21 can span even higher values. Image21's values span larger values are further from its mean, while text21's values do not spread out as much, making its mean a more reliable value of comparison, and showing that it doesn't get high failure values as much as image21. This proves to show that image21 has higher failed login values than that of text21. When we look at the successful login standard deviation, the opposite is established, as text21 has a 3.438061 value while image21 has a 1.387015 value. This means text21 has higher successful login values than that of image21. According to our data, we can also conclude that the median points to text21 being more reliable. Even though both text21 and image21 have the same successful median (15), we also need to remember that the total for median logins is higher for Image21. According to the median value, Image21 has a successful login rate of 83 % ($15/18$), while text21 has a rate of 93.75 % Moreover, image21 has a higher login failure median (3) than that of text21 (1). Everything related to the frequency of logins point to text21 being more reliable except for the mean for successful login, text21 being 14.05556, while image21 is 14.73333. The difference in value is pretty small. Taking this value into consideration might give us a big probability of falling with the fishing expedition phenomenon. Hence, giving us the illusion that this piece of information is valuable, when in reality, it might not. We also need to understand we had a larger mean for total logins in image21 than text21. If we view this within probability standards of getting success, then according to our mean value, we realize that text21 has a greater probability of successful logins (84.6 %) than image21 (77 %). However, given that we do take consideration of this data. This might indicate that the participants had an easier time

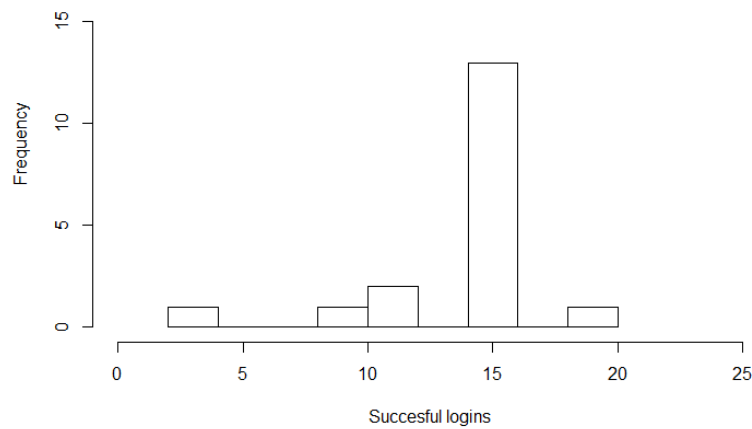
remembering the image passwords given they were successful, or in other words, once they've memorized it or stored it somewhere.

When looking at login times, everything seems to point against the image21 system. The mean, median and standard deviation all point out how much faster it is to use the text21 system. Making it more compatible, functional and usable to the user. This piece of data can show us how much easier it is for the user to use the text21 system. It can also show us how much easier it is for the user to remember the text password rather than the image password. All in all, all the data discussed so far works on showing how much more reliable the text21 system is than the image21 system.

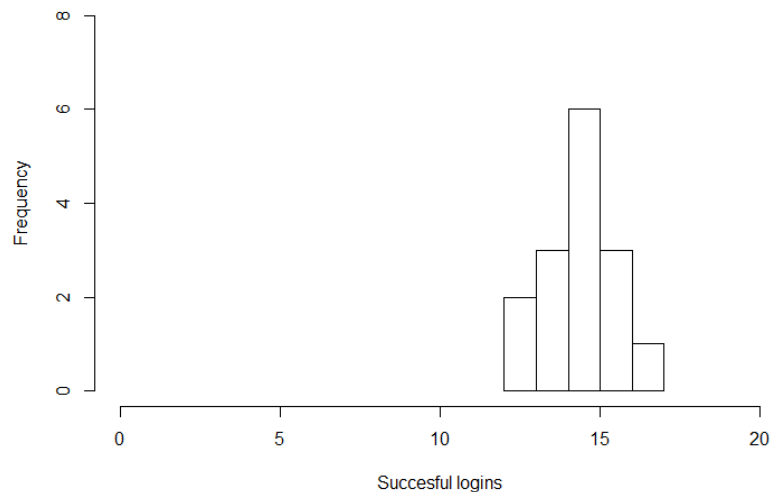


From this piece of information we can tell that we had a smaller range of people logging in in text21. Text21 has people logging in 1-10 times, while in image21, that doesn't exist. Image21 also has 30-35 people logging in while Text21 does not. This might be because it took image21 participants more tries in order to get a successful login, while for text21, it was easier to get a successful login without going through as much fails.

Histogram of Successful text21 Logins

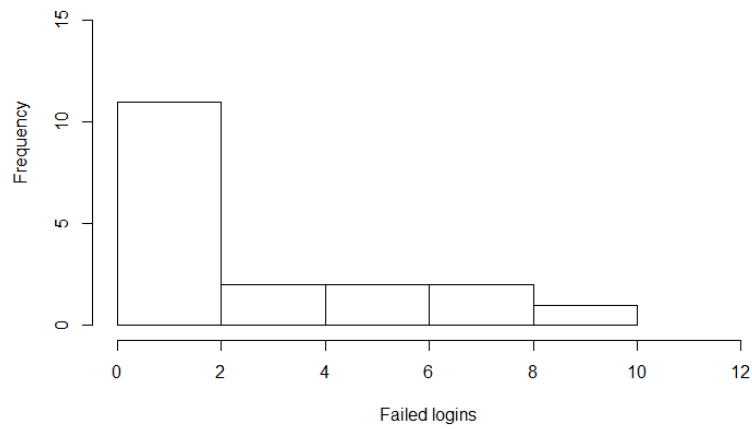


Histogram of Successful image21 Logins

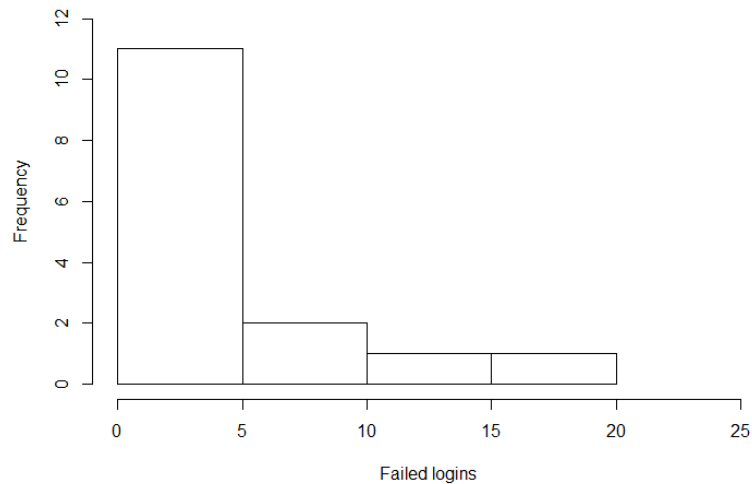


From this piece of information, we can see text21 having more frequent successful logins than that of image21. Text21's most frequent successful login value (14-16) peaks at around 14. While image21's most frequent value (14) peaks at only 6. Image21's 15 successful value is 3, and its 16 value is 1, meaning image21's 14-16 value is 10, which is less than that of text21. Text21 also has more distributed data, hence meaning they can slightly hit higher successful login values. However, since image21's data is less distributed, it seems like Image2's successful login values show to be more consistent amongst people who remember their password, or in other words people who get more frequent successful logins.

Histogram of Failed text21 Logins

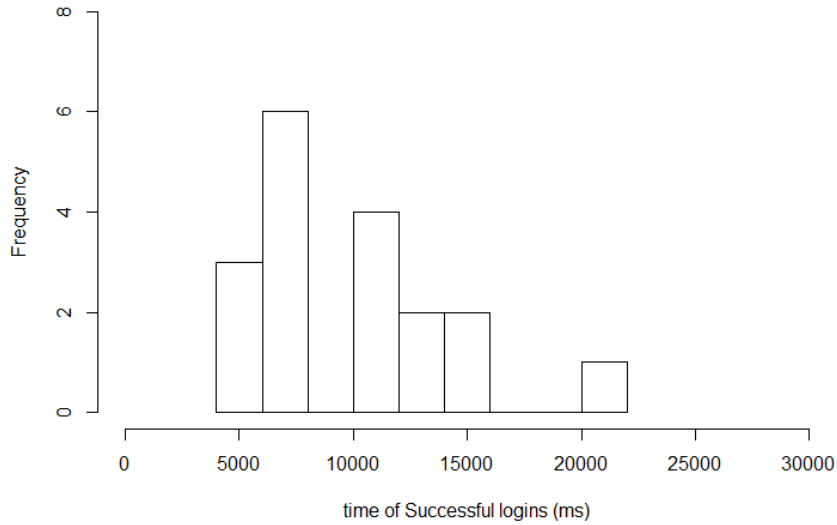


Histogram of Failed image21 Logins

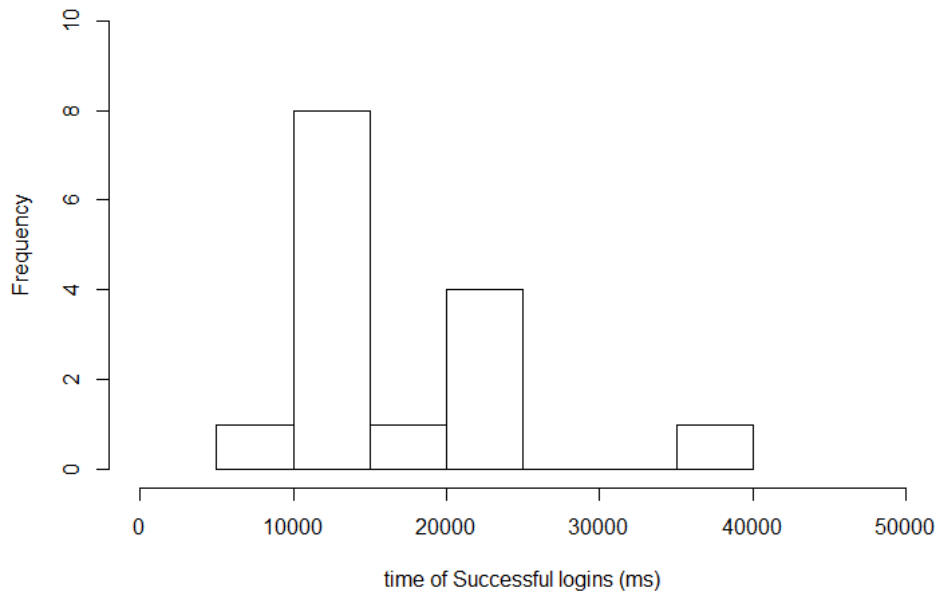


This piece of information further proves my point for the total login histograms. It seems as if text21 had less participants getting failed logins. Image21 shows people failing around the 10-20 margin, while in text21, that doesn't exist at all. Hence, showing us that people in image21 tend to get more failed logins than text21.

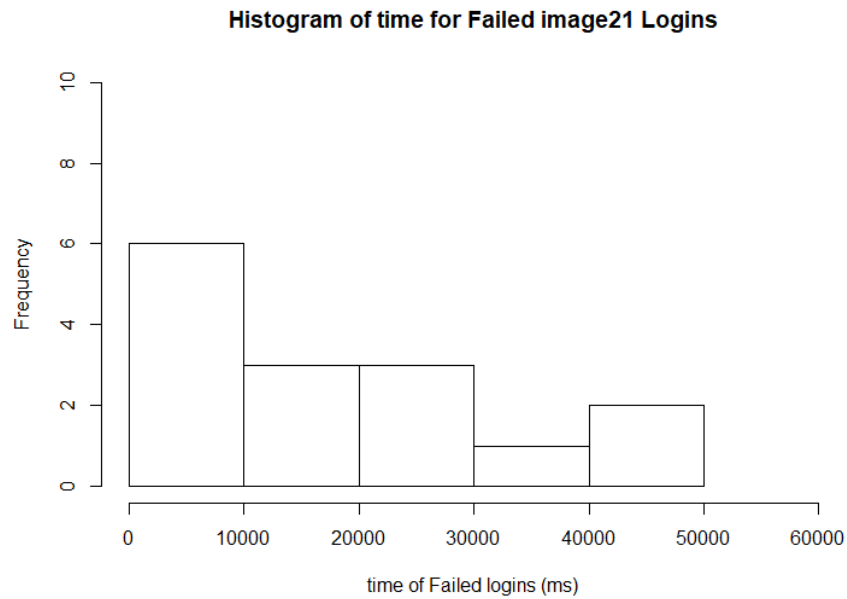
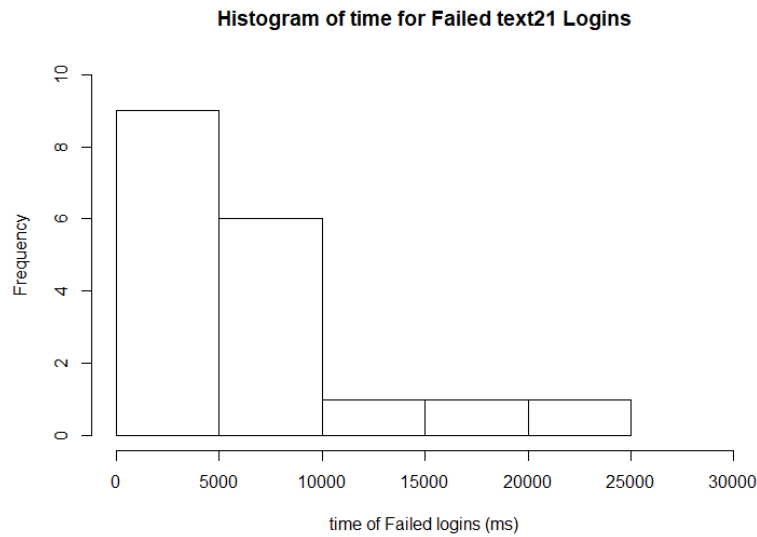
Histogram of time for Successful text21 Logins



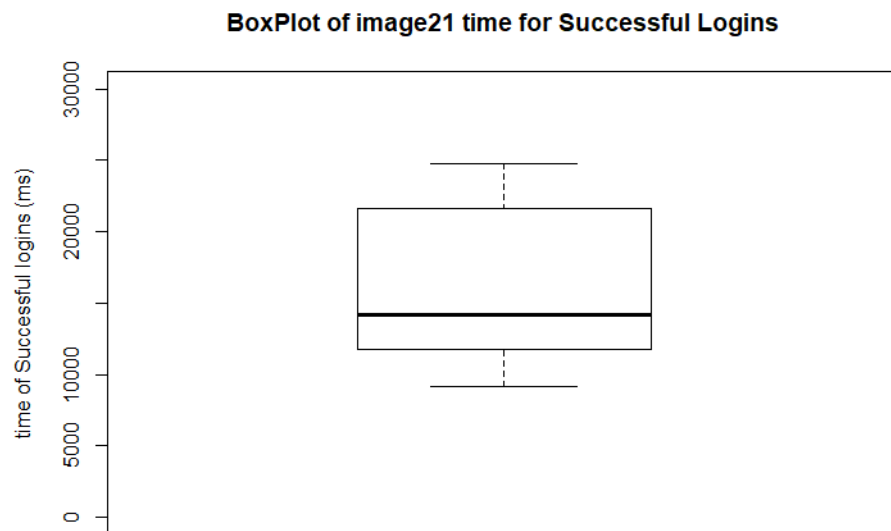
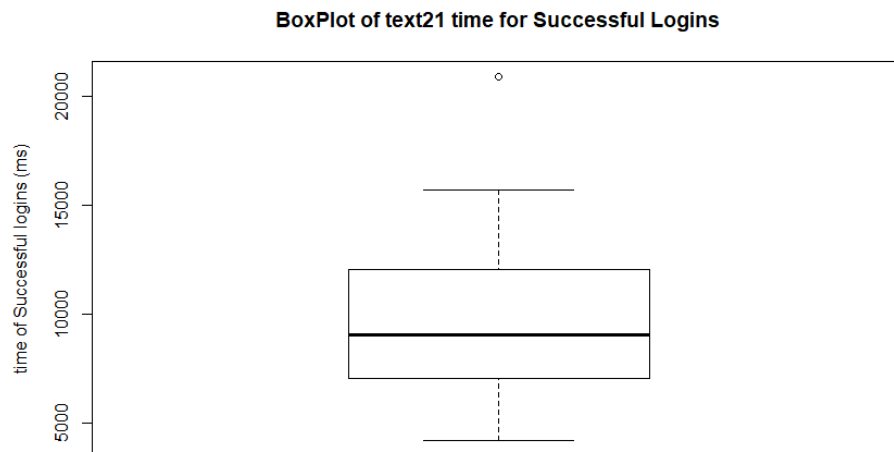
Histogram of time for Successful image21 Logins



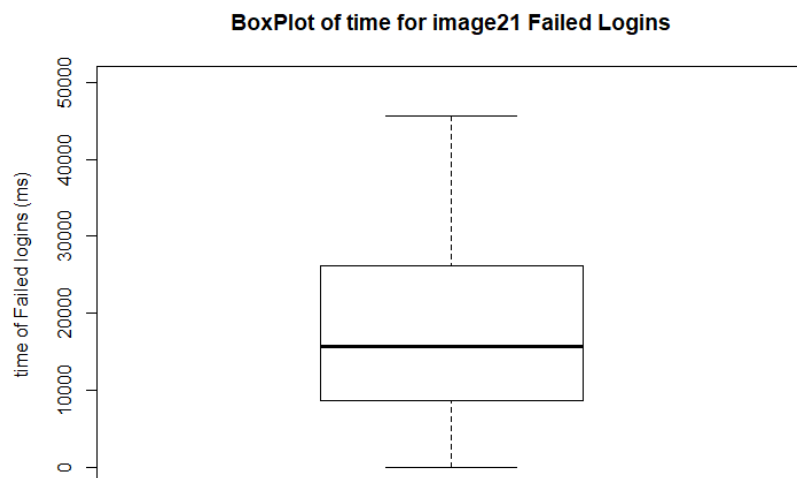
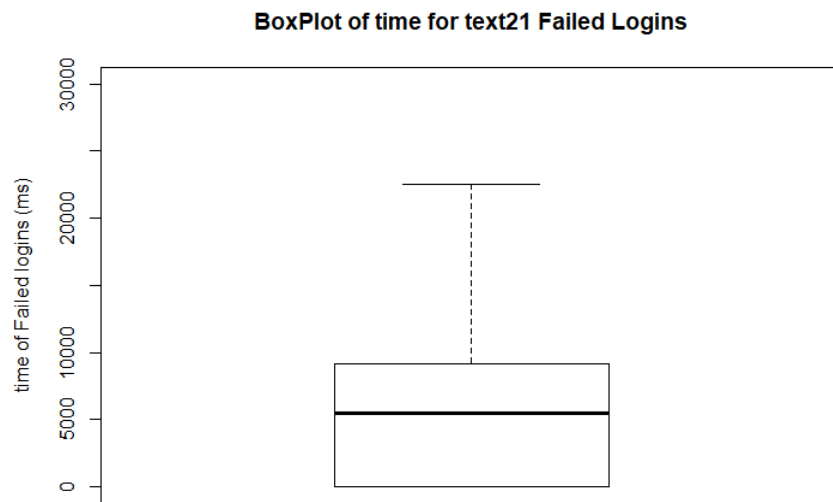
From this data, we can easily tell how much faster it is to use the text21 scheme. Image21's time for a successful login can reach values of 40 seconds (40,000 ms), while text21's max time value is about 20-22 seconds (20,000-22,000 ms). Also, most of text21's values end at around 16 seconds, while for image21, the values end at around 25 seconds. This is further proof of how much slower image21 is than text21.



This data also proves how much faster it is to use the text21 system. It also shows how unreliable image21 really is. We cannot imagine how frustrating it could be to spend 50 seconds trying to input a password, just to get it wrong and try again. That is what this data tells us about image21. Text21's data is more positively skewed, meaning that most of its login time values are within the shorter times, as most of the values are between 0-10 seconds. The values also only peak at 20-25 seconds at the worst case scenario with a frequency of 1. While image21 peaks at 40-50 seconds at frequency 2.



This piece of information shows us that the mean for the time of successful logins is drastically smaller for text21 than that of image21. Text21 also has its outliers reach smaller values that image21 are so far from reaching. This data also proves that login time for image21 is more consistent than text21 due to less variation in the data. This might show us that people succeeding with image21 might have an easier time remembering their password.



This data also helps us understand how unreliable image21 can be, as the mean for failed logins in image21 is much higher than that of text21. Just like the histogram. We can also see how image21's failed times can span up to 45,000 while text21 only spans to around 22,000 on a bad day.

Final conclusion:

All in all, we can easily conclude that text21 is a far much better scheme than image21. Text21 can take far much less fails in order to get a successful login, hence showing us how much easier it to use text21 rather image21 as the data suggests it is overall much easier to remember the text passwords. They also take far much less time to login. I have previously mentioned how much annoyance it could be for the user to spend so much time inputting his password, just to get it wrong and try again, because he forgot to select an image or for whatever reason. Even when getting it right, spending that much time on a password is highly unusable. The only point that image21 gets from this is the consistency. It seems like people who know their image password tend to take about the same time and tries to get into the system. While for text21, the user's time and frequency of successful login varies much more. This might indicate that even though the image21 system gets more fails and takes longer time to get in. Once the user masters their practice with memorizing the image passwords, the passwords for image21 might be easier to remember than that of text21. However, all in all, text21 proves to be more usable.

Section 2.1 Description of password scheme

Our password scheme was designed to have 3 major parts. Each part has 3 components and each component has an image and color combination that needs to be memorized for success.

Therefore to successfully use this password scheme, one has to memorize the image and color combinations assigned to all 3 major parts and replicate those very same combinations in the same order they were assigned. For each of the components only a limited number of colors and images are used. To be specific there are only 10 colors and 13 animals used.

The password space is 2,197,000 which is $(10 \times 13)^3$.

I think our password scheme might have good usability in cases where similar patterns are assigned to the 3 different parts of the scheme. If for instance all 3 parts of our password have an elephant or a blue animal, it will be easier to remember and replicate that pattern, since it already exists in other passwords. Even if the pattern is not exactly the same in all major parts, the similarities could help users in terms of usability and memorization of the scheme.

Our scheme really tests the strength of human memory because memorizing image patterns really exercises the brain's ability to memorize. Having a photographic memory will make this password scheme easier to remember.

In general, the goal of our scheme was to combine elements from image21 and text21. We have learned that users find text passwords more usable. We also learned that users find image/graphical passwords to be remembered for longer times than that of text passwords. Even though we were not using text as an input. The password uses real words within the images. If we get a picture of a red elephant on our password. We also recognize the text form of the image as being "red elephant", as it is not completely random and gibberish. Hence, we recognize the password in image and text form. We are aiming to make this a big contribution in terms of memorability and usability.

Section 2.2-2.3 Password System Implementation

The user interface for the password system tester is built to work the same as the password systems for both image21 and text21. The system will first give the user 3 passwords and record them, showing the user each password one at a time when the user selects the "Create" button for each password. The "Create" button for each password will only be clickable after the password for the last field/site is created. After all the passwords are created, the "Check" buttons will then become clickable. When each "Check" button is clicked, the user will be prompted to input the password for that buttons field/site. After the user enters the password, the system will check if it is correct, and then output to the log either "success" or "failure". After one password is entered, the next "Check" button will become clickable.

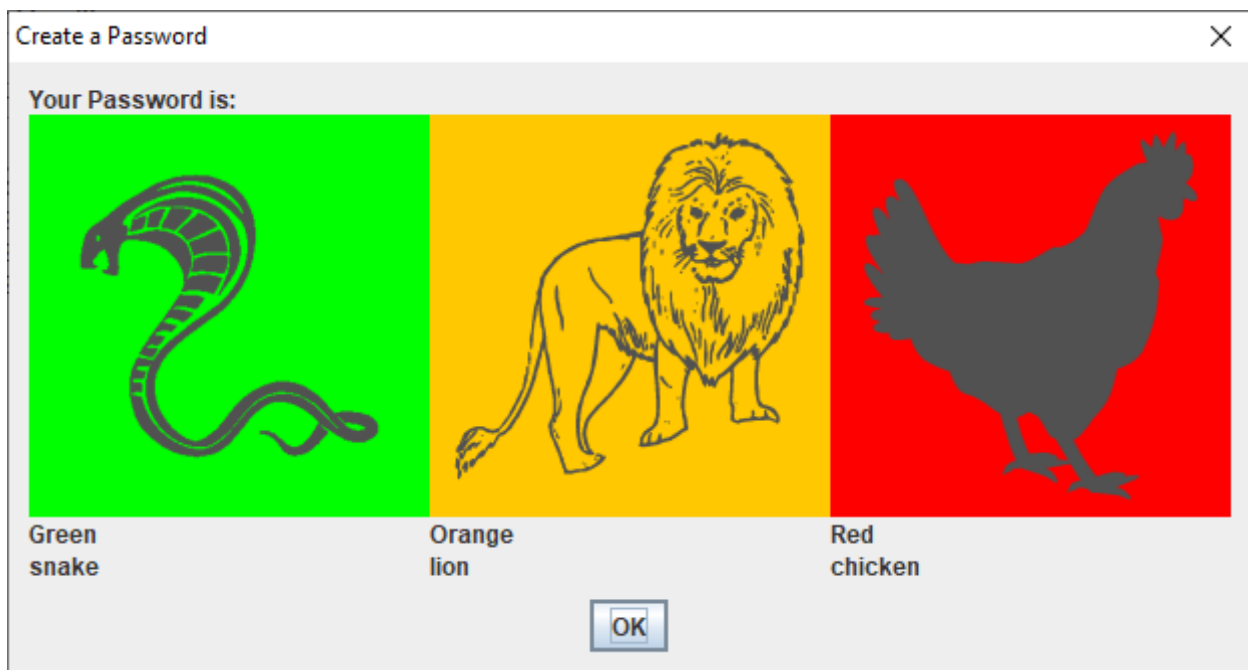
When the user clicks the "Create" buttons for the passwords, the system will make a popup that will show a new randomly created password and store that password in memory. The password will be shown as an image of the selected animal with the background being the selected color. Below the image is two labels that say the name of the animal and the color of the image for the user to be able to read if they have issues with the images.

When the user clicks the "Check" buttons, the system will make a popup that will allow the user to enter a password. When the user enters the password, they are shown an image of the currently selected pairs in password. Below each pair are two drop boxes with the currently selected animal and color for that pair for the user to use to enter the password. When the user

selects an animal or color using the drop menus, the images of the pairs will update to match the new selected pair, allowing the user to see their currently selected pairs. The user then clicks ok to finish entering the password, which is then compared to the correct password.

Passwords are displayed in the system as a row of images showing the animal images pairs, with the image of the animal having the background being the selected color. Below each image will be either a pair of labels or drop boxes depending on whether the user is being shown or entering a password. The labels or drop boxes will contain the currently selected color and animal for that pair in the password sequence. If the image has drop boxes below it, if the color or animal in the drop box changes, the image above them will be updated to show the new animal/color pair.

All logs from the system are written as they happen to both the text field at the bottom of the systems window and to a new csv file on the desktop labelled “KeyPairPassword-UserID”. This file will contain all the data from when the user is creating passwords and data on when the user tried to login and if they were successful or not.

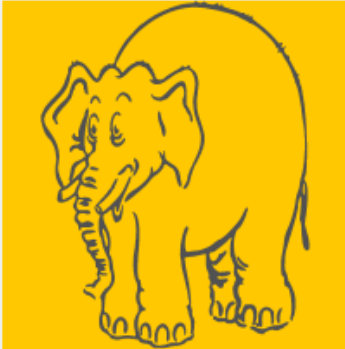

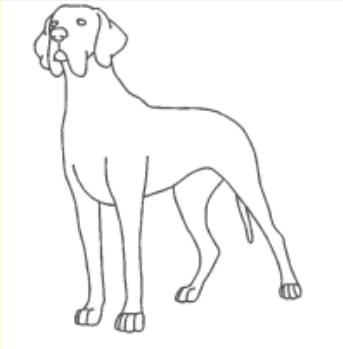


The output display of the system to display the password created to the user. Contains an image with the image of the animal on a background of the color given to each pair in the password sequence. Below each image is 2 labels telling the user in words the name of the animal and the color used in the given pair. The “OK” button is for the user to click when they are finished viewing the given password and wish to continue.

Enter Shopping Password

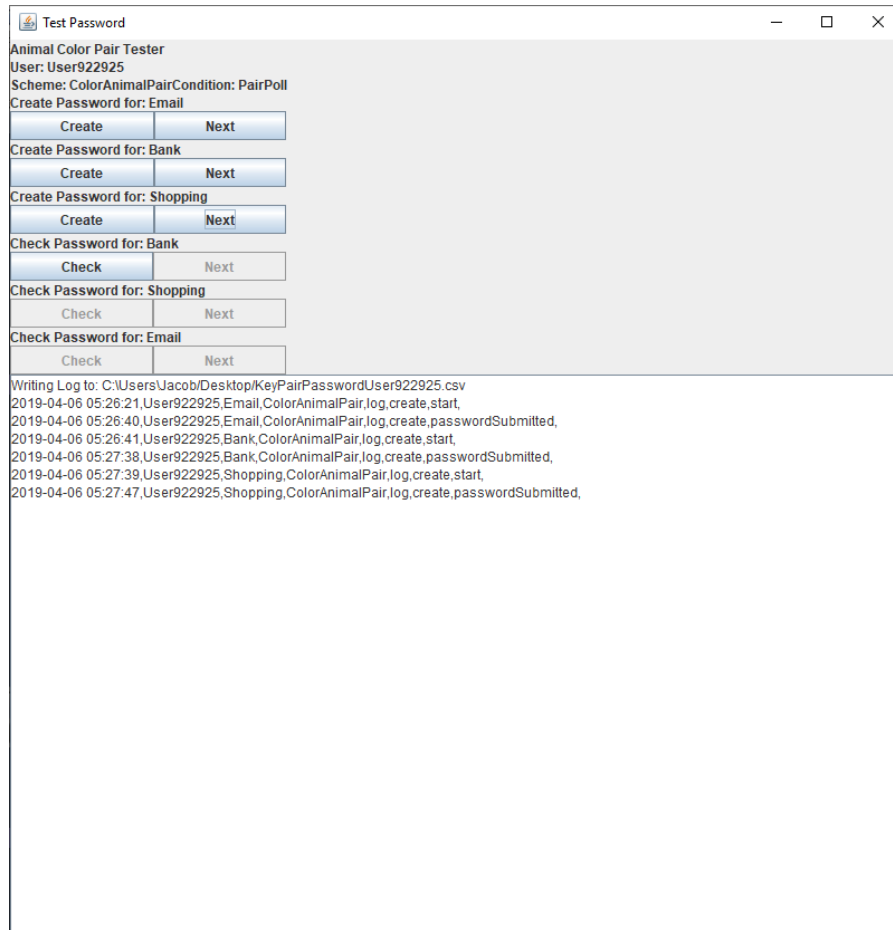
?

Password:

		
Orange	Yellow	White
elephant	bear	dog

OK Cancel

The input display of the system to allow the user to input a password into the system. Contains an image with the image of the animal on a background of the color given to each pair in the password sequence that the user has currently selected. Below each image is 2 drop box menus to allow the user to select the animal and color for that pair in the password sequence. When the user changes the animal or color for any pair, the image for that pair will be updated to show that new color/animal pair. The “OK” button is for the user to click when they have finished entering the password, and the “Cancel” button is for if the user wishes to cancel entering the password.



This is the system's main window where the user will be able to create and test how well they remember passwords. At the top of the window is basic information for the system section like the user id, testing scheme and condition. Below the system conditions is the buttons to start creating and testing passwords. The top three button pairs are for creating passwords for three different sites which are labelled above each pair of buttons. Once the user has created a password for one site, the buttons to create a password for the next site will be enabled to create a password for that site. The next three button pairs are for testing the users memory of passwords. The first test will be enabled after all the passwords are created, and each test after that will be enabled after the last test has been done once. The site that is being tested is labelled above the pair of buttons for the tests. At the bottom of the window is a log panel that will output logs of what the user is doing, such as creating a password, starting a password test, or successful or failed password entry tests.

Section 2.4-2.5

Questions used for our survey:

1. Please rate your satisfaction with the password process.
2. I was able to quickly recall my password
3. Do you think our password scheme is difficult to remember?
4. I prefer the text-based text21 password scheme compared to this one
5. I found the password system too unnecessarily complex.
6. I think most people could use this system without technical assistance from someone.
7. I do not understand the password process without assistance
8. I would recommend this password scheme to someone else.
9. Do you feel this password scheme is secure?
10. It would be easy for others to guess my password
11. I found the various functions in the password scheme were well integrated.
12. I found this to be easier than the image21 scheme
13. I thought there was too much inconsistency in this system.
14. I think that I would like to use this system frequently.
15. I thought the system was interactive and fun

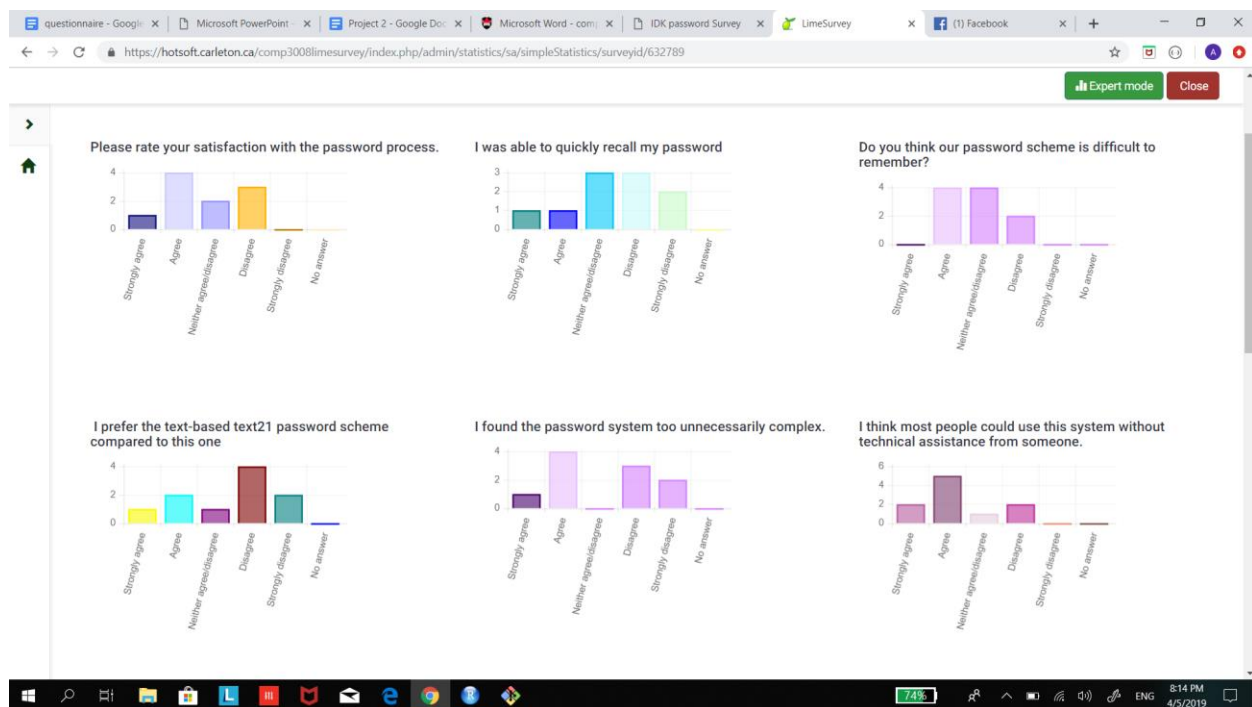
Section 2.6

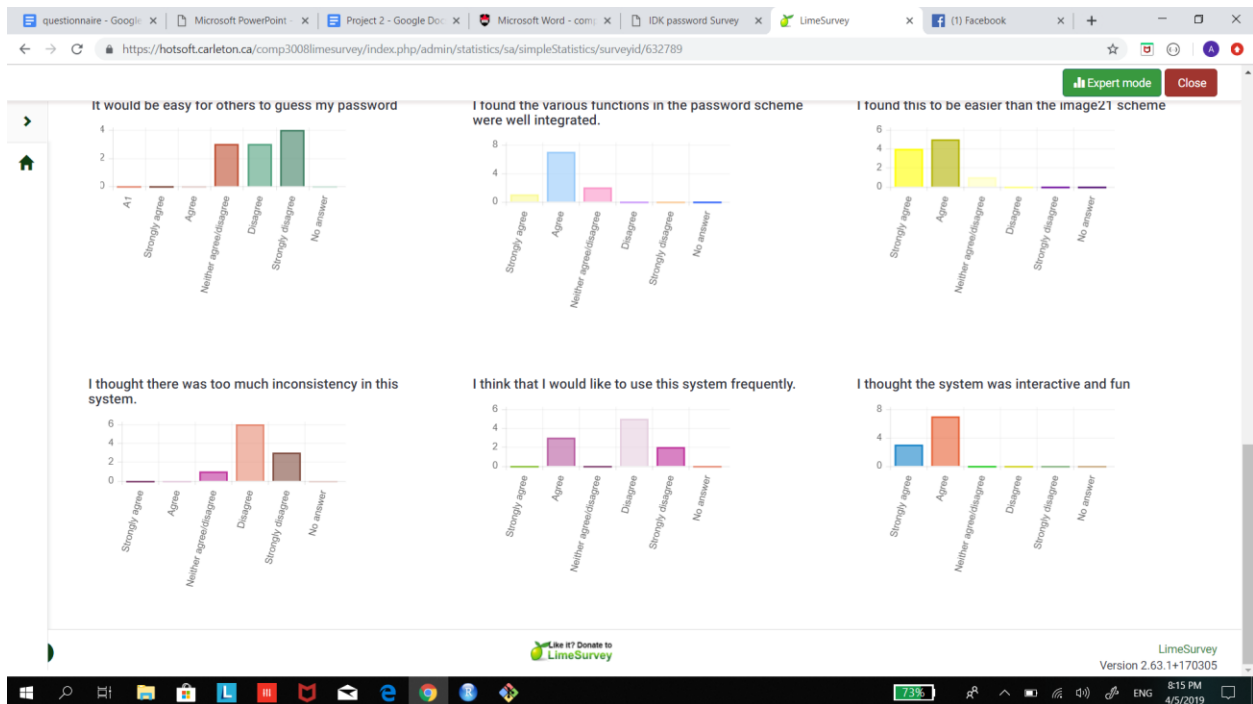
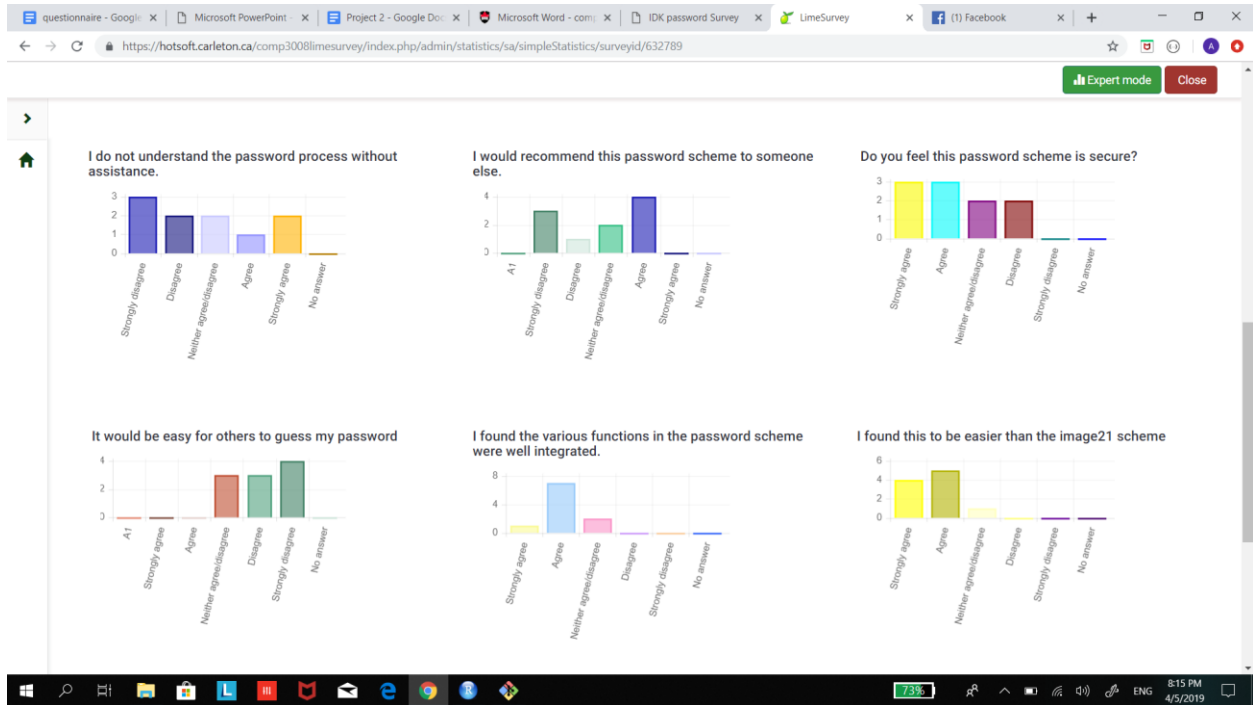
	ColorAnimalPair
Mean for Total Login	3.5
Mean for Successful Login	1.1
Mean for Failed login	2.4
Median for total login	3
Median for successful login	0.5
Median for Failed login	2.5

Standard deviation for Total login	1.178511
Standard deviation for Successful login	1.37032
Standard deviation for Failed login	1.712698
Mean for successful login time	15966.6 ms
Mean for failed login time	21083.1 ms
Median for successful login time	10500 ms
Median for failed login time	20916.5 ms
Standard deviation for successful login time	18866.15 ms
Standard deviation for failed login time	14762.73 ms

According to our data, we have significantly more people failing than succeeding to login. According to our mean for total logins (3.5), we have a 31 % chance of getting a successful login ($1.1/3.5$), and a 69 % chance of getting a failed login. According to our median for total logins (3), we have a 17 % chance of getting a successful login ($0.5/3$), and a 83 % chance of getting a failed one. Comparing these values to the text21 and image21 schemes, we can easily tell that both of the old schemes have larger successful logins and less failed logins. When looking at the standard deviation data, we notice that successful and failed logins seem to more consistent than that of image21 and text21. Meaning that most users will get around the same results each time when it comes to successful and failed logins. This can be seen as a good thing as we have less outliers and more accurate less random results. When looking at the time data, we notice that the mean, median and standard deviation of successful logins for our own scheme are shorter in time than that of image21. However, the mean, median and standard deviation of failed logins for our own scheme are in fact larger than that of image21. This means users are able to login faster and in more consistent times when they remember their password (when they are successful), than that of image21. However, image21 users are able to login faster and in more consistent times when entering a wrong password than that of our own scheme that we came up

with. From this data, it seems like our system shows the same issues that were present in the image21 system. The user does spend a lot of time trying to enter their passwords just to fail at the end, making it pretty frustrating for the user. However, when comparing with image21, we did manage to decrease the time users spend entering their passwords when successfully logging in. When we compare these values to the data from text21, we can easily tell that text21 is a much faster and more usable system for the user. However, after all that said, we must understand that it is difficult for us to conclude which system is better solely from this information provided, as our participants were given minimal time to practice their passwords, (maximum 3 minutes on average), and then they were queued to immediately enter their passwords, while the participants from the text21 and image21 could have been practicing for a longer time, and aren't necessarily queued right after practicing. All in all, we must take precaution and understand that we must consider other things when trying to compare.

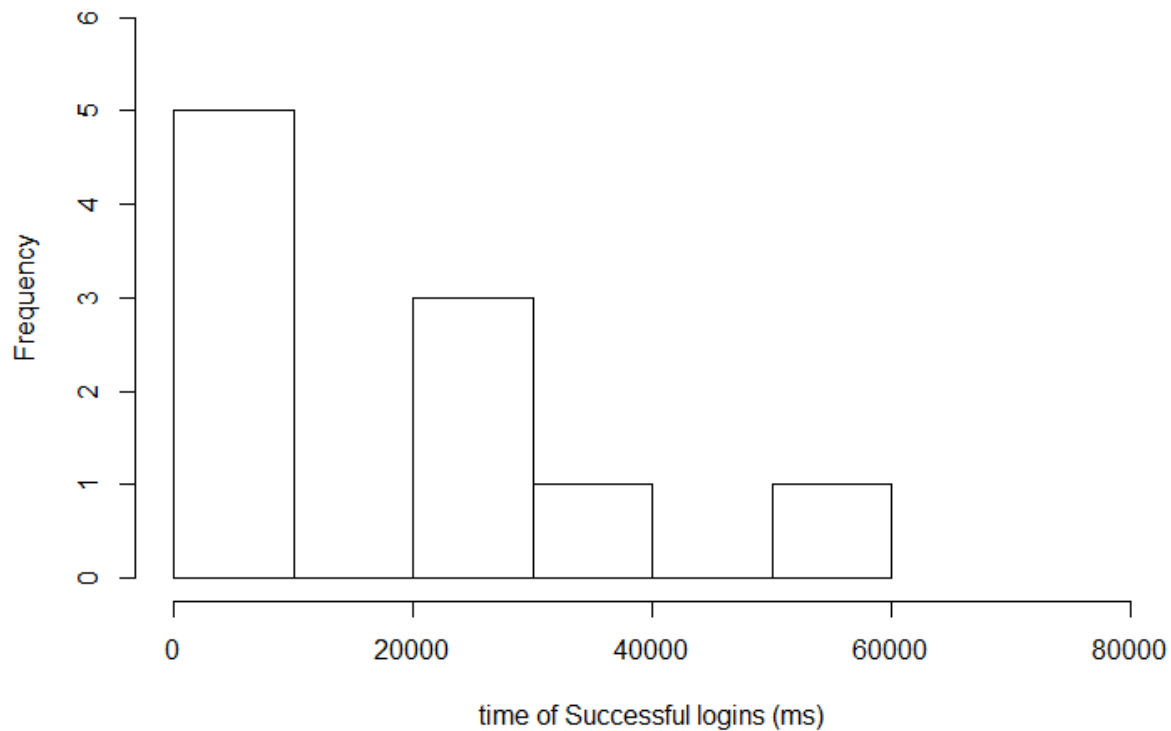




Overall, most people thought our system was secure and satisfying to use, despite having most of them think it was pretty hard to remember their passwords. Some of the people thought our

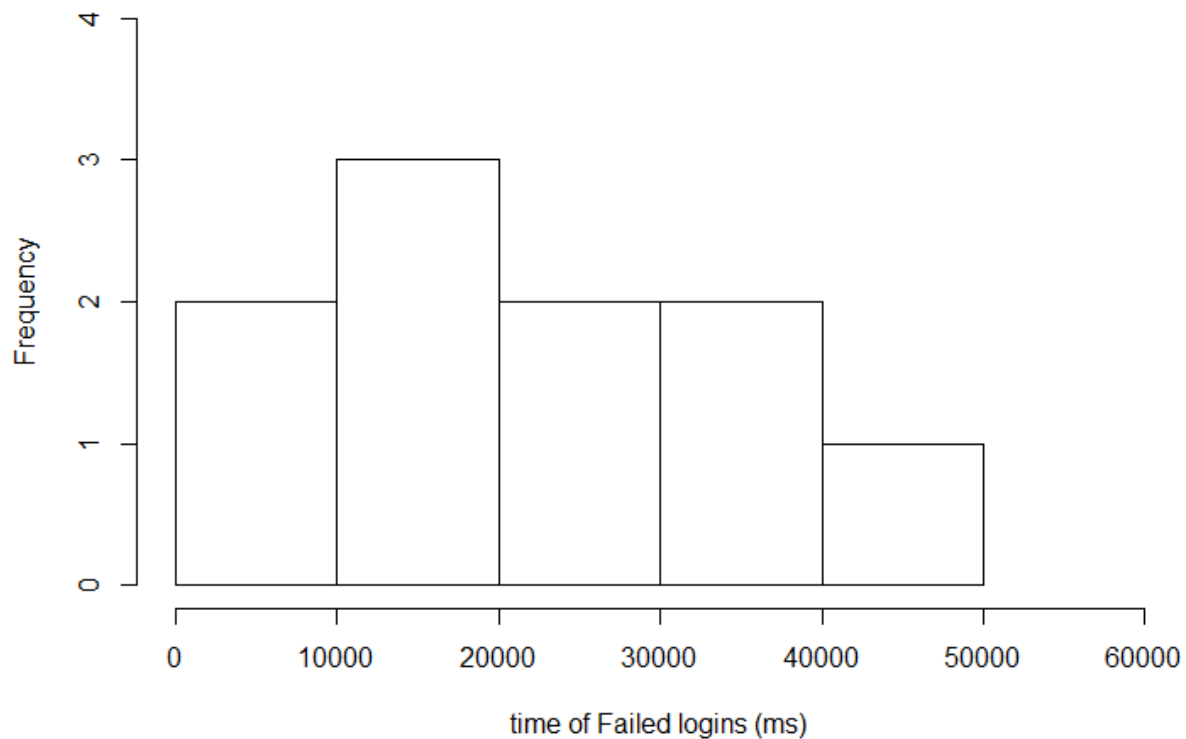
scheme was pretty complex and hard to follow without any help. We had organized the setting password stages and the entering password stages to come in unexpected order, hence confusing users and making them mix up the password entry stage with other sites (ie user enters correct password for one site into another site accidentally). This means we should have better indication on what site is about to get password entry, in order to make sure the user knows which password he needs to enter to get into the site. According to our survey data, we noticed that most people actually prefer to use our system rather than the text21 and the image21 system. Many of these people also think that our system is pretty interactive and fun. This might be a reason to why they prefer it over the text21/image21 system despite it potentially being more time consuming.

Histogram of time for Successful ColorAnimalPair Logins

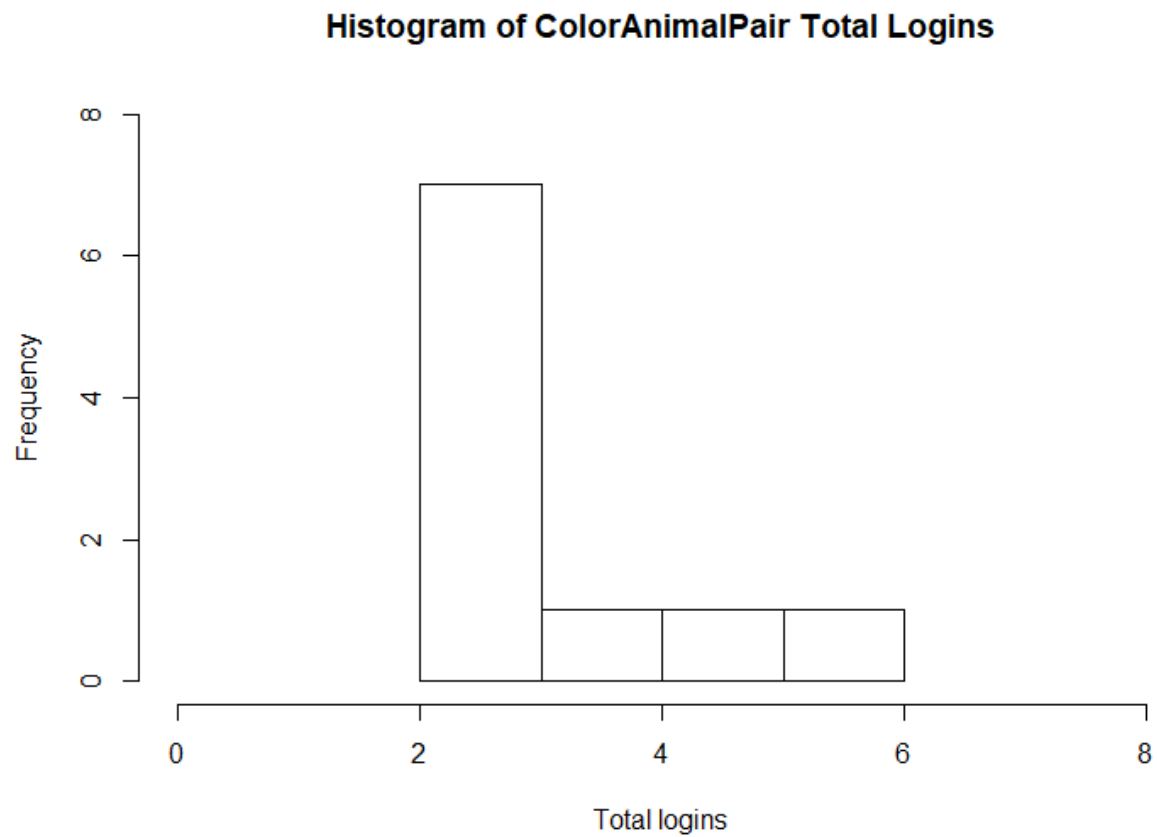


From this data we can tell that most users who were successful at logging in managed to login in under 10 seconds which is a little close to that of text21's data. At the same time, this data does show that is a little close to that of image21's data. However, we can deduce that our scheme wins the battle against image21 since with less users, we were able to attain more results under the 10 second margin. Also, I cannot say this scheme is better than text21's scheme since text21's scheme did not show to have any data past the 20-22 second margin, while our scheme does show to have data in the 50-60 second margin.

Histogram of time for Failed ColorAnimalPair Logins

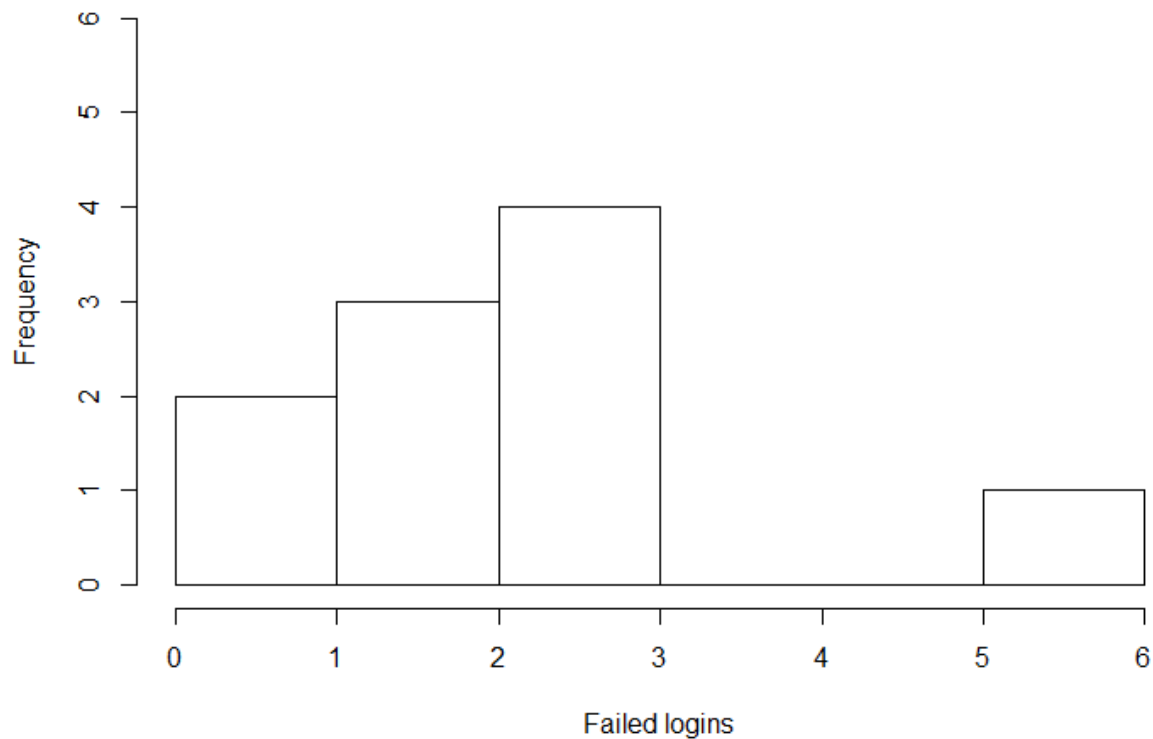


Sadly, this data doesn't show us much, since all it does is tell us that most of the values lie between 0-40 seconds when it comes to the time taken for a user to find himself getting a failed login. We can say that most values are between 15 and 20 seconds. However, the difference is by 1 value when comparing it the secondary majority. We cannot guarantee the outcome would be the same given we had more participants. If this data were accurate, then we have to conclude that both text21 and image21 win against our system when looking at this quality. However, I believe we need more data in order to make that decision.



