Improving Long Term Memory Recognition and Recall of System Assigned Passwords

Submitted By:

Jayesh Doolani

&

Arnav Garg

As part of coursework for CSE 4329/5329/6329:
Human Computer Interaction

Under guidance of:

Dr. Filia Makedon (Instructor)

Michalis Papakostas (GTA)

University of Texas at Arlington

Fall 2015

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

System assigned passwords have always provided high security because of the randomness in their character ordering. This random ordering helps avoid dictionary attacks and attacks by guessing password. People avoid using system assigned passwords because it's hard to remember and learn them. In some cases, users even write down their system assigned passwords on a piece of paper, thereby improving the chances of it being accessed by adversary.

In this project, we implemented a game to help users memorize system assigned passwords. We used psychology principles to help users in memorizing these tough passwords. We achieve this by making the user perform repetitive tasks on a chunk of password, thereby planting the password implicitly in his mind. It was noticed that users do remember their password using chunking and repetitive action and were able to recall their passwords up to 2 weeks after memorizing it.

1. Pilot Study: Phase 1

We started out Piot study: Phase 1 with the hypothesis that users will remember their system assigned passwords if they use games to memorize them. We did a study of related works and found that much work had already been done on passwords such as graphical passwords [1], passwords in form of poems [2], geographical cued points [3] etc. These systems used user assigned passwords which don't always tend to be secure as compared to system assigned passwords. So we decided to come up with a game which can help users memorize these random strings as passwords.

We carried out an experiment on 4 participants who were assigned the same password of length 6 characters. The only difference was in the method to memorize that 6 character password. We came up with 4 different methods of memorization, which were:

a. Traditional method of learning by memorizing it.
b. Dividing the 6 character into 2 chunks and solving a puzzle game using the 2 chunks.
c. Playing an existing game based on repeatability of a sequence.
d. Relating a story to each character of password.

We found that users who used the normal method of memorization, performed very badly. Our technique of using chunks for memorization proved to be an optimal strategy and the idea of memorizing a sequence through games was also effective.

After concluding this study, we were able to prove our hypothesis that games can be used as a great medium to help users memorize the password. We also figured that chunking method was also effective, so we decided to incorporate chunking method in our game and this was the basis of our Pilot Study: Phase 2.

2. *Pilot Study: Phase 2*

In this pilot study, we started with the results of previous study to build our system. We designed several games, each had their own pros and cons but in the end we came up with one design which matched our expectations. We developed a small prototype initially on paper, and took comments from the participants about the system. We received a mixed reaction from our participants, so we decided to implement the system and then test it with the users.

a) System Prototype

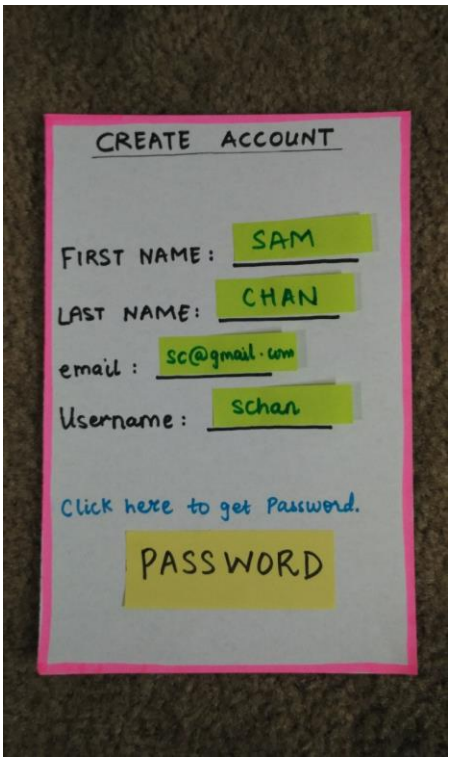


Fig 1: Create Account page, Phase 2

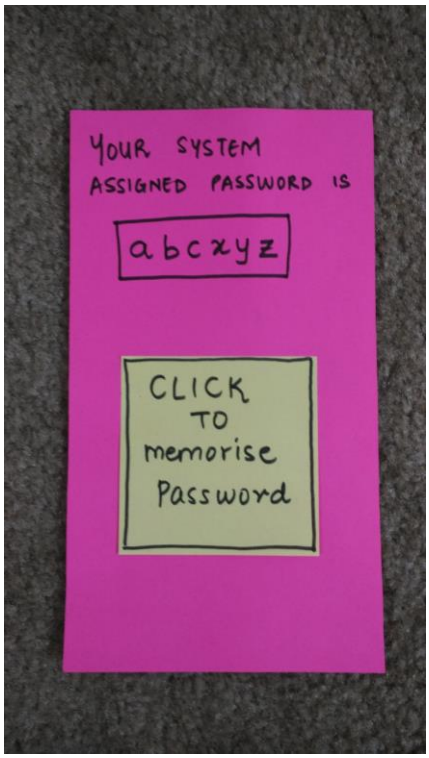


Fig 2: Confirmation page, Phase 2

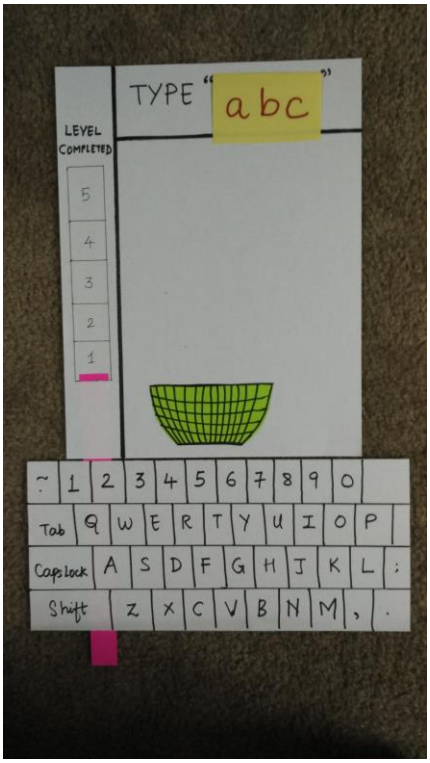


Fig 3: Game chunk 1, Phase 2

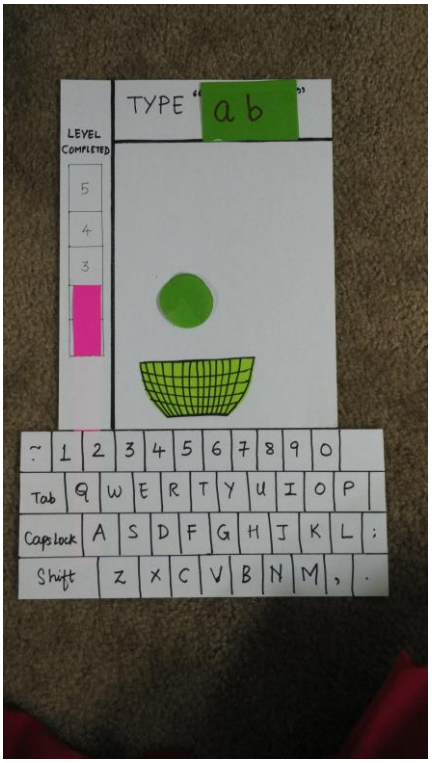


Fig 4: Game chunk level2, Phase 2

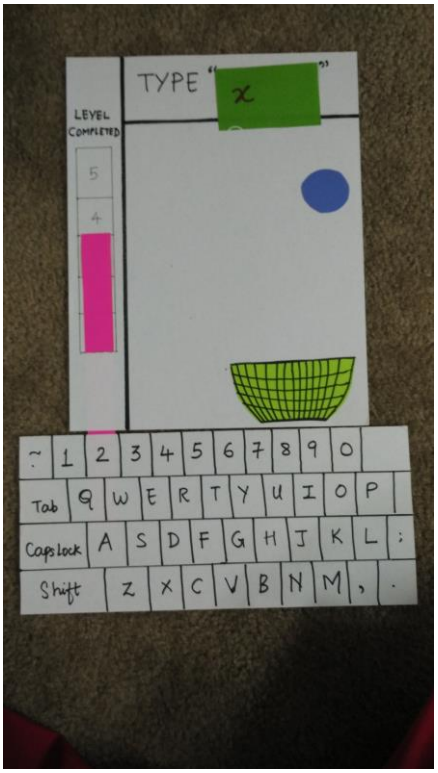


Fig 5: Game chunk 2, Phase 2

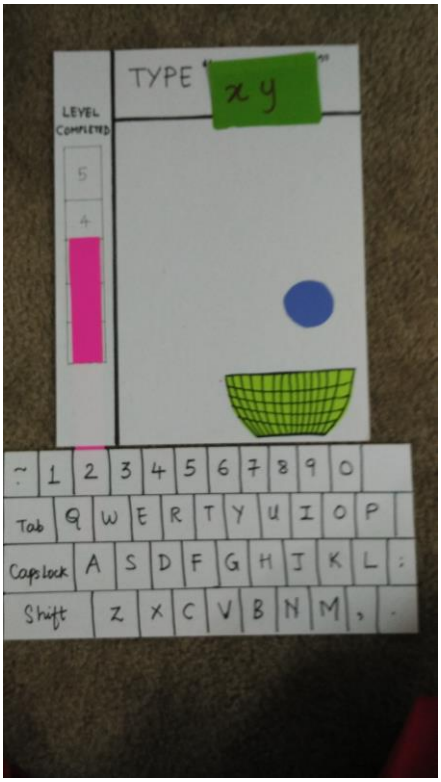


Fig 6: Game chunk 2, Phase 2

3. Pilot Study: Phase 3

We carried out user study on the system we had designed to test its effectiveness. The in class discussion with the Shadow Team, Suraj Doddi and Pradeep Raju, was also very helpful in our evaluation. We figured out that although the design was much better, it was still not of high standards to provide 99.9% recall after 1 weeks of memorizing. The analysis of this study is as follows:

