Password Authentication Project 2

Quantitative Usability Evaluation Report

Team Rainbow - Group 28

Matthew Pacitto	100650012
Roy Xia	101009419
Qudus Agbalaya	101007487
Janielle Scarlett	101003398
Elijah Doern	100981549

Part 1 - Sample Data and Descriptive Statistics

Section 1 - Text21 and Imagept21 Password Scheme Reflections

We explored two different password schemes, *Text21* and *Imagept21*, accessible from the Web (link: https://mvp.soft.carleton.ca/svp3008). The schemes are designed as follows:

Text21: Passwords are randomly assigned, 5 letters long, character set of a-z and 0-9 aka “alphanumeric.”

Imagept21: Passwords are also randomly assigned as an unordered choice of 5 random tiles on an image split into 48 tiles.

Each password scheme included a testing framework where the user had to create three different passwords simulating different websites: Email, Banking, and Shopping. After a password was created, the user could practice that password as much as they liked. We explored this process for what we considered a ‘reasonable’ amount of time, practicing for a few minutes at most for each password. After that, we felt emotionally at a limit for ‘caring’ to practice a password. The testing framework then quizzes you to see if you remember your passwords for each website, and records performance data.

We performed two ‘runs’ of each password testing framework. In all cases, we did not write down our passwords. Writing down our passwords presents its own (albeit local) security vulnerability, and we expected it would greatly increase successful password login, while reducing password login time (having to find your Post-It note, reading it, etc). On our first run, our performance and memorability of passwords was very low for both Text21 and Imagept21. We noticed easily the effect of list primacy. We remembered - or almost remembered - our first passwords (Email website) but we didn’t even feel close to remembering passwords after that.

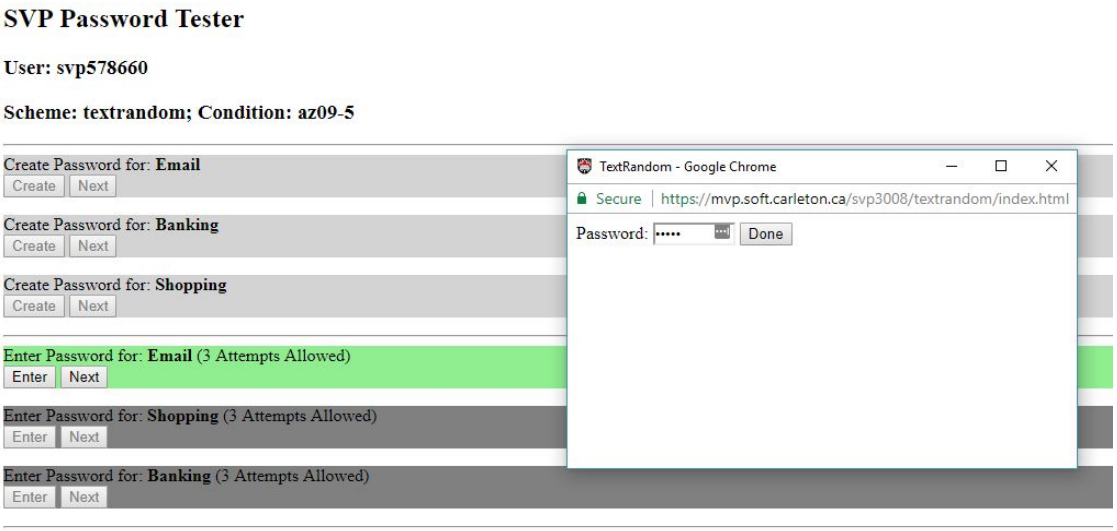


Figure 1. Screenshot of Text21 password scheme testing framework.

On our second run of both password schemes, we performed better on both. We hypothesize that at least some of this performance improvement can be accounted by increased familiarity with the system and testing framework itself. The user who provided the screenshot of Figure 1 also ‘got lucky’ with the randomly assigned Text21 passwords on the second run. Two out of three were letters only, making them both weak and easier to remember. On the second run of Imagept21, the user who provided the screenshot of Figure 2 utilized a new cognitive strategy for aiding in memorization. They tried to use relative “compass” and “coordinate” labelling for their passwords.

In Figure 2, the user later reflected that he remembered the password by memorizing something like: “The tile northeast of the bottom-right corner; The tile northeast of the center hood of the truck.” As well, groups of adjacent tiles provided a better cognitive ability to ‘chunk’ the information. One didn’t need a cognitive “coordinate” for each of the three tiles grouped in Figure 2, one only needed to remember the shape of the grouping and the cognitive “coordinate” of one starter tile. With that approach, three tiles are remembered nearly for the load of one.

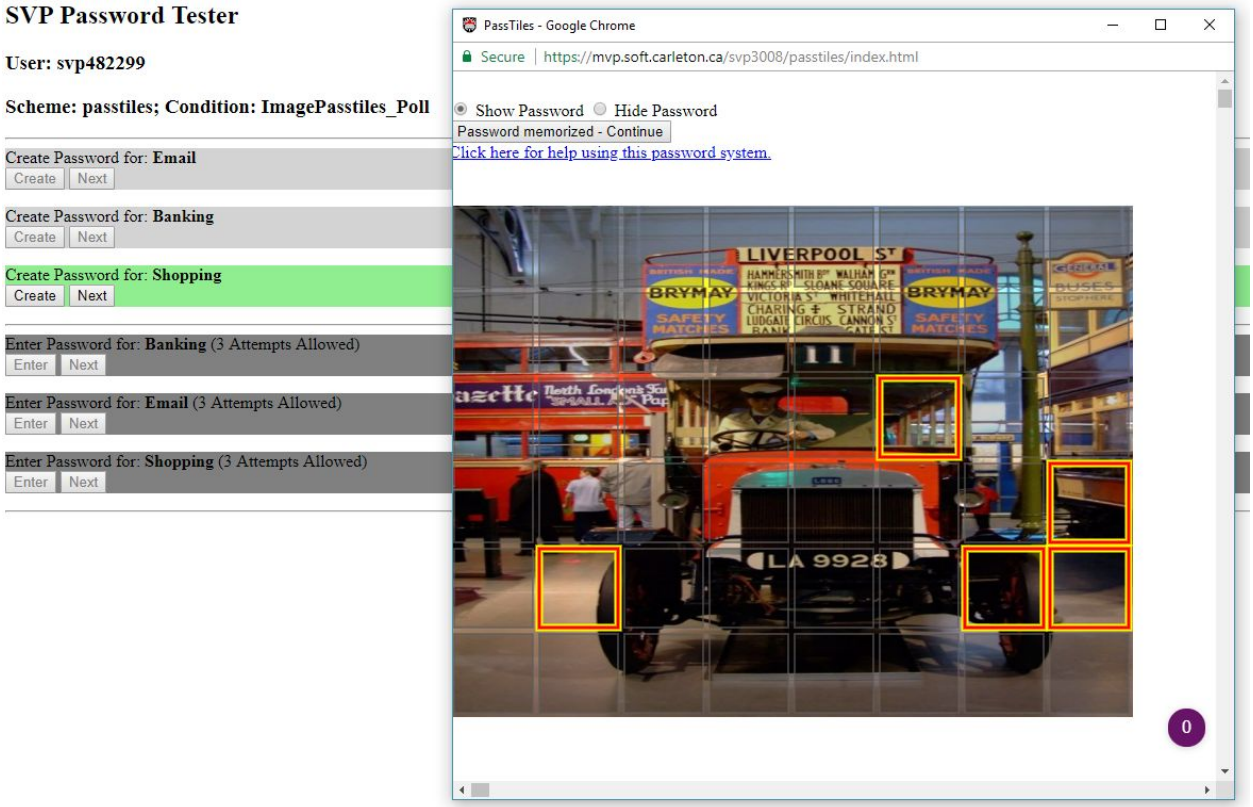


Figure 2. Screenshot of Imagept21 password scheme testing framework.

Overall, our own reflections of the two password schemes were that neither were easier to remember, or 'better' than the other. We expected that Imagept21 would be the scheme with easier to remember passwords, and the use of cognitive strategies mentioned above seemed to support that. Randomly assigned alphanumeric passwords in Text21 were very difficult to remember without writing down, and they are only 5 characters long! Imagine trying to use a text based system that gave out random 20 character passwords. It would be impossible without writing it down, or using a password manager, or if the user got 'lucky' and the password was very easier to remember (letters only, numbers only, dictionary, etc), and that latter scenario generally means the password is weak.

It seems at first glance that Imagept21 will have better memorability, due to the aforementioned tricks a user can employ such as chunking of image tiles, cognitive "coordinate" systems, and so on. However, similar strategies could be used for Text21 if one tried: turn every character into a dictionary word, and create a story for oneself. For example, given the random password 't8fj3' the user could encode with 'Taste Eight Figs Just Thrice' or some other silly phrase. As Text21 or Image21 had its password space increased (longer passwords, more tiles on a larger tile board), or as the number of needed passwords increased, both schemes would be expected to show degrading performance. The cognitive strategies employed in Imagept21 would be expected to degrade as well, if for example many of the image tileboards looked similar to one another, or if the user needed to remember so many tiles that even chunking could not help them.

Section 2 - Password Scheme Log Processors: log-processor.R and stats-graph-builder.R

"Report: Documentation for your log data processing software, including high-level explanation and pseudocode for your approach, and the documented source code. Also provide the resulting data in CSV format."

High-Level Description and Pseudocode

We developed a script in R to process two aggregate log files of user events in Text21 and Imagept21: ***log-processor.R***. Since both password schemes used the same structured CSV, we only needed to write one script to process both log files. In theory, if new password schemes were tested and followed the same structure and format conventions, the script would not need to be updated.

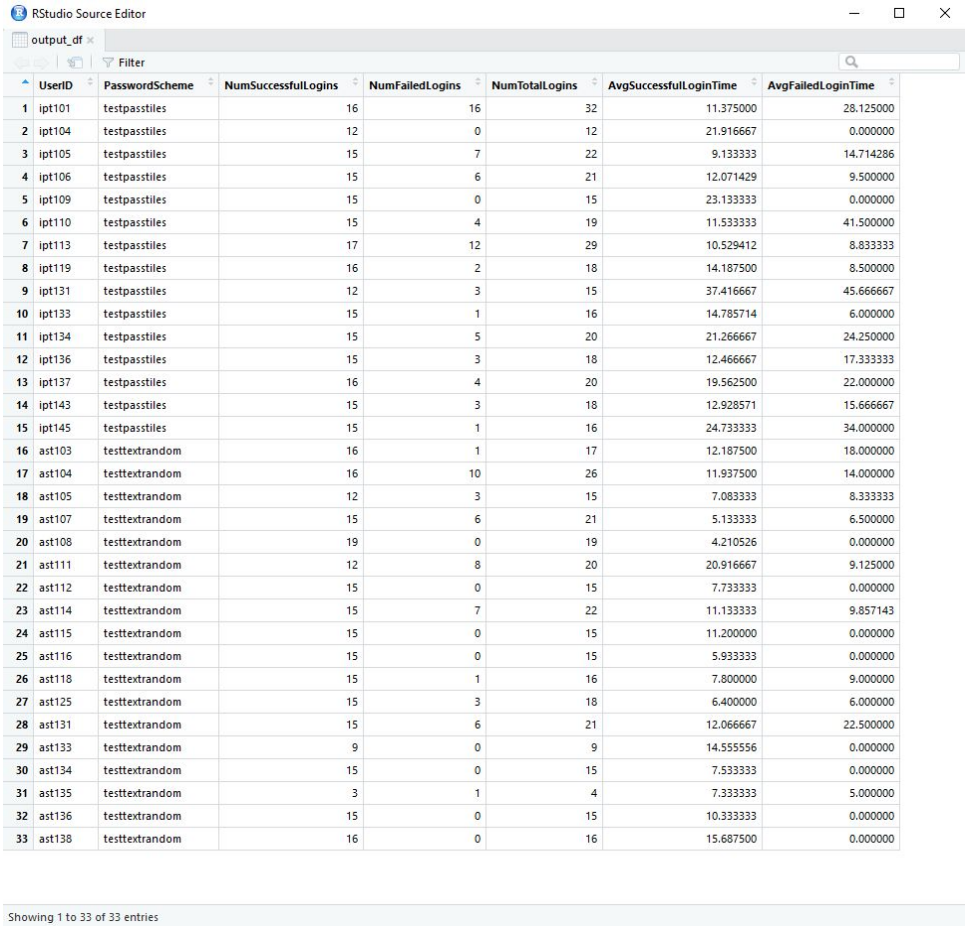
By default, the script is from our Git project repository, where the working directory is set to the location of the source file. The repository also includes input and output subdirectories, where the input directories contain a copy of the log files. The script reads in the CSV data as an R data frame, and through the use of a multitude of intermediate data frames, subsets, and vectors, creates a final data frame (Figure 3). The final data frame is then exported as a CSV file to the output directory.

A second script, ***stats-graph-builder.R***, was developed to take as input the resulting CSV file of ***log-processor.R***. This script was developed with the expectation that a user will run ***log-processor.R*** and then run ***stats-graph-builder.R*** on the output. This second script takes in a CSV file and computes the following statistics and graphs:

- The mean, median, and standard deviation of logins per user (total, successful, and unsuccessful)
- The mean, median, and standard deviation of login times per user (successful and unsuccessful)
- Density histograms of the number of logins per user (total, successful, unsuccessful)
- Density histograms of login times per user (successful and unsuccessful)
- Boxplots of login times per user (successful and unsuccessful)

The computed statistics are stored in a data frame (Figure 4) and exported as a CSV file. The graphs (see Section 3) are exported as PNG images.

A copy of our Git project repository has been bundled with this report, which includes the documented source code and a readme instructing users how to run the scripts manually. As well, the pseudocode approaches for ***log-processor.R*** and ***stats-graph-builder.R*** are shown in Figures 5 and 6 respectively.



RStudio Source Editor

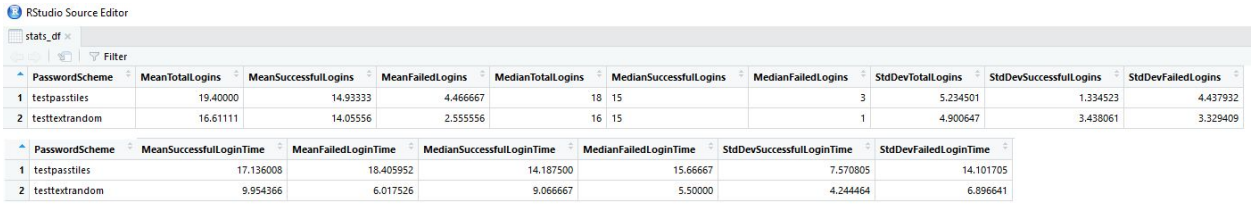
output_df

Filter

	UserID	PasswordScheme	NumSuccessfulLogins	NumFailedLogins	NumTotalLogins	AvgSuccessfulLoginTime	AvgFailedLoginTime
1	ipt101	testpasstiles	16	16	32	11.375000	28.125000
2	ipt104	testpasstiles	12	0	12	21.916667	0.000000
3	ipt105	testpasstiles	15	7	22	9.133333	14.714286
4	ipt106	testpasstiles	15	6	21	12.071429	9.500000
5	ipt109	testpasstiles	15	0	15	23.133333	0.000000
6	ipt110	testpasstiles	15	4	19	11.533333	41.500000
7	ipt113	testpasstiles	17	12	29	10.529412	8.833333
8	ipt119	testpasstiles	16	2	18	14.187500	8.500000
9	ipt131	testpasstiles	12	3	15	37.416667	45.666667
10	ipt133	testpasstiles	15	1	16	14.785714	6.000000
11	ipt134	testpasstiles	15	5	20	21.266667	24.250000
12	ipt136	testpasstiles	15	3	18	12.466667	17.333333
13	ipt137	testpasstiles	16	4	20	19.562500	22.000000
14	ipt143	testpasstiles	15	3	18	12.928571	15.666667
15	ipt145	testpasstiles	15	1	16	24.733333	34.000000
16	ast103	testtextrandom	16	1	17	12.187500	18.000000
17	ast104	testtextrandom	16	10	26	11.937500	14.000000
18	ast105	testtextrandom	12	3	15	7.083333	8.333333
19	ast107	testtextrandom	15	6	21	5.133333	6.500000
20	ast108	testtextrandom	19	0	19	4.210526	0.000000
21	ast111	testtextrandom	12	8	20	20.916667	9.125000
22	ast112	testtextrandom	15	0	15	7.733333	0.000000
23	ast114	testtextrandom	15	7	22	11.133333	9.857143
24	ast115	testtextrandom	15	0	15	11.200000	0.000000
25	ast116	testtextrandom	15	0	15	5.933333	0.000000
26	ast118	testtextrandom	15	1	16	7.800000	9.000000
27	ast125	testtextrandom	15	3	18	6.400000	6.000000
28	ast131	testtextrandom	15	6	21	12.066667	22.500000
29	ast133	testtextrandom	9	0	9	14.555556	0.000000
30	ast134	testtextrandom	15	0	15	7.533333	0.000000
31	ast135	testtextrandom	3	1	4	7.333333	5.000000
32	ast136	testtextrandom	15	0	15	10.333333	0.000000
33	ast138	testtextrandom	16	0	16	15.687500	0.000000

Showing 1 to 33 of 33 entries

Figure 3. Screenshot of output data frame in log-processor.R taken from RStudio.



RStudio Source Editor

stats_df

Filter

	PasswordScheme	MeanTotalLogins	MeanSuccessfulLogins	MeanFailedLogins	MedianTotalLogins	MedianSuccessfulLogins	MedianFailedLogins	StdDevTotalLogins	StdDevSuccessfulLogins	StdDevFailedLogins
1	testpasstiles	19.40000	14.93333	4.466667	18	15	3	5.234501	1.334523	4.437932
2	testtextrandom	16.61111	14.05556	2.555556	16	15	1	4.900647	3.438061	3.329409

	PasswordScheme	MeanSuccessfulLoginTime	MeanFailedLoginTime	MedianSuccessfulLoginTime	MedianFailedLoginTime	StdDevSuccessfulLoginTime	StdDevFailedLoginTime
1	testpasstiles	17.136008	18.405952	14.187500	15.66667	7.570805	14.101705
2	testtextrandom	9.954366	6.017526	9.066667	5.50000	4.244464	6.896641

Figure 4. Photoedited screenshot of output data frame in stats-graph-builder.

```
SET path variables:
        work_dir = directory of this source file
        input_dir = work_dir + "/input/"
        output_dir = work_dir + "/output/"
SET data header labels for log_data:
        log_headers = ["EventID", "Timestamp", "UserID", "PasswordSite" , "PasswordScheme",
                       "PasswordSet", "UserAction", "ActionResult", "ResponseInfo"]
file_list = GET list of log file paths

FOR EACH i in length(file_list):
        log_data[i] = Read data in from CSV at input_dir
        SET data header labels of log_data[i] to log_headers
        log_users = Unique "UserID" rows of log_data[i]
END

FOR EACH j in length(log_users):
        good_logins = 0
        bad_logins = 0
        k = 0
        FOR EACH k in length(log_data):
                pw_scheme = GET UNIQUE entries of column "PasswordScheme" in log_data[k]
                good_logins = COUNT ROWS of column "ActionResult" in log_data[k]
                                WHERE "UserAction" == "login" AND "ActionResult" == "success"
                bad_logins = COUNT ROWS of column "ActionResult" in log_data[k]
                                WHERE "UserAction" == "login" AND "ActionResult" == "failure"
                total_logins = good_logins + bad_logins
                login_events = GET SUBSET of log_data[k] WHERE "UserID" == log_users[j] AND
                                ("UserAction" == "enter" AND "ActionResult" == "start" OR
                                "UserAction" == "login" AND "ActionResult" == "success" OR
                                "UserAction" == "login" AND "ActionResult" == "failure")
                IF NUM ROWS login_events > 0:
                        l = 0
                        good_login_time = NULL
                        bad_login_time = NULL
                        FOR EACH l in length(login_events):
                                IF columns "UserAction" of login_events[l] == "enter" AND
                                    "ActionResult" == "start"
                                IF columns "UserAction" of login_events[l+1] == "login" AND
                                        "ActionResult" == "success"
                                        good_login_time[l] = COMPUTE time difference in SECONDS between
                                                             login_events[l] and login_events[l+1] on
                                                             column "Timestamp"
                                ENDIF

                                IF columns "UserAction" of login_events[l+1] == "login" AND
                                        "ActionResult" == "failure"
                                        bad_login_time[l] = COMPUTE time difference in SECONDS between
                                                             login_events[l] and login_events[l+1] on
                                                             column "Timestamp"
                                ENDIF
                                ENDIF
                        END
                ENDIF
        END

        num_good_logins[j] = good_logins
        num_bad_logins[j] = bad_logins
        num_total_logins[j] = total_logins

        IF good_login_time == NULL
                mean_good_login_time[j] = 0
        ELSE
                mean_good_login_time[j] = MEAN of good_login_time
        ENDIF

        IF bad_login_time == NULL
                mean_bad_login_time[j] = 0
        ELSE
                mean_bad_login_time[j] = MEAN of bad_login_time
        ENDIF
END

output_table = CREATE TABLE of log_users, pw_scheme, num_good_logins, num_bad_logins, num_total_logins,
                               mean_good_login_time, mean_bad_login_time
WRITE output_table to CSV file at output_dir
```

Figure 5. Pseudocode for the R script log-processor.R

```
SET path variables:
        work_dir = directory of this source file
        data_dir = work_dir + "/output/"

data_frame = Read data in from CSV at data_dir

num_schemes = GET UNIQUE entries of data_frame from column "PasswordScheme"

// Note that this pseudocode is meant to run on a CSV data file produced by log-processor
// Therefore it has a specific structure to it's CSV data column header labels, used throughout:
// data_headers = ["UserID", "PasswordScheme", "NumSuccessfulLogins", "NumFailedLogins",
//                 "NumTotalLogins", "AvgSuccessfulLoginTime", "AvgFailedLoginTime"]

num_histograms = 5

FOR EACH i in length(num_schemes):
        data_scheme = SUBSET of data_frame WHERE column "PasswordScheme" == num_schemes[i]

        mean_logins_total[i] = COMPUTE MEAN of data_scheme[i] WHERE column is "NumTotalLogins"
        mean_logins_success[i] = COMPUTE MEAN of data_scheme[i] WHERE column is "NumSuccessfulLogins"
        mean_logins_failure[i] = COMPUTE MEAN of data_scheme[i] WHERE column is "NumFailedLogins"

        median_logins_total[i] = COMPUTE MEDIAN of data_scheme[i] WHERE column is "NumTotalLogins"
        median_logins_success[i] = COMPUTE MEDIAN of data_scheme[i] WHERE column is "NumSuccessfulLogins"
        median_logins_failure[i] = COMPUTE MEDIAN of data_scheme[i] WHERE column is "NumFailedLogins"

        sd_logins_total[i] = COMPUTE STANDARD DEVIATION of data_scheme[i] WHERE column is "NumTotalLogins"
        sd_logins_success[i] = COMPUTE STANDARD DEVIATION of data_scheme[i] WHERE column is "NumSuccessfulLogins"
        sd_logins_failure[i] = COMPUTE STANDARD DEVIATION of data_scheme[i] WHERE column is "NumFailedLogins"

        mean_login_time_success[i] = COMPUTE MEAN of data_scheme[i] WHERE column is "AvgSuccessfulLoginTime"
        mean_login_time_fail[i] = COMPUTE MEAN of data_scheme[i] WHERE column is "AvgFailedLoginTime"

        median_login_time_success[i] = COMPUTE MEDIAN of data_scheme[i] WHERE column is "AvgSuccessfulLoginTime"
        median_login_time_fail[i] = COMPUTE MEDIAN of data_scheme[i] WHERE column is "AvgFailedLoginTime"

        sd_login_time_success[i] = COMPUTE STANDARD DEVIATION of data_scheme[i] WHERE column is "AvgSuccessfulLoginTime"
        sd_login_time_success[i] = COMPUTE STANDARD DEVIATION of data_scheme[i] WHERE column is "AvgFailedLoginTime"

        hist_logins_total[i] = COMPUTE HISTOGRAM of data_scheme[i] WHERE column is "NumTotalLogins"
        EXPORT hist_logins_total[i] to PNG bitmap file in data_dir

        hist_logins_success[i] = COMPUTE HISTOGRAM of data_scheme[i] WHERE column is "NumSuccessfulLogins"
        EXPORT hist_logins_success[i] to PNG bitmap file in data_dir

        hist_logins_fail[i] = COMPUTE HISTOGRAM of data_scheme[i] WHERE column is "NumFailedLogins"
        EXPORT hist_logins_fail[i] to PNG bitmap file in data_dir

        hist_login_time_success[i] = COMPUTE HISTOGRAM of data_scheme[i] WHERE column is "AvgSuccessfulLoginTime"
        EXPORT hist_login_time_success[i] to PNG bitmap file in data_dir

        hist_login_time_fail[i] = COMPUTE HISTOGRAM of data_scheme[i] WHERE column is "AvgFailedLoginTime"
        EXPORT hist_login_time_fail[i] to PNG bitmap file in data_dir

        boxp_login_time_success[i] = SUBSET of data_scheme[i] WHERE column is "AvgSuccessfulLoginTime"
        boxp_login_time_fail[i] = SUBSET of data_scheme[i] WHERE column is "AvgFailedLoginTime"
END

COMPUTE BOXPLOT of boxp_login_time_success
EXPORT BOXPLOT to PNG bitmap file in data_dir

COMPUTE BOXPLOT of boxp_login_time_fail
EXPORT BOXPLOT to PNG bitmap file in data_dir

output_table = CREATE TABLE of num_schemes, mean_logins_total, mean_logins_success, mean_logins_fail,
                               median_logins_total, median_logins_success, median_logins_fail,
                               sd_logins_total, sd_logins_success, sd_logins_fail,
                               mean_login_time_success, mean_login_time_fail,
                               median_login_time_success, median_login_time_fail,
                               sd_login_time_success, sd_login_time_fail)

WRITE output_table to CSV file at output_dir
```

Figure 6. Pseudocode for the R script stats-graph-builder.R

Section 3 - Password Scheme Statistical Usability Comparison

Imagept21 had the highest (or in one case equal) mean and median number of logins per user for total (Table 1), successful (Table 2), and failed (Table 3) cases. Drawing meaning from this result is difficult based on the tables alone. Both density curves for Imagept21 and Text21 for total logins (Figure 7) are similar, unimodal, and look almost normal. However, the distribution of Imagept21 is clustered a little more tightly around the mean, whereas for Text21 it is slightly more spread out. This spread can be investigated further by looking at successful and failed number of logins.

Password Scheme	Mean Total Logins	Median Total Logins	Std. Dev. Total Logins
Imagept21	19.40	18.00	5.23
Text21	16.61	16.00	4.90

Table 1. Mean, median, and standard deviation of Total User Logins

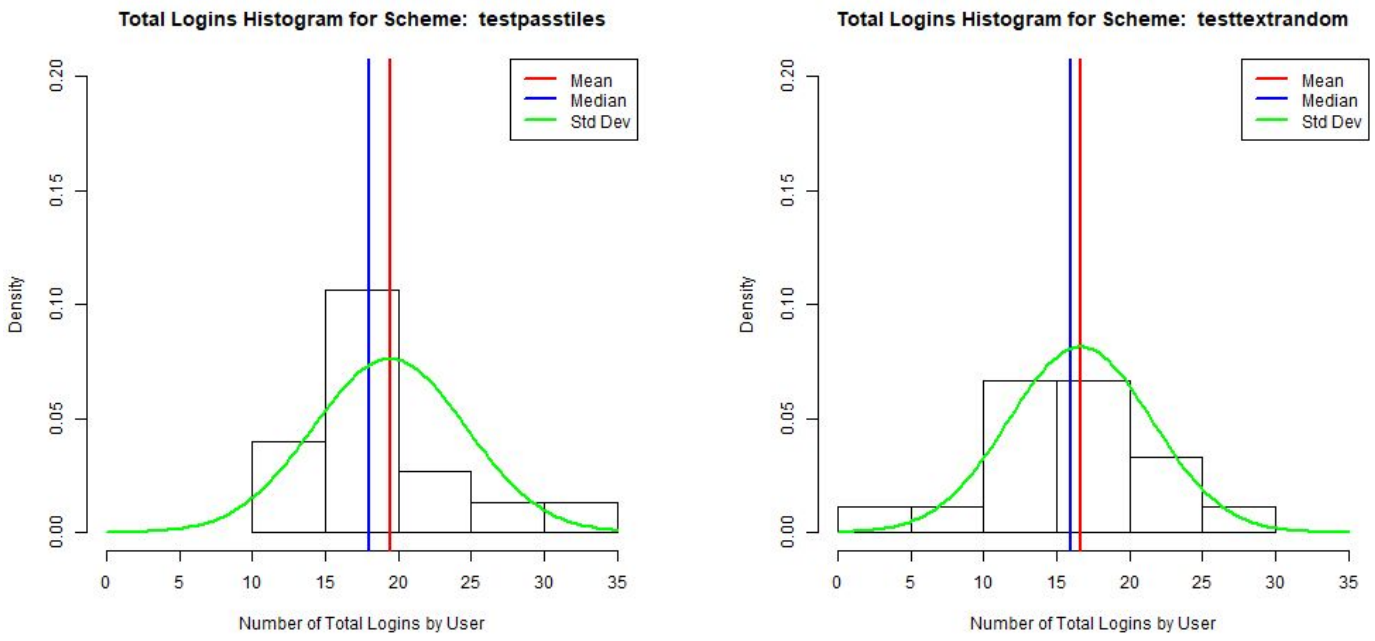


Figure 7. Histogram of Total Logins by User for Imagept21 (left) and Text21 (right)

In Table 2, for successful number of logins, we can see initially that the mean and median values are close to identical. However, a look at the related Figure 8 shows a much different distribution. Imagept21 has a very tightly clustered distribution, and thus a very low standard deviation. Text21, on the other hand, has a similar median number of successful logins, but quite a few users that rest beyond first standard deviation. For Text21, in Figure 8, there also appears to be an outlier who hardly logged in at all (3 logins compared to a

mean of 14.05). Even with this outlier removed, the distribution curve for successful logins for Text21 remains quite spread out. These results may indicate that users tend to have more consistent, successful logins with Imagept21 than with Text21.

Password Scheme	Mean Successful Logins	Median Successful Logins	Std. Dev. Successful Logins
Imagept21	14.93	15.00	1.33
Text21	14.05	15.00	3.43

Table 2. Mean, median, and standard deviation of Successful User Logins

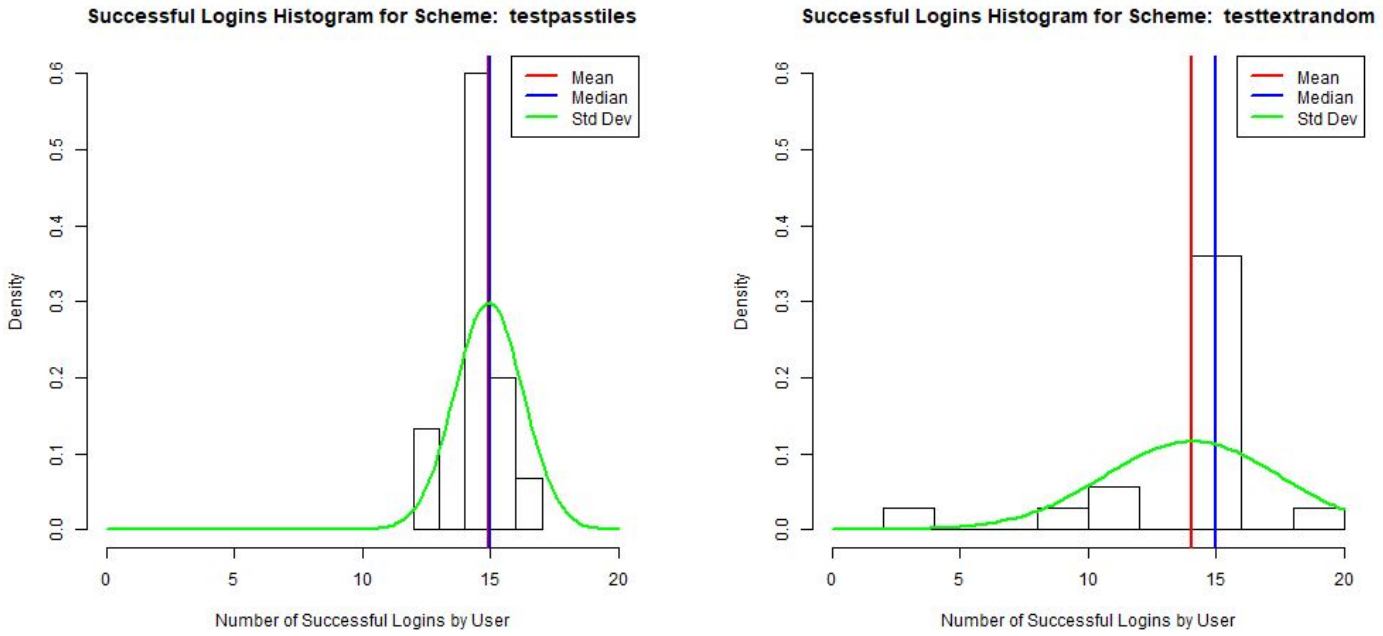


Figure 8. Histogram of Successful Logins by User for Imagept21 (left) and Text21 (right)

Statistics for the number of failed logins by user differed more than total or successful logins (Table 3). Even without a graph, we can see that Imagept21 had a higher mean and median failure rate. However, for both Imagept21 and Text21, the data on number of failed logins sport very large standard deviations compared to their means, suggesting very non-normal distributions. This suggestion is confirmed in Figure 9. In this instance, the reverse pattern has emerged compared to number of successful logins. For Imagept21, the distribution is very spread out compared to the distribution of Text21. Text21 users tended to have very few failures, while Imagept21 users tended to have few failures as well, but a minority of users experienced many failures. These results may be an early indication that Imagept21 users experience a higher failure rate and that some Imagept21 users fail “more spectacularly” than Text21 users. However, since these distributions appear non-normal, a larger dataset may change the patterns.

Password Scheme	Mean Failed Logins	Median Failed Logins	Std. Dev. Failed Logins
Imagept21	4.46	3.00	4.43
Text21	2.55	1.00	3.32

Table 3. Mean, median, and standard deviation of Failed User Logins

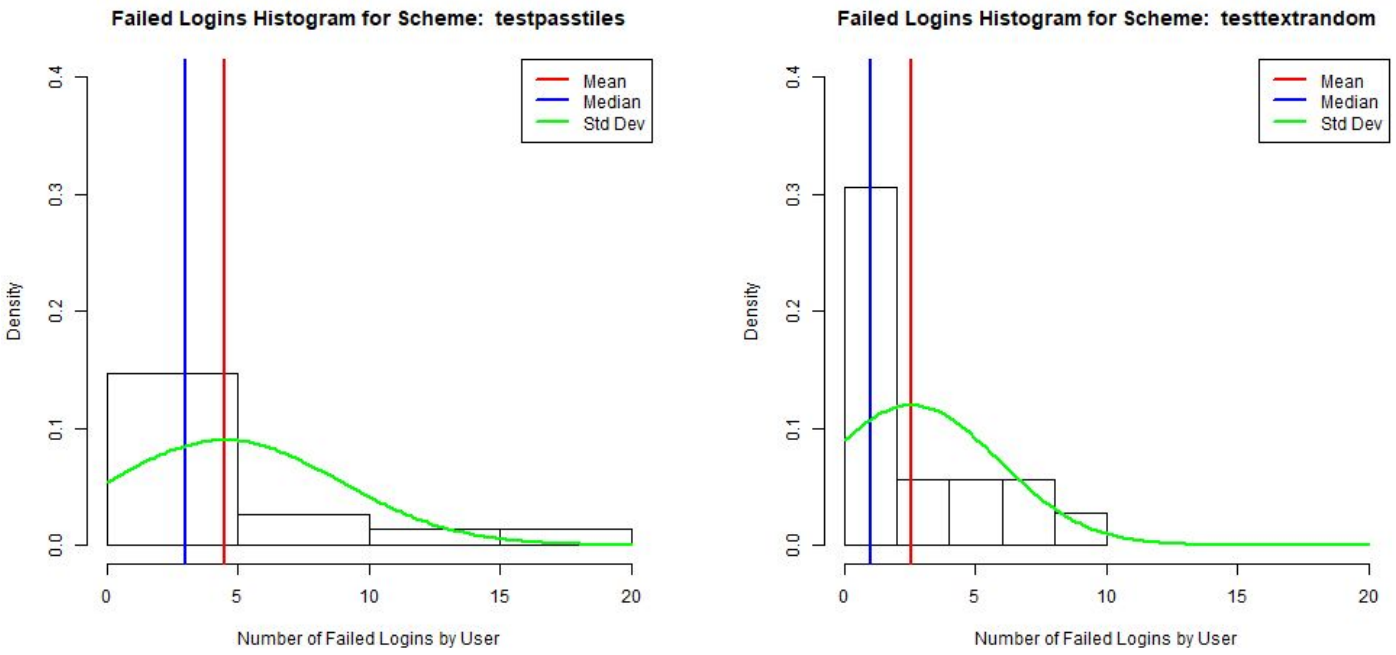


Figure 9. Histogram of Failed Logins by User for Imagept21 (left) and Text21 (right)

It comes as no surprise in our interpretation, after taking into account successful and failed logins, that the statistics for total logins seem difficult to analyze. For successful logins, Text21 showed a highly spread distribution, and for failed logins, Imagept21 showed a highly spread distribution. Once the events (and their sample sizes) were combined, a more normal looking distribution emerged. It is difficult to apply an assessment to the usability of Text21 or Imagept21 with numbers of logins. What reasons could there be for the patterns observed, from the user perspective? We posit from this first statistic that users tend to succeed more consistently with Imagept21, but when they fail at remembering their passwords, they tend to “fail harder” compared to Text21.

Password Scheme	Mean Successful Login Times (secs)	Median Successful Login Times (secs)	Std. Dev. Successful Login Times (secs)
Imagept21	17.13	14.18	7.57
Text21	9.95	9.06	4.24

Table 4. Mean, median, and standard deviation of Successful User Login Times

Next, we looked at mean, median, and standard deviation of successful and failed login times (measured in seconds). This statistic should be more illuminating in the assessment of password scheme usability: the faster login times are, the better for the user. Users don't want to spend any longer than they need to passing security barriers, because they want to get to work (or play). Looking at successful login times (Table 4), it is clear even without a graph that Imagept21 has a higher successful login time. This means that users of Text21 successfully entered their passwords faster than users of Imagept21. In Figure 10, there is an outlier worth pointing out: one user had an extremely long login time of almost 40 seconds compared to a mean of 17.13. This is three standard deviations away from the mean, and may skew the results by a small amount. However, one outlier may account for some of the distribution's spread, the overall effect on the mean would not make a big impact. As it happened, Text21 had a near-outlier as well, and in the same skew: a few users took an inordinate amount of time to successfully login compared to the mean. Removing all outliers does not change the result: Successful login times are faster for Text21 than Imagept21.

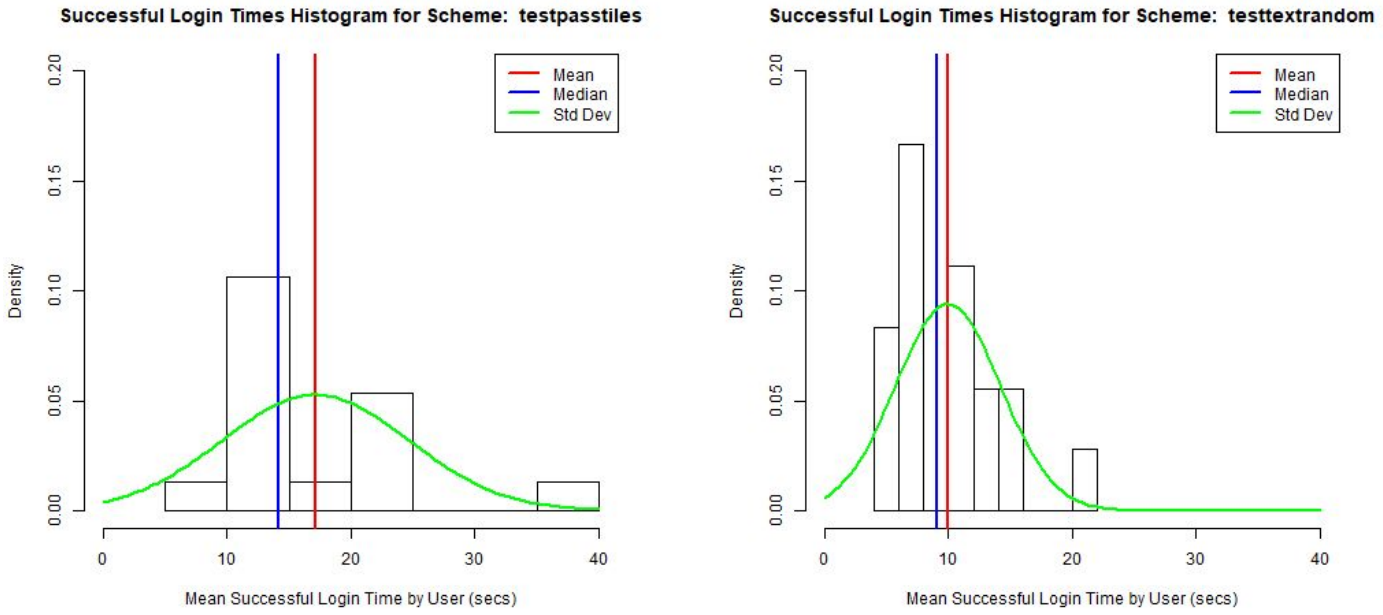


Figure 10. Histogram of Successful Login Times by User for Imagept21 (left) and Text21 (right)

For failed login times, Figure 11 shows a large difference between Imagept21 results and Text21. Text21 has a highly left-shifted, high spread distribution that is vaguely unimodal. Imagept21, on the other hand, has a very highly spread out distribution that shows a modality approaching flatness. Table 5 confirms that Text21 failed login times were shorter than Imagept21, and by a good margin. The bulk of Text21's distribution lies within the first standard deviation, with a median login time of just 5 seconds. Imagept21 users had a mean of 18.4 seconds and a median of 15.66 seconds, with a very spread out distributions (multiple users failed to login by the 30, 40, or 50 second marks). The results here mirror the results of successful login times, that Text21 users login faster and with greater consistency than Imagept21 users.

Password Scheme	**Mean Failed Login Times (secs)**	**Median Failed Login Times (secs)**	**Std. Dev. Failed Login Times (secs)**
Imagept21	18.40	15.66	14.10
Text21	6.01	5.50	6.89

Table 5. Mean, median, and standard deviation of Failed User Login Times

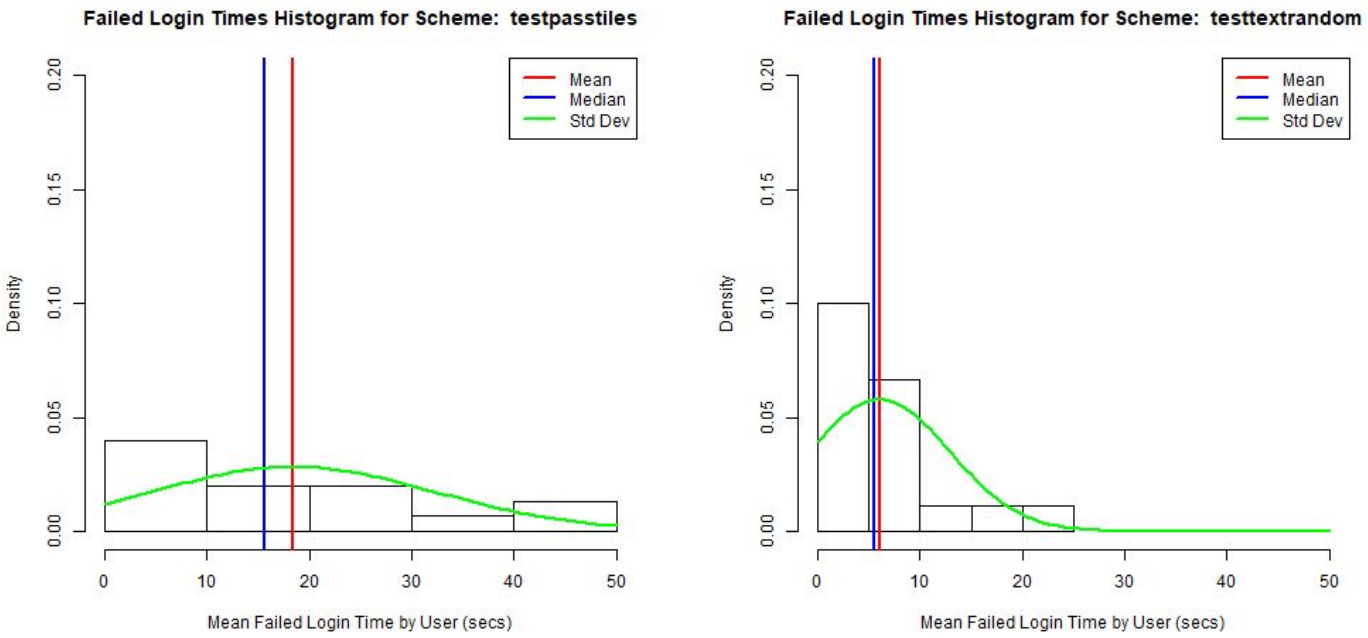


Figure 11. Histogram of Failed Login Times by User for Imagept21 (left) and Text21 (right)

Boxplots of successful and failed login times (Figures 12 and 13 respectively) give a different perspective of the distributions for side by side comparison. The outliers are visible in Figure 12 as small circles. For successful login times, with the outliers ignored we can see clearly on the boxplot that even the worst login times for Text21 were nearly as fast as the best login times for Imagept21. In Figure 13, for failed login times, the trend is again the same as in Figure 12. It should be noted that the distributions for all login

times seem non-normal, with large standard deviations, and that future study could focus on increasing the dataset of these statistics to create a more normal distribution.

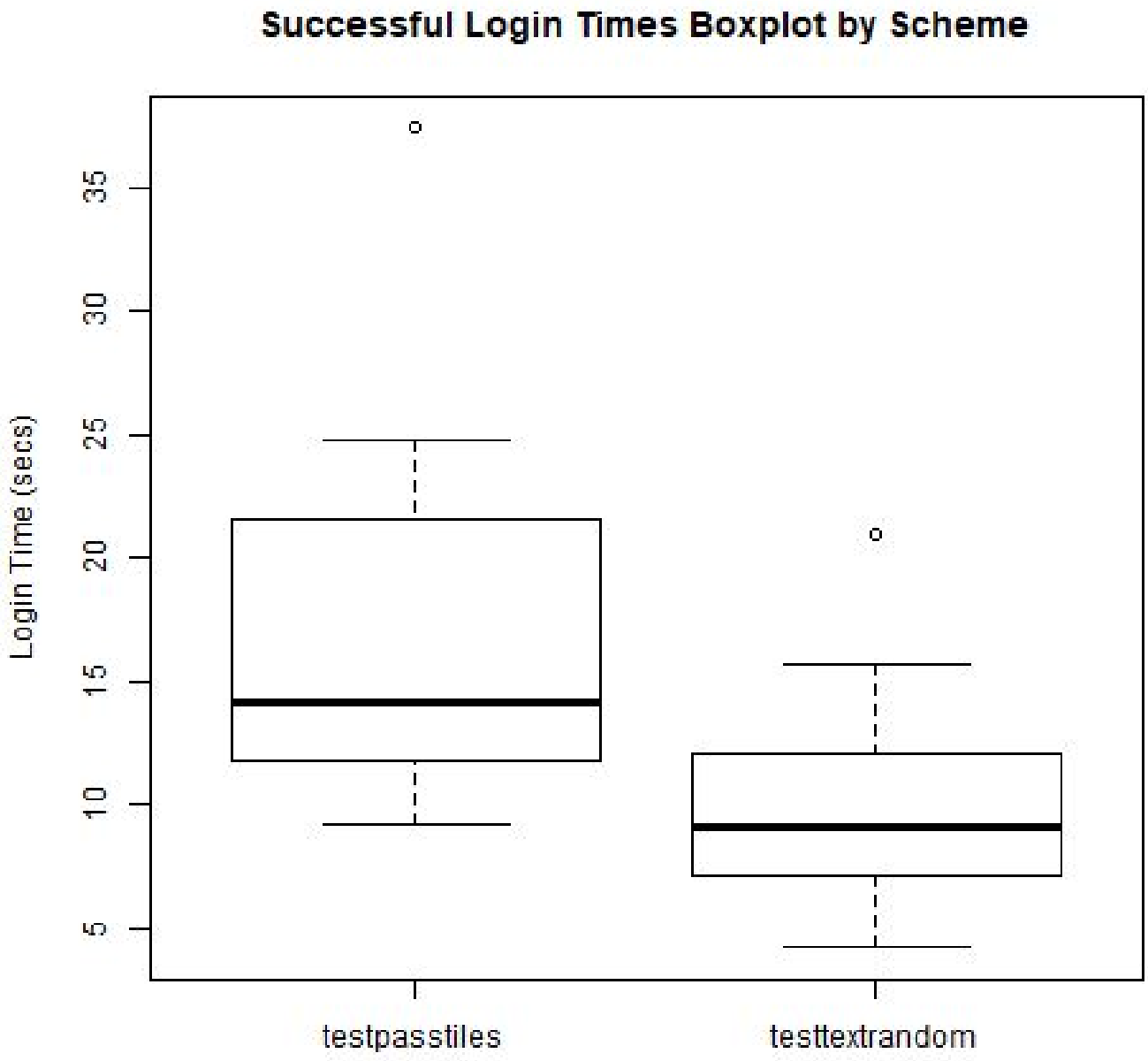


Figure 12. Boxplot of Successful Login Times by User for Imagept21 (left) and Text21 (right)

In the boxplot, the thick black line denotes the mean and small circles denote outlier data points that lie beyond the error bars.

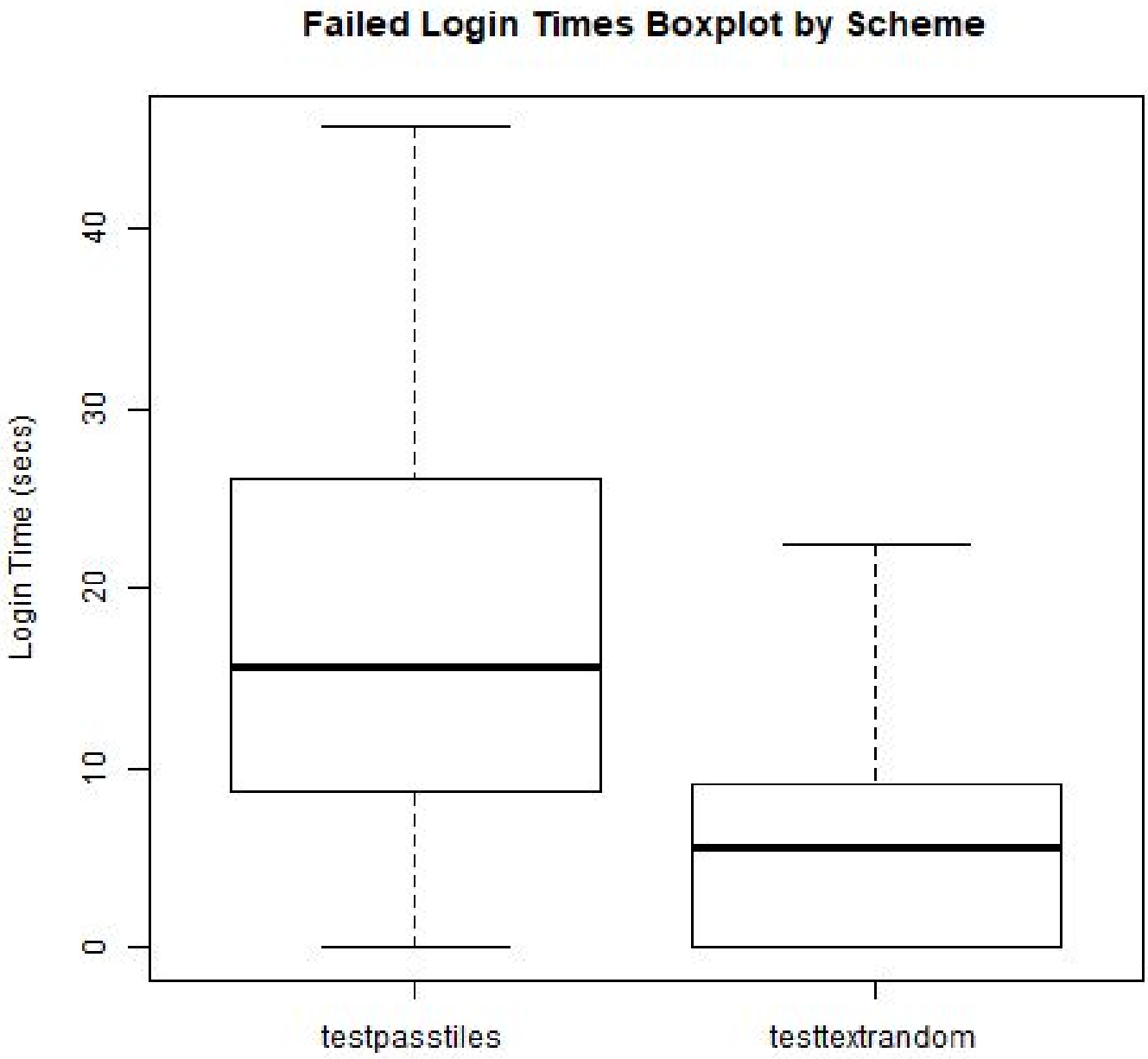


Figure 13. Boxplot of Successful Login Times by User for Imagept21 (left) and Text21 (right)

In the boxplot, the thick black line denotes the mean and small circles denote outlier data points that lie beyond the error bars.

What can we synthesize from our above analysis? In summary, Imagept21 users tend to have more consistent, successful logins and a lower, but more spectacular failure rate for logins. Imagept21 users also take significantly longer to login. We can almost imagine the users sitting there, staring at the image tiles, trying to remember which ones are correct and often struggling. An average login time, success or failure, that falls between 17 to 19 seconds is quite a long time when we imagine an “ideal” password login time that should be as close to instantaneous as possible. Text21, on the other hand, has an average login time that falls in the 6 to 10 second range, much closer to ideal.

Overall, Text21 appears to be the password scheme with higher usability. Login times are much faster on Text21, and the difference in success and failure rates between Imagept21 and Text21 are not large. However, this does not invalidate image-based password schemes for further study. There could be many reasons why Imagept21 failed to prove more usable than Text21, but probing those reasons are beyond the scope of these statistics and their analysis.

Part 2 - Design, Implementation, and Statistical Inference of a New Password Scheme

Section 1 - Design Rationale and Password Space

Design

Our design presents the user with a 4×4 miniaturized chessboard upon which to place pieces, taking cues from both PassTiles and Chase & Simon's 1973 experiment on chunking. To manipulate passwords, participants choose a set of chess pieces and place them on the board. The system allows for repetition of pieces (For example, two black queens), but not repetition of spaces, resulting in a total of 1,478,256 possible password

The Math

The project requires a password entropy of 21 bits, or roughly 2^{21} possible passwords. The formula for password entropy is as follows:

$$H = L log_2 N$$

… Where H is the information entropy of the password, L is the length of each password, and N is the number of possible symbols. There are 16 tiles on our chessboard, and 13 options for a piece on each (two colours of rook, bishop, knight, queen, king, pawn, as well as an empty tile). Therefore, $N = 16 \times 13 = 208$.

$$L = \frac{21}{log_2 208} = 2.72$$

The goal then, is 2.72 chess pieces to achieve an entropy of 21, which we will round to 3. (A password of length 3 has $H \cong 23.1$ and a password of length 2 has $H \cong 15.1$.)

The assumption of the above equation is that the number of possible characters does not change. However, two pieces cannot be placed on the same tile. As a result, the total number of passwords is $(208\ 3)$, or $1,478,256$. A quick calculation shows that the true password space still has entropy of almost 21…

$$H = log_2\ 1,478,256\ \ = 20.5$$

… So our choice of 3 characters will suffice.

Qualities

This system might seem difficult to use because it is unfamiliar and unfamiliar things tend to difficult at first sight. But some common sense should undo the initial impression. If we look at the way infants learn about the world, they encounter pictorial representation before learning about text and characters (Norman Fraser, 2009). Not all adults learned to read and write, so it is more difficult or them to handle text.

While it is possible not everyone who uses our system has played chess, it's likely that many are familiar with the rules and pieces. A player might find meaning in certain organizations of pieces, like in Chase & Simon (1973), but only if they are allowed to choose a password for themselves. For chess novices, we expect users may create narratives about what is happening in their password's "game" to explain the configuration of pieces.

This system does not rely on characters being in order, which means users can recall their pieces in any order meaningful to them. While this could increase the likelihood of guessing another user's password, the lack of semantic meaning in a password means a password is unlikely to be as guessable as say, a name or date.

Section 2 - New Password Scheme Implementation

```
/*
    function : build
    purpose  : creates the password
    return   : the chess pieces and their positions
*/
function build(){
    var pieces = Array('blackQueen','whiteQueen','blackKing','whiteKing','blackPawn','whitePawn','whiteKnight',
        'blackKnight','whiteRook','blackRook','blackBishop','whiteBishop');
    var piece1 = pieces[Math.floor(Math.random()*pieces.length)];
    var piece2 = pieces[Math.floor(Math.random()*pieces.length)];
    var piece3 = pieces[Math.floor(Math.random()*pieces.length)];
    var pos = Array('r1c1','r1c2','r1c3','r1c4','r2c1','r2c2','r2c3','r2c4','r3c1','r3c2','r3c3','r3c4','r4c1','r4c2','r4c3','r4c4');
    var pos1 = pos[Math.floor(Math.random()*pos.length)];

    //remove position of first piece..
    var indexToRemove = pos.indexOf(pos1);
    if (indexToRemove > -1) { pos.splice(indexToRemove, 1);}

    var pos2 = pos[Math.floor(Math.random()*pos.length)];

    //remove position of second piece ..
    indexToRemove = pos.indexOf(pos2);
    if (indexToRemove > -1) { pos.splice(indexToRemove, 1);}

    var pos3 = pos[Math.floor(Math.random()*pos.length)];
    var posNpiece = [pos1, pos2, pos3, getpieceID(piece1)
    , getpieceID(piece2), getpieceID(piece3)];

    //adds piece to its corresponding tile
    $('#'+pos1).append("<img class='imgs' src='Pieces/" + piece1 + ".png' style='display:block;margin: 0 auto; padding-top:10px;'/>");
    $('#'+pos2).append("<img class='imgs' src='Pieces/" + piece2 + ".png' style='display:block;margin: 0 auto; padding-top:10px;'/>");
    $('#'+pos3).append("<img class='imgs' src='Pieces/" + piece3 + ".png' style='display:block;margin: 0 auto; padding-top:10px;'/>");

    return posNpiece;
}
```

Figure 5.10. Password Scheme

For Chess21 Password Scheme, we made a function called build that is responsible for creating the password. There is an array with all the possible positions and pieces. Using the Math library provided for javascript, three random pieces and positions are chosen. There can be duplicate pieces in the password, however, the positions for each piece must be unique. Therefore, after each position is chosen randomly, it is removed from the array of all possible positions. Once the positions and pieces are chosen, the images corresponding with the pieces are attached to the tiles on the board.

Figure 5.11. Prompt for username

When the web page is first loaded, a username is requested by the user. Once the user has entered a name, the ‘Confirmation phase’ of the web page is displayed.

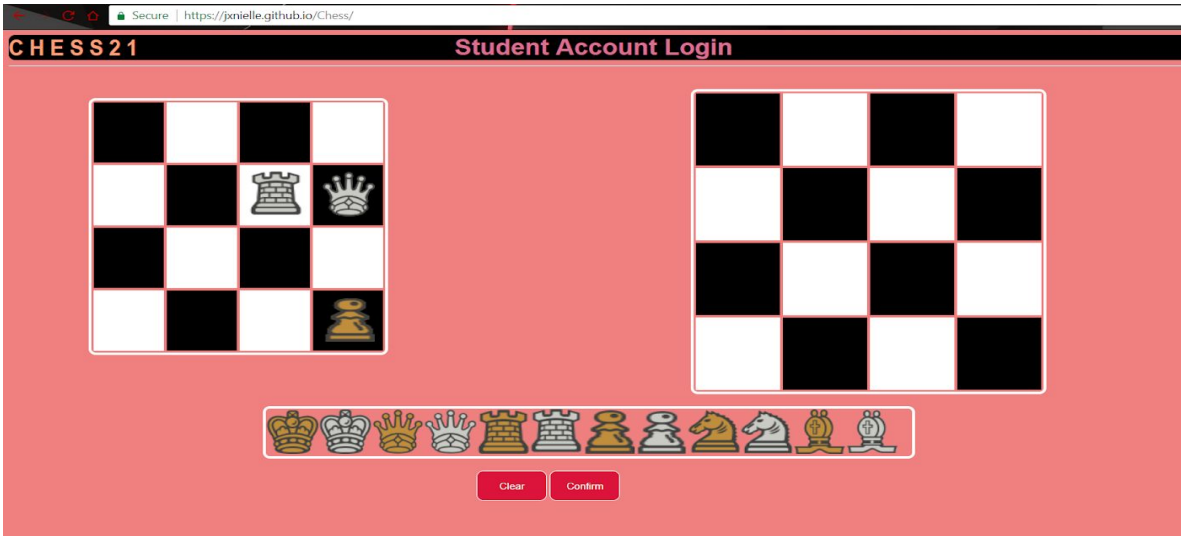


Figure 5.12. Confirmation phase.

In the Confirmation Phase, 2 boards are displayed. The left board shows the password given to the user, and the right board is what the user will use to confirm the password. The pieces the user will drag to the right board is shown at the bottom of the page. The ‘Confirm’ button is used when the user wants to validate his or her choice. If the user dragged a piece incorrectly, there is a ‘Clear’ button that will reset the board, however, if the user entered the incorrect password and clicked the ‘Confirm’ button, an error message is displayed and the right board resets.

There are 3 different types of password: Student Account Login, Footlocker Login and Outlook Login. The user will know which type of password they are currently working with by the heading at the top of the page.

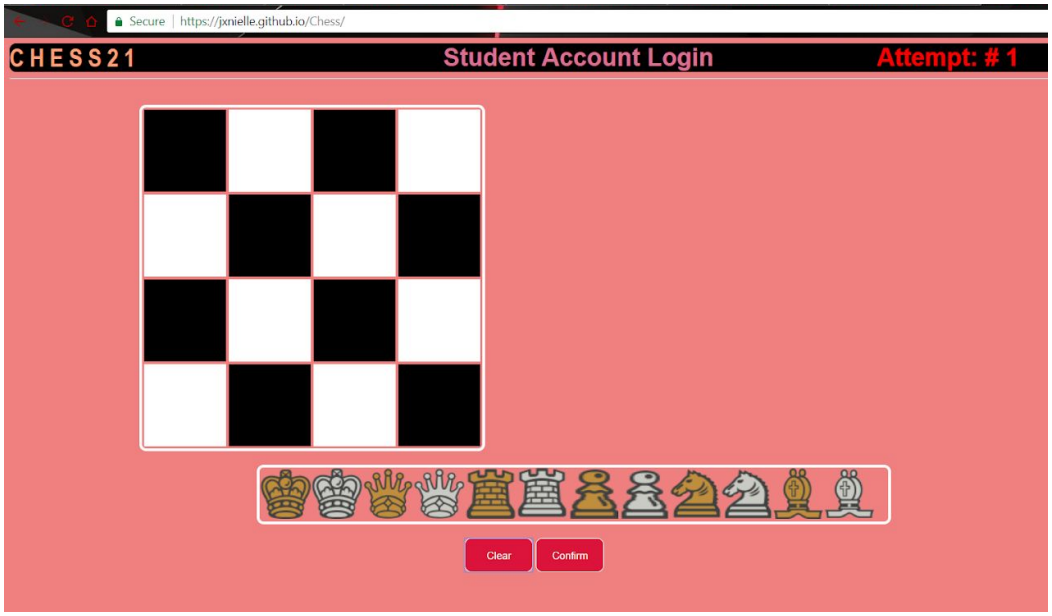


Figure 5.21. Login Phase - User is randomly asked for password.

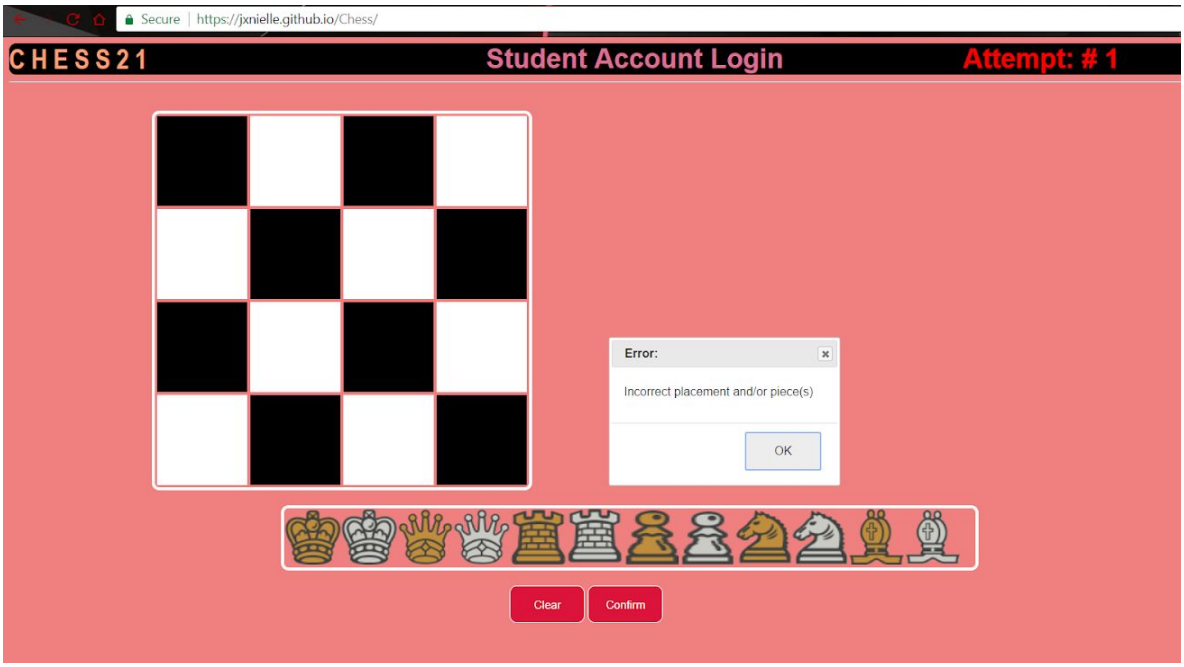


Figure 5.22. Login Phase - Alert box when user enters wrong password.

After the Confirmation phase, there is the Login Phase. The user is asked to enter the password in a random order. The password given to the user will not be displayed, however, the Password Type which is displayed at the top of the web page should serve as a hint. The user has three attempts to enter each password. The number of attempts is shown at the top of the screen. If the user enters the correct password, their success is recorded in the log file and the next password is displayed. If after three attempts the user is unable to correctly

enter the password, their failure is recorded and the next password is displayed. When all three passwords have been tested, there is an option to save the log file or try a new set of passwords.

Section 3 - New Password Scheme Testing Framework

```
<!--Hidden tags-->
<p id="testing" hidden="true">0</p>
<p id="passwordNum" hidden="true">1</p>
<p id="dropCounter" hidden="true">0</p>
<p id="time" hidden="true"></p>
```

In the index.html file, we used a number of hidden fields to assist in the logging process. “testing “ is used to distinguish between the confirmation phase and login phase. “dropCounter” is used to ensure that a maximum of 3 pieces is dragged onto a tile on the board. “Time”, holds the current time that an event is triggered.

```
/*
    function : nextPass
    purpose  : displays next password
*/
function nextPass(){
    var test = $('#testing').html() // 1 - login phase, 0 - confirmation phase
    $("#dropCounter").html(0);
    var nPass = parseInt($('#passwordNum').html()) + 1;
    var passType = Array('Student Account Login', 'FootLocker Login', 'Outlook Login');
    $('#passwordNum').html(nPass);
    $('.imgs').remove();
    $( "#sec" ).remove();
    addSection();
    DragNDrop();

    if ($('#passwordNum').html() == 2 && test == 0){
        Passwords.pass2 = build();
        $('#passwordType').html(passType[1]);
        $("#passwordType").css("color", "yellow");
        LogRow(passType[1],'create','start');
    }
    if($('#passwordNum').html() == 2 && test == 1){
        $('#passwordType').html(passType[1]);
        $("#passwordType").css("color", "yellow");
        LogRow(passType[1],'enter','start');
    }
    if($('#passwordNum').html() == 3 && test == 1){
        $('#passwordType').html(passType[2]);
        $("#passwordType").css("color", "springgreen");
        LogRow(passType[2],'enter','start');

    }
    if($('#passwordNum').html() == 3 && test == 0){
        Passwords.pass3 = build();
        $('#passwordType').html(passType[2]);
        $("#passwordType").css("color", "springgreen");
        LogRow(passType[2],'create','start');
    }
}
```

The function nextPass decides which password to show next. The “test” variable is used to differentiate between the confirmation phase and login phase. The password number corresponded to a particular password type (ex. Student login, footlocker login, outlook login).

```
    /*
        function : confirmUserChoice
        purpose  : confirms if user entered password correctly or not
    */
    function confirmUserChoice(){
        var attempt = $('#passAttempt').html();
        var passed;
        var password;
        var passType = $('#passwordType').html();
        var passNum = $('#passwordNum').html()
        var test = $('#testing').html(); // 0 - confirmation phase, 1 - login phase

        if (passNum == 1){
            password = Passwords.pass1;
            passed = confirmPass(password,uChoice);
        }else if (passNum == 2){
            password = Passwords.pass2;
            passed = confirmPass(password,uChoice);
        }else if (passNum == 3){
            password = Passwords.pass3;
            passed = confirmPass(password,uChoice);
        }else{} // should never happen

        if(passed && (passNum < 3)){
            if(test == 1){
                LogRow(passType,'login','success');
                $('#passAttempt').html(0);
                attempt=0;
            }
            nextPass();
        }
```

```
        if(!passed && (passNum < 3)){
            $( "#dialog" ).dialog( "open" );
            ResetTable();
            if(test == 1){ //login phase
                attempt++;
                $('#passAttempt').html(attempt);
                if(attempt == 3){
                    LogRow(passType,'login','failure');
                    $('#passAttempt').html(0);
                    attempt=0;
                    nextPass();
                }
            }
        }
        if(passed && (test == 0) && (passNum == 3)){
            $('#passAttempt').html(0);
            attempt=0;
            ResetTable();
            TestUser();
        }
        if(passed && (test == 1) && (passNum == 3)){
            LogRow(passType,'login','success');
            End();
        }
        if(!passed && (passNum == 3)){
            $( "#dialog" ).dialog( "open" );
            ResetTable();
            if(test == 1){ //login phase
                attempt++;
                $('#passAttempt').html(attempt);
                if(attempt == 3){
                    LogRow(passType,'login','failure');
                    End();
                }
            }
        }
    }
```

The confirmUserChoice function tests whether the user entered the password correctly or not. Depending on the result, either an error message or the next password is shown. An “attempt” variable is used to track the number of attempts by the user in the Login phase. This is used to ensure that the user does not go pass three attempts per password. If the user has passed or reached the maximum number of attempts on the last password in the login phase, then the option to download the log file is displayed.

A new script, **inferential-testing.R**, was created to analyze descriptive and inferential statistics for Chess21. It creates several vectors from the columns of our pre-processed data and uses them as the inputs of several Welch’s two-sample t-tests. The data recorded was:

- Total number of logins, number of successful logins, and number of failed logins for each scheme
- Total time to login, Time of each successful login, and time of each failed login for each scheme

The specific t-tests used and their results can be found in the discussion section further below. The pseudocode for **inferential-testing.R** is shown here:

```
SET path variables:
  work_dir directory of this source file

data_frame <- read in from CSV
num_schemes <- The number of unique entries in data_fram from column "PasswordScheme"

Create results list and vectors for statistics calculations, initialize as empty

for each i in length(num_schemes):
  data_scheme  = subset of data_frame where column "PasswordScheme" == num_schemes[i]

# Create vectors for success rates
success_tiles <- Total number of successful logins for Imagept21
success_text <- Total number of successful logins for Text21
success_chess <- Total number of successful logins for Chess21

# Create vectors for failure rates
fail_tiles <- Total number of failed logins for Imagept21
fail_text <- Total number of failed logins for Text21
fail_chess <- appendTotal number of failed logins for Chess21

# Create vectors for time data
  time_tiles <- Total login times for Imagept21
  time_text <- Total login times for Text21
  time_chess <- Total login times for Chess21
  time_succ_tiles <- Successful login times for Imagept21
  time_fail_tiles <- Failed login times for Imapgept21
  time_succ_text <- Successful login times for Text21
  time_fail_text <- Failed login times for Text21
  time_succ_chess <- Successful login times for Chess21
  time_fail_chess <- Failed login times for Chess21

  Omit Zeros from the Chess21 avg. times to see if it has an impact on statistical significance.
  Calculate new standard deviations for success and failure

# Run a Welch's Unpaired t-test on the following (because this is not a within-subjects design)
succ_TeC = # Rate of success, Text vs Chess
succ_TiC = # Rate of Success, Tiles vs Chess

fail_TeC = # Rate of Failure, Text vs Chess
fail_TiC = # Rate of Failure, Tiles vs Chess

time_succ_TeC = # Time to succeed, Text vs Chess
time_succ_TiC = # Time to succeed, Tiles vs Chess
time_succ_TeC_noZeros = # Time to succeed, Text vs Chess NO ZEROS
time_succ_TiC_noZeros = # Time to succeed, Tiles vs Chess NO ZEROS
time_fail_TeC = # Time to fail, Text vs Chess
time_fail_TiC = # Time to fail, Tiles vs Chess
time_fail_TeC_noZeros = # Time to fail, Text vs Chess NO ZEROS
time_fail_TiC_noZeros = # Time to fail, Tiles vs Chess NO ZEROS
time_total_TeC = # Total time taken, Text vs Chess
time_total_TiC = # Total time taken, Tiles vs Chess

succ_vs_fail = # Success vs Failure rates within Chess21
time_succ_TvT = # Tiles vs Text, Success rates
time_fail_TvT = # Tiles vs Text, Failure rates
```

Section 4 - New Password Scheme User Questionnaire

Our questionnaire is composed of 13 likert scale questions, as follows:

1. On a scale of 1-5, how familiar are you with chess? (1 is not at all, 5 is very familiar)

2. On a scale of 1-5, where 1 is not secure and 5 is very secure, how secure do you feel this password scheme is?

3. On a scale of 1-5, how would you judge this password system's security relative to a regular text password? (1 is much less secure, 5 is much more secure)

4. On a scale of 1-5, how memorable do you find the passwords generated by this scheme? (1 is not at all memorable and 5 is very memorable)

5. How distinct did each password feel to you, on a scale from 1-5? (1 is "nearly identical", 5 is "extremely distinct")

6. On a scale from 1-5, rate how much you agree with the following statement, where 1 is "strongly disagree" and 5 is "strongly agree":
    - *"I'll use a password scheme that takes longer to login if it results in added security."*

7. On a scale of 1-5, where 1 is "strongly disagree" and 5 is "strongly agree", please rate your agreement with the following question:
    - *"I found that the use of a chess metaphor positively impacted my ability to recall passwords."*

8. On a scale from 1-5 where 1 is "strongly disliked" and 5 is "strongly liked", please rate your level of enjoyment of this password scheme.

9. How often did you mistake one password for another due to the fact that they're passwords not connected to anything memorable (to the user)? (1 being not often, 5 being very often)

10. On a scale of 1-5, how distinct was each chess piece visually? (Could you easily tell the king apart from the queen) (1 being very similar, 5 being very distinct

11. On a scale of 1-5, how often would you prefer this password scheme over a text based scheme? (1 being never, 5 being always)

12. On a scale of 1-5, how much harder is it for a user to generate a memorable password using our scheme? (Most passwords relate to some user perceived event in which they find memorable eg. birth date ; 1 being very easy, 5 being very hard)

13. On a scale of 1-5, when given a random password using our chess scheme, how long did it take for you to memorize the password? (1 being very short, 5 being very long)

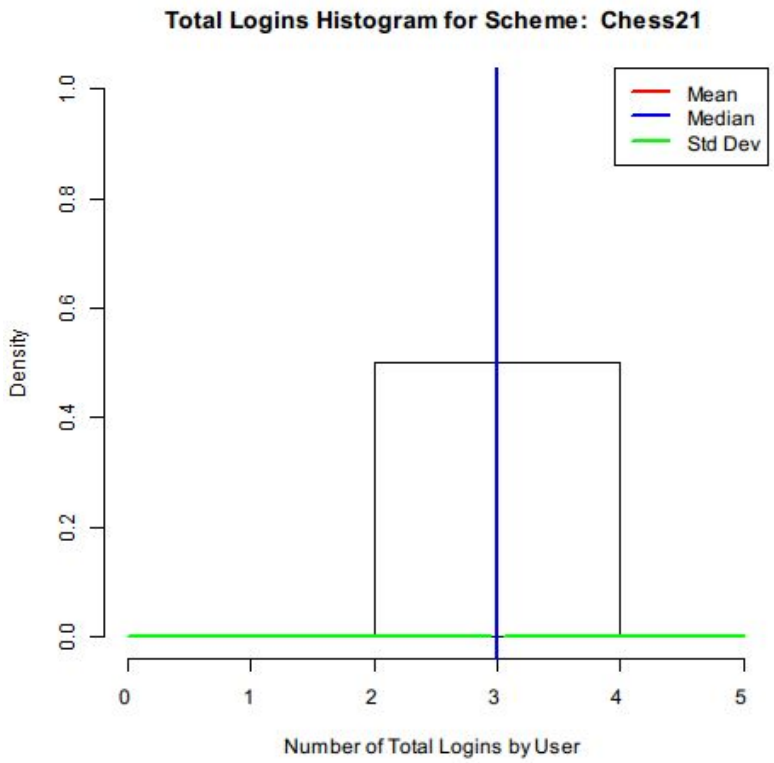
The link to the questionnaire can be found here, and the original questions can be found included in our project folder under the title *team_Rainbow_Questionnaire.pdf*.

Section 5 - Usability Testing Results with New Password Scheme

Every participant who tested Chess21 made exactly three logins. This may seem like an error, but the testing methodology specified for each user to test three passwords, whereas sample data shows a highly varied login count for its users. This did result in a relatively small number of logins across all participants, and could have been avoided by instructing participants to test the scheme several times. However, we would still have collected data in multiples of 3 total logins.

Password Scheme	Mean Total Logins	Median Total Logins	Std. Dev. Total Logins
Imagept21	19.40	18.00	5.23
Text21	16.61	16.00	4.90
Chess21	3.00	3.00	0.00

Table 6: Mean, Median, and Std. Deviation of Total User Logins

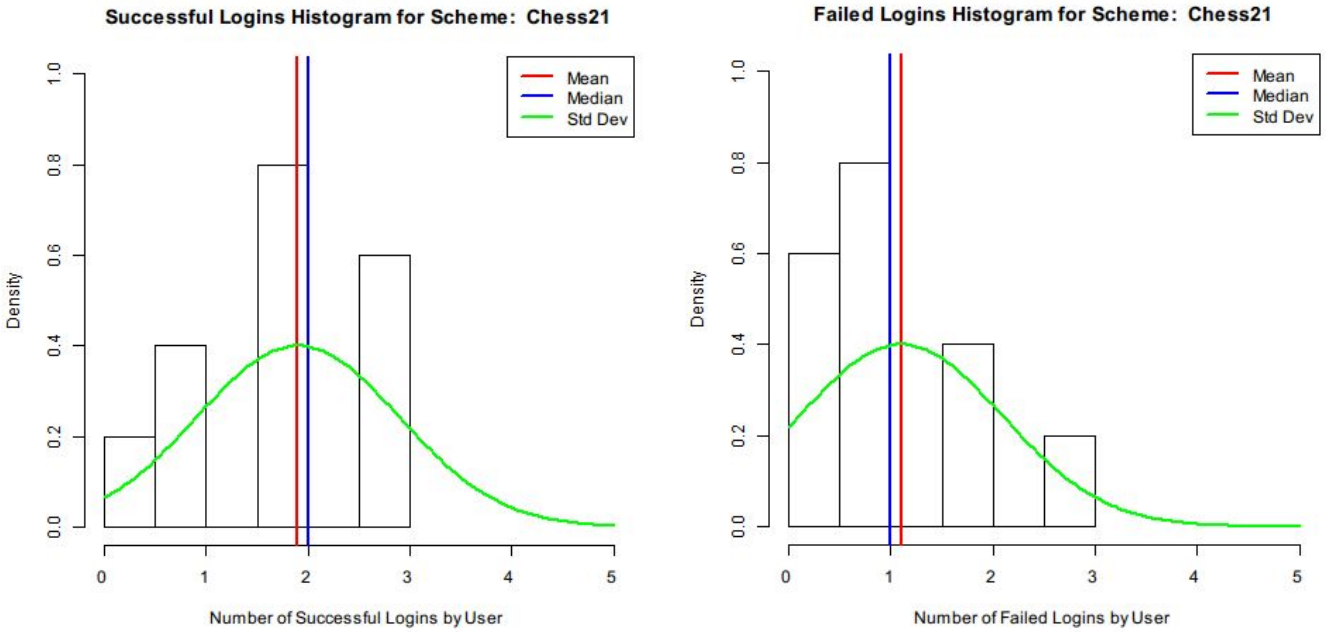


Password Scheme	Mean Successful Logins	Median Successful Logins	Std. Dev. Successful Logins
Imagept21	14.93	15.00	1.33
Text21	14.05	15.00	3.43
Chess21	1.90	2	0.99

Table 7. Mean, median, and standard deviation of Successful User Logins

Password Scheme	Mean Failed Logins	Median Failed Logins	Std. Dev. Failed Logins
Imagept21	4.46	3.00	4.43
Text21	2.55	1.00	3.32
Chess21	1.10	1	0.99

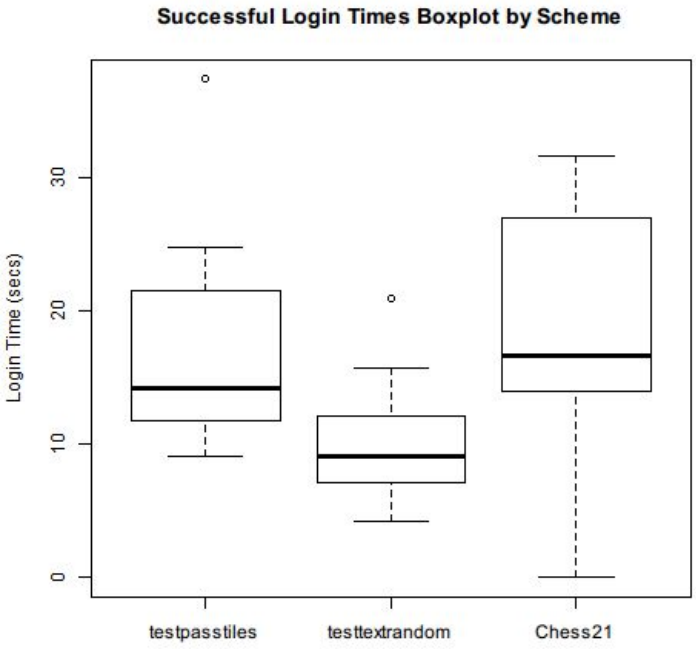
Table 8. Mean, median, and standard deviation of Failed User Logins



Due to the low number of logins per user, we had similarly low rates of success and failure. The average user succeeded in logging in roughly twice as often as they failed, with a tight spread of success and fail rates in both cases (*sd=0.99*). This means that on average, participants were able to successfully recall a password two-thirds of the time. A t-test was run between successes (M=1.9, SD=0.99) and failures (M=1.10, SD=0.99) for Chess21 and found that there was a strong, but not quite significant effect (t(18)=1.79, p=0.08). This is likely due to our small sample data size. However, the relatively high strength of the association leads us to predict that given more trials per participant, the result would likely become significant.

Password Scheme	Mean Successful Login Times (secs)	Median Successful Login Times (secs)	Std. Dev. Successful Login Times (secs)
Imagept21	17.13	14.18	7.57
Text21	9.95	9.06	4.24
Chess21	18.2	16.7	9.36 (7.24 w/o zeros)

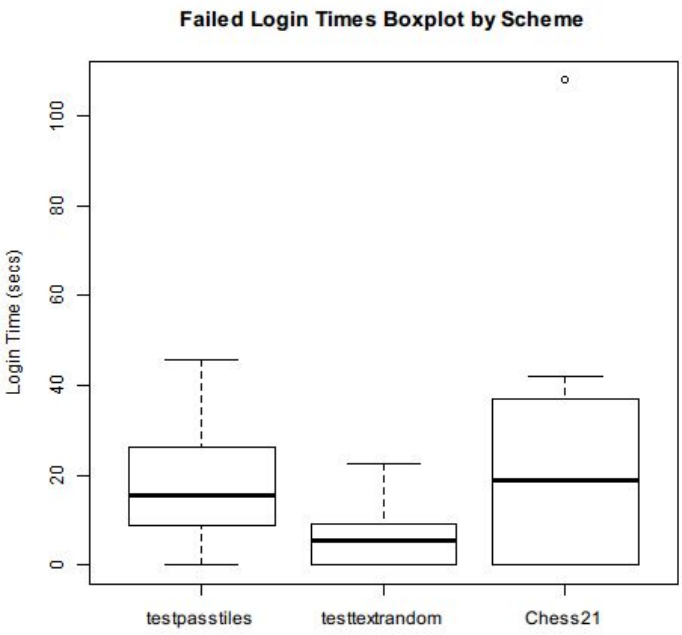
Table 9. Mean, median, and standard deviation of Successful Login Times



As shown in Table 9 (above) and the boxplot to the left, Chess21 had the highest login time for successes between all three of the password schemes, at 18.2 seconds for entry. Unsurprisingly, this is a very similar time to the average successful login time of Imagept21 passwords (M=17.13). In addition, they vary by a similar amount, both having a larger Standard Deviation than Text21. The difference in successful login time between Chess21 and Imagept21 is not a statistically significant difference (t(28.7)-1.74, p=0.09), nor is the difference between Text21 and Chess21 (t(43.4)= -1.70, p=0.97). However, since some participants recorded no successes while testing Chess21, their success time was recorded as 0. This is why the first quartile of Chess21 starts at 0. However, since they do not have a success time, we will remove these nonexistent zeros from the equation (new sd=7.24). Running the t-test again shows that the difference between Chess21 and Imagept21 is still not significant (t(28.0)=1.56, p=0.13) but the difference between Chess21 and Text21 is (t(42.5)= -2.00, p=0.05)!

Password Scheme	Mean Failed Login Times (secs)	Median Failed Login Times (secs)	Std. Dev. Failed Login Times (secs)
Imagept21	18.40	15.66	14.10
Text21	6.01	5.50	6.89
Chess21	26.3	19	32.5 (24.7 w/o zeros)

Table 10. Mean, median, and standard deviation of Failed Login Times



Similar results were found for failed login times, with Chess21 having a much higher mean than both Imagept21 and Text21. The differences between them are not statistically significant in either case. The difference between Chess21 and Imagept21 means results in a p-value of 0.35, and the difference between Chess21 and Text21 results in a p-value of 0.11 when a Welch's t-test is performed. However, some Chess21 participants never failed a password, so removing their zeros from the database (new sd=24.7) presents us with new p-values: 0.63 between Imagept21 and Chess21, but a much more significant 0.02 when performing a Welch's[1] t-test between Chess21 and Text21 failure time means.

Chess21 had a higher mean login time than Text21 and Imagept21 in both success and failure conditions. While the difference in means between Chess21 and Imagept21 was not significant in either case, there was a significant difference between login times between Chess21 and Text21 for both success and failure cases. We can conclude that Chess21 demands a significantly longer input time than Text21 with a confidence of greater than 95%. Welch's t-tests reveal that Imagept21 also has a significantly longer input time than Text21 in both success (p=0.04) and failure (p=0.001) conditions, values much more significant than Chess21 which we attribute to its smaller Standard Deviation. Predictably then, both visual password systems have a significantly longer input time than a text-based system, but there is not a significant difference in input time between the two visual systems.

Additionally, we found that the mean login success rate of Chess21 users (63%) was much lower than the mean success rate of both Imagept21 (77%) and Text21 (85%) users. While this variance is likely due to the low sample size of our study, there is a strong chance that with more data, we would find a similar result.

[1] Note: Every t-test run in this study was a Welch Two-Sample t-test. This was chosen because we were not sure if the variance between cases would be similar before analysis. This is because we are not using a within-subjects study and cannot pair subjects with their own data from the other schemes. We also knew we were working with relatively small sample sizes. Effects caused by both these facts are mitigated better by Welch's t-test than Student's t-test.

Questionnaire Conclusion

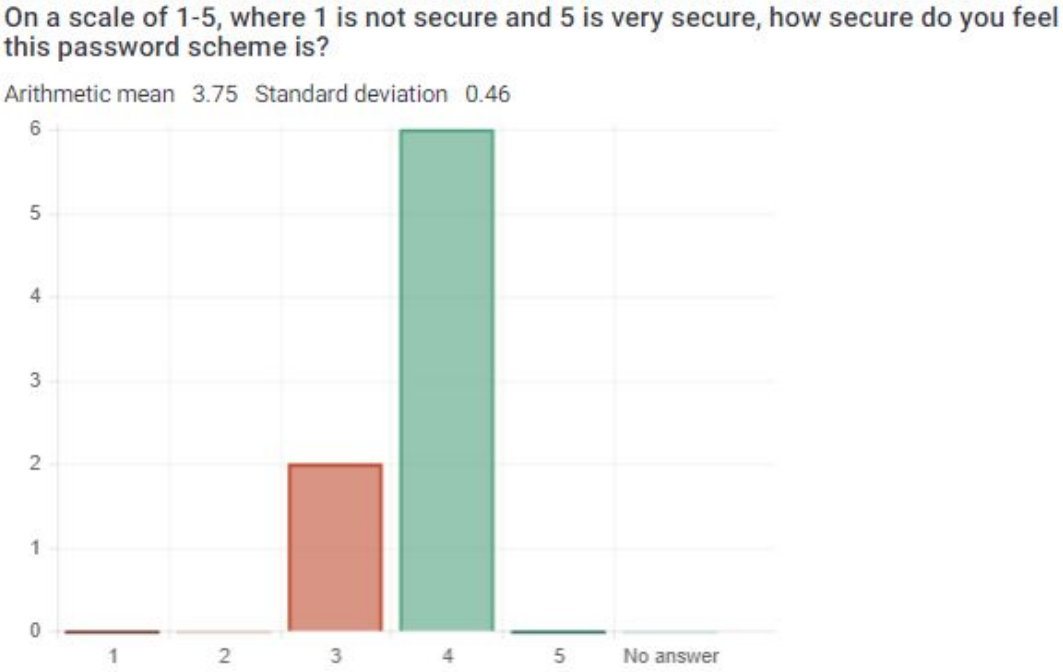
Our questionnaire has provided us with a significant amount of informative statistics that have allowed us to draw several conclusions regarding our password generation scheme. Shown below, is a graph regarding the familiarity of chess to users.

It is evident that a good amount of users are within the lower half of the spectrum in regards to their knowledge about chess. This impacts the effectiveness of our password generation scheme, as it would be more time consuming and difficult to distinguish certain pieces and their relative positioning. This can also be seen within the graph of the question “How memorable do you find the passwords generated by this password scheme?” and “How distinct is each generated password?”.

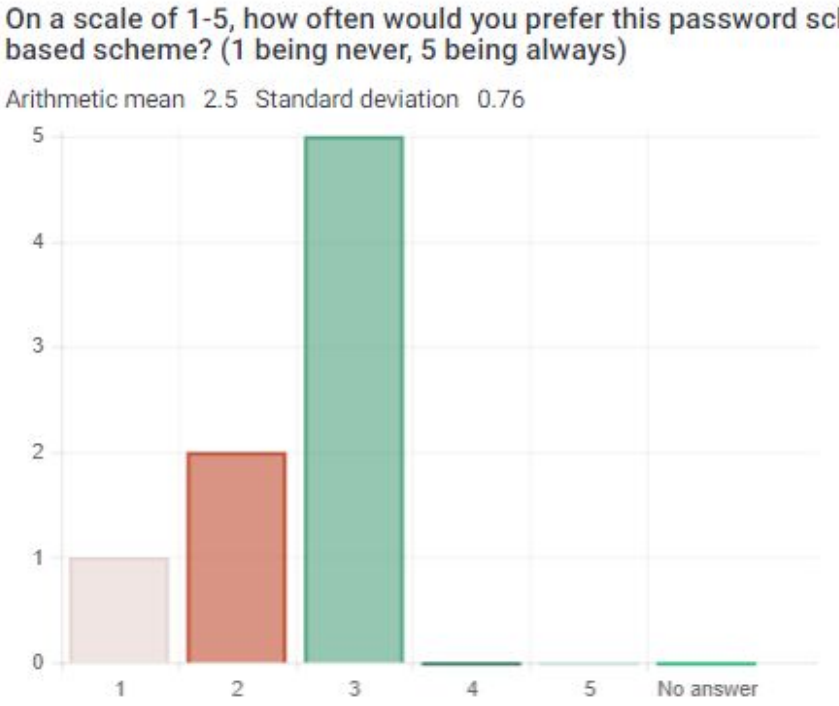
It is clear to us that because many of our users aren't very familiar with chess, the generated chess passwords aren't as memorable as they could be. Due to user unfamiliarity, many of the generated passwords can be seen to be similar to another, as shown below.

Our next conclusion is that, many users value better security over the time needed to login. This can be seen within the graph below.

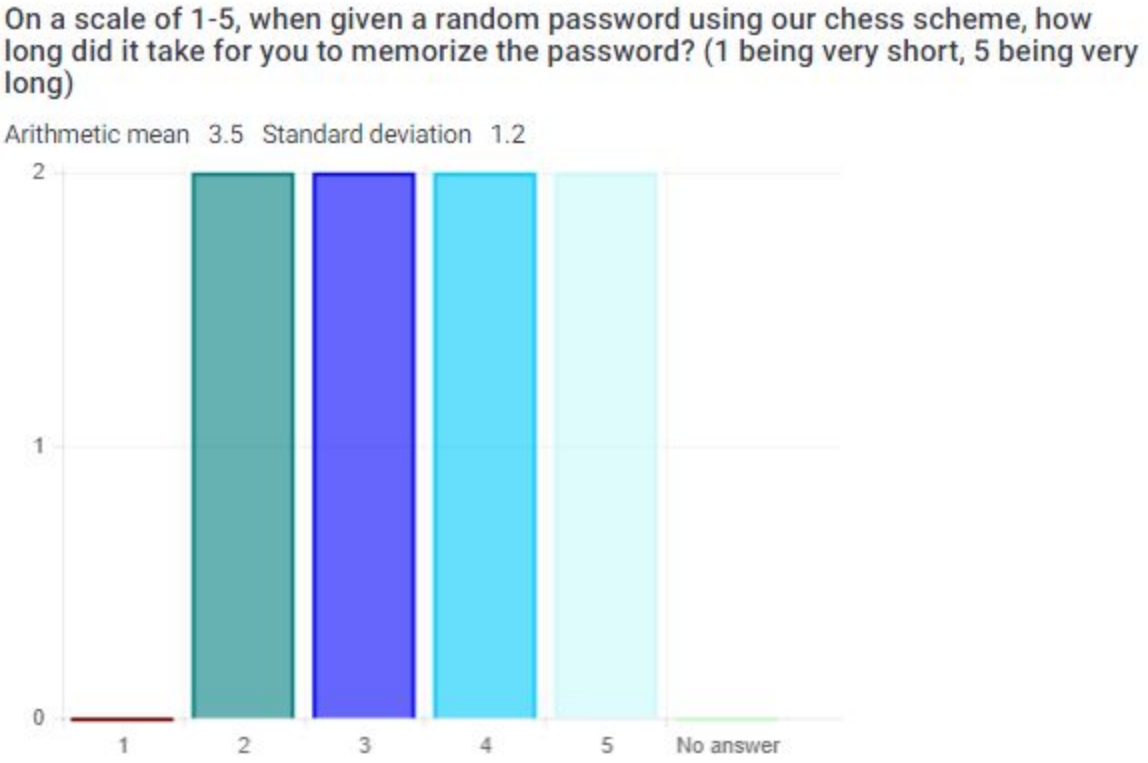
This is one area where our password generation scheme excels. From the two graphs provided, it is clear that many users believe our password scheme is very secure, and even to the point where it is more secure than a standard text based password.



The last conclusion that can be drawn from the questionnaire is that although our password scheme provides solid security, it is clear that many users would still prefer a standard text based password scheme.



This is simply due to that fact that not everyone is familiar with chess. This is detrimental, as many people struggle to memorize the given passwords as they cannot draw the links between the positioning and visuals of the given pieces, whereas a text based password provides for easy mental links between passwords and specific events that the specific user is easily able to distinguish.



As the survey shows statistically, about 30% of users are not familiar with chess, 15.38% were fairly okay with their knowledge of chess and 15.38% were confident in their knowledge of chess. The majority of the users were not familiar with chess at all, thus negatively impacting the user of the given password generation scheme. However, there was about 63% successful logins and users were able to successfully use the system regardless of their knowledge of chess. About 46% of users feel that security is great and the majority think it provides fairly the same level of security as regular text based passwords. A good number of users were fairly okay with their ability to remember each password. About 30.77% to be precise and about 7% didn't think the password were easily memorable. A large majority felt the password were identical, similar, and hard to memorize which reduces the optimization our chess21. Most users would prefer a system that was very secure but takes longer time to login. Although our system took longer time to login, the security level was never an issue. The majority of the users could easily distinguish between chess pieces but this had no effect on memorability. With these usability and memorability issues, we can conclude Chess21 would not be a suitable solution to text based passwords.

Appendix A - Study Participant Consent and Debrief Forms

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:

Matthew Pacitto, Janielle Scarlett, Qudus Agbalaya, Elijah Doem, Roy Xia

---

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: April 6, 2018

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: Matthew Pacitto Roy Xia
Qudus Agbalaya Janielle Scarlett Elijah Doern

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: MPP Date: 4/5/2018

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:

Matthew Pacitto, Janielle Scarlett, Qudus Agbalaya, Elijah Doem, Roy Xia

---

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: JS Date: April 6, 2018

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:

Matthew Pacitto, Janielle Scarlett, Qudus Agbalaya, Elijah Doem, Roy Xia

---

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: VS Date: April 6, 2018

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: Elyjah Doerr, Matt Pacitto, Danielle Scarlett, Roy Xia, Qudus Agbalaya

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: C.S.W. Date: 5 April 2018

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: Matt Pacitto Elijah Doem Danielle Scarlett
Qudus Agbalaya Roy Xing

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: ED Date: 2018/04/06

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: Matt Pacitto, Elijah Doerr Qudus Agbalaya
Danielle Scarlett, Ray Xia

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: RS Date: 2018/05/04

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: Matt Pacitto, Roy Jia, Jonielle Scarlett, Qudus Agbalaya, Eljad Doem

---

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: JM Date: April 6th 2018

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: Elijah Doerr, Matt Pacitto, Ray Xia
Janelle Scarlett, Qudus Agbalaya

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: RS Date: April 5 2018

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: Matt Pacitto, Danielle Scarlett, Qudus Adebalaya, Elijah Doerr, Roy Xia

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: SS Date: April 6, 2018