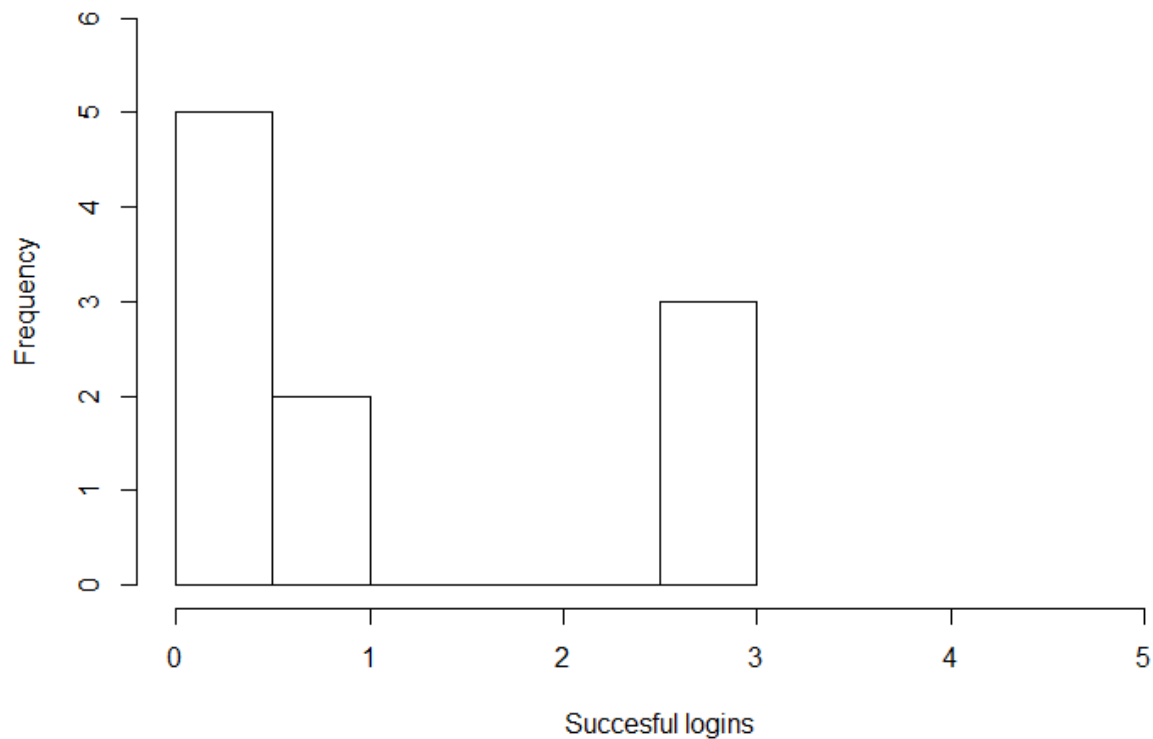
From this data, the first thing we notice is how much less logins we have in our scheme rather than the past 2 schemes. We must take this into account when measuring the data. Both of the past schemes had peaking login numbers in the 20 and 30 areas. Our scheme only peaks at 6.

Histogram of Failed ColorAnimalPair Logins

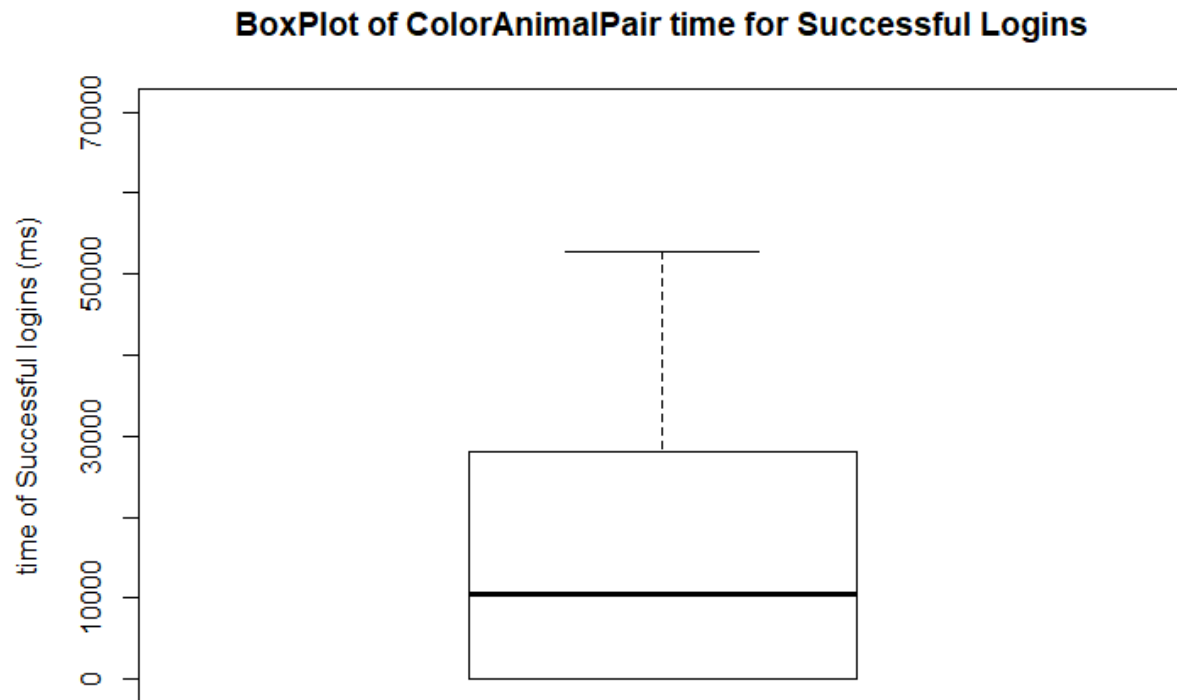


From this data, we notice that our failed logins are negatively skewed, while both our failed values from the past schemes were actually positively skewed. This shows us that our scheme gives us more login failures than text21. However, even though the image21 scheme is positively skewed. Our scheme proves to be better than it since we have most of our values being from 1-3. While most of the image21's positive skewness comes from 1-5. Yet again, we have more logins in general for the past systems. So it is harder for us to compare both systems.

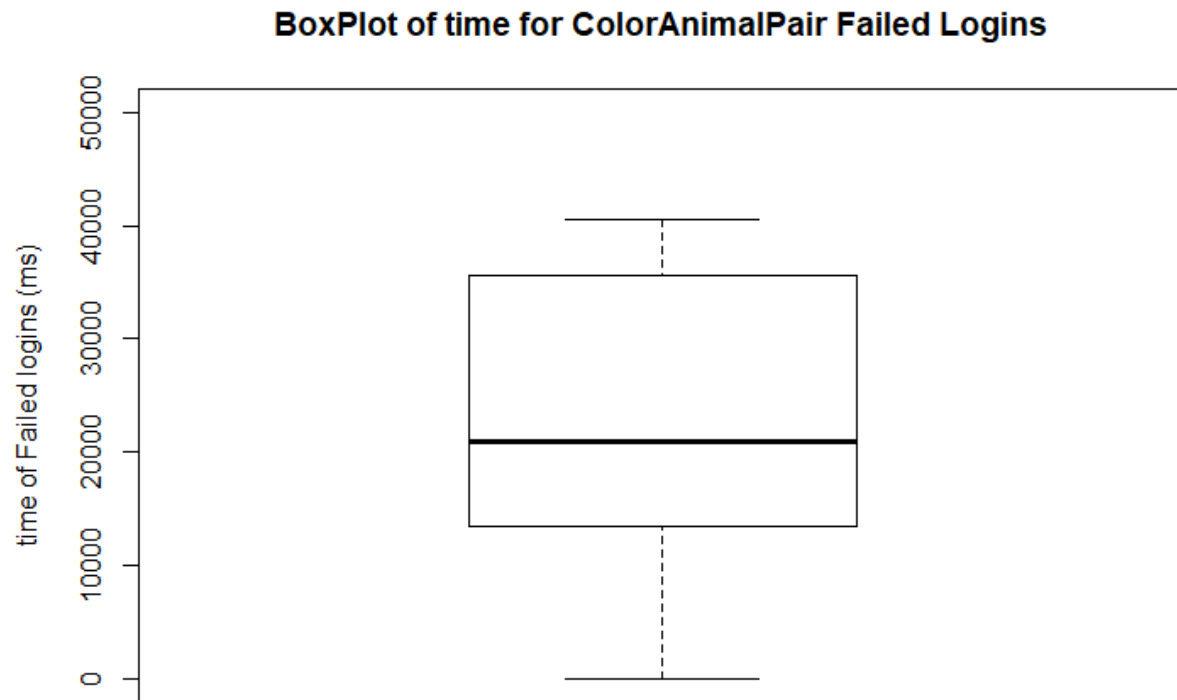
Histogram of Successful ColorAnimalPair Logins



From this data, we notice a lot of users failing to get any successful logins. We only had our participants go through our scheme once for 3 sites right after password creation. Hence, making the lack of successful logins a frequent sight. This can also show us how complex our system is as compared to the other 2 schemes. This is both a good and bad thing, as it means our system is highly secure, but this also makes our system very hard to navigate through (i.e. login). It is difficult to compare this graph with the other 2 graphs due to lack of data.



This shows us the median for successful login time to be 10,500 ms, which is almost as good as that of text21 (9063 ms). This is quite impressive, as it shows, this is potentially an enhanced version of image21, since they are both image related passwords and share some properties with each other. However, our system does have outliers that span all the way to almost 55.000 ms. Since we only had 10 users use our system. It is difficult for us to determine whether they really are outliers or if this is an illusion that has been created out of lack of users using the system and giving us appropriate enough data to study.



Since we have decided to compare our system to that of image21, we notice that image21 actually has a smaller median (Our scheme: 20916.5 ms, Image21: 14184 ms), meaning image21 is more usable than our scheme in terms of failed login time. Users are wasting less time with failed logins on image21 than ours. The difference is not huge, but will still be taken into account. Our system also shows to have slightly less distributed data than image21, making it a slightly more stable system.

All in all, from the data that we have, we might find ourselves in the middle of text21 and image21 in terms of usability. While our system proves to be less usable than that of text21, we have valuable information that can prove that our system is more interactive and fun. The same seems to apply when comparing the system with image21. This means that users would rather spend 20 seconds doing our scheme rather than do the image21/text21 scheme. We also believe that it would be easier to remember our scheme on a long term basis rather than text21 and image21 since our scheme does not generate gibberish data as the image21/text21 scheme do.

People realize what animals and colors are so it would be easier to remember that, than remember random characters or random parts of a picture. We also believe that a lot of the participants we were testing, did not have the same opportunity that the people from the text21/image21 had. Our participants rushed the process and did not put as much effort as we imagine the users of the other schemes did. The users that did put effort towards the scheme, (the people that I personally know and decided to take the system seriously) managed to do a very good job with the scheme. Despite that said, the majority of our users did agree that they would prefer our system rather than the text21/image21 system. So from that data, that might indicate that our system serves to be better than the 2 older schemes. This does go against some of our statistics. However, as mentioned before, we must always remember that we do not have as much users as the other schemes have, hence, making our data much less accurate. At the end of the day, we cannot be sure whether our system is actually better than the text21/image21 systems. When looking at this system in broader terms, we realize that users are always able to store their passwords. I imagine it would be far more convenient to use our system rather than random tiles and characters. Writing down the passwords for our system is easy since we recognize the words being used for the password, and in time, I can imagine that memorizing the password overtime would come quicker. This system might serve to be very useful when trying to serve a secure purpose and might rival normal password schemes.

Responsibilities:

Amr Shurman: Section 1.1 (page 2-3) (Went through both text21 and image21 schemes, and brainstormed all the flaws and discussed certain details. Documented the results.

Section 1.4 (page 5-15): (Used R to create graphs and statistics. Documented the results in detail, and discussed the reasoning to the phenomena. Came up with conclusions by using quantitative analysis.

Section 2.1 with Jacob: Came up with the idea of the scheme with Jacob, added some information and reasoning about our scheme on top of Eto's answer.

Section 2.4 with Marco: Came up with some questions with Marco, did some polishing to the existing questions

Section 2.5: Surveyed a few people on our scheme. Completed a survey

Section 2.6 (page 20-32): Used R to come up with statistics and graphs. Documented the results in detail, and discussed the reasoning to the phenomena. Came up with conclusions by using quantitative analysis.

Jacob Martin: Section 1.3 (page 3-5): Created the log file parser to extract relevant data from the password tester log files and put them into the new csv file

Section 2.1 with Amr: Came up with the idea of the scheme with Amr

Section 2.2 & Section 2.3 (page 16-19): Created the implementation of the groups password system for users to test it on

Section 2.5: Surveyed a few people on our scheme

Marco Paulo: Section 2.4 with Amr: Created the limeSurvey account, added questions/answers

Section 2.5: Surveyed a few people on our scheme

Eto-Oluwa Segun: Section 2.1 documentation (page 15-16): documented how the scheme works

Section 2.5: Surveyed a few people on our scheme

Consent Form

Title: COMP3008 Project 2

Date of ethics clearance: *January 18, 2019*

Ethics Clearance for the Collection of Data Expires: *April 30, 2019*

Project clearance number: 109939

This study aims to assess the usability of a computer user interface for the purpose of improving its design. This project is being completed as part of COMP3008 – Human Computer Interaction, an undergraduate course in Computer Science at Carleton University.

This study involves one session lasting at most 60 minutes. During the session, you will be asked to complete some tasks on a computer system, provide your opinion of the system, and offer feedback about how it can be improved. Data may be collected through observation, questionnaires, interviews, or tools to measure user actions on the interface (e.g., timing information or screen capturing the interaction). You will be provided with an anonymous username for use during the study and none of your personal accounts or data will be accessed.

You have the right to end your participation in the study at any time, for any reason, up until the end of the session. To withdraw, simply tell the researcher; no reason or explanation is necessary. If you

withdraw from the study, all information you have provided will be immediately destroyed. Withdrawal is not possible after you have completed the study.

All research data, including notes will be password-protected. When the analysis is completed, any hard copies of data (including any handwritten notes) will be kept in a cabinet in a locked office at Carleton University. Data will only be accessible by the experimenters and the research supervisor.

Questionnaire data will be collected using limesurvey, and will be stored on a password protected server at Carleton.

Since this is part of a class project, data will be kept until the end of the course. All data will be securely destroyed by June 2019. Electronic data will be erased and hard copies will be shredded.

The ethics protocol for this project was reviewed by the Carleton University Research Ethics Board (CUREB-B), which provided clearance to carry out the research. Should you have any ethical concerns with the study, please contact Dr. Bernadette Campbell, Chair, Carleton University Research Ethics Board-B (by phone: 613-520-2600 ext. 4085 or by email: ethics@carleton.ca).

Researchers' contact information:

Marcelo Paulo
Name Department Comp Sci
Carleton University
Tel: 819 700 1940
Email: official Carleton email address

marcelo.paulo@carleton.ca

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ☒ Yes ☐ No

I agree to participate in this user study:

[Signature]

Signature of participant

04/04/2019

Date

[Signature]

Signature of researcher

4/4/19

Date

Researchers' contact information:

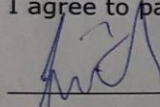
Marcio Paulo, comp Sci
Name Department
Carleton University
Tel: 819 700 1940
Email: official Carleton email address

Supervisor contact information:

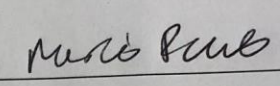
Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ☒ Yes ☐ No

I agree to participate in this user study:


Signature of participant

4/4/19
Date


Signature of researcher

4/4/19
Date

Researchers' contact information:

Marcio Paulo, Comp Sci
Name Department
Carleton University
Tel: 819 760 1940
Email: official Carleton email address

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ☒ Yes ☐ No

I agree to participate in this user study:

[Signature]
Signature of participant

Apr. 14th, 2019
Date

Marcio Paulo
Signature of researcher

4/4/19
Date

Researchers' contact information:

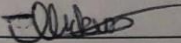
Amr Shurman
Name Department School of Comp Sci
Carleton University
Tel: 819 319 8541
Email: official Carleton email address
amrshurman@mail.carleton.ca

Supervisor contact information:

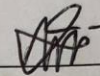
Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ☒ Yes ☐ No

I agree to participate in this user study:


Signature of participant

4/4/2019
Date


Signature of researcher

4/4/19
Date

Researchers' contact information:

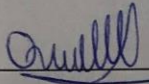
~~MAQSOOD~~ Amr Shurman
Name Department school of comp science
Carleton University
Tel: 919 319 8541
Email: official Carleton email address
amrshurman@gmail.com (carleton.ca)

Supervisor contact information:


Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ☒ Yes ☐ No

I agree to participate in this user study:


Signature of participant

04-04-2019
Date


Signature of researcher

4/4/2019
Date

Researchers' contact information:

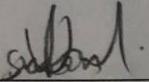
ITC AMY Sherman
Name Department School of comp science
Carleton University
Tel: 819 319 8541
Email: official Carleton email address
amrsherman@carlton.ca

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ☒ Yes ☐ No


I agree to participate in this user study:



Signature of participant

Apr 1 / 4th / 2019

Date



Signature of researcher

4/4/2019

Date

Researchers' contact information:

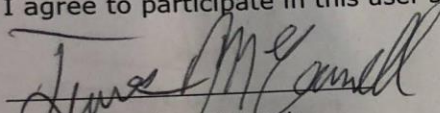
Amr Shurman
Name Department school of comp sci
Carleton University
Tel: 2193198541
Email: official Carleton email address
amrshurman@carleton.ca

Supervisor contact information:


Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ☒ Yes ☐ No

I agree to participate in this user study:


Signature of participant

09/09/19
Date


Signature of researcher

4/4/19
Date

Researchers' contact information:


1 Jacob Martin
Name Department: School of Computer Science
Carleton University
Tel:
Email: official Carleton email address
jacob.j.martin@carleton.ca

Supervisor contact information:

Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ☒ Yes ☐ No

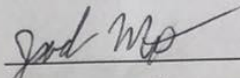
I agree to participate in this user study:



Signature of participant

4/4/2019

Date



Signature of researcher

4/4/19

Date

Researchers' contact information:

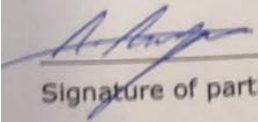
Jacob Martin
Name Department School of Computer Science
Carleton University
Tel:
Email: official Carleton email address
jacobj.martin@carleton.ca

Supervisor contact information:

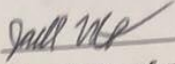
Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ☒ Yes ☐ No

I agree to participate in this user study:


Signature of participant

4/4/2019
Date


Signature of researcher

4/4/19
Date

Researchers' contact information:

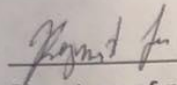
Jacob Martin -
Name Department
Carleton University
Tel:
Email: official Carleton email address
jacob.j.martin@carleton.ca

Supervisor contact information:

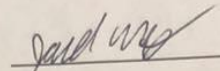
Sana Maqsood
School of Computer Science
Carleton University
Tel: 613-520-2600 x 8753
Email: sana.maqsood@carleton.ca

Do you agree to have your computer screen recorded: ☒ Yes ☐ No

I agree to participate in this user study:


Signature of participant

04/04/2019
Date


Signature of researcher

4/4/19
Date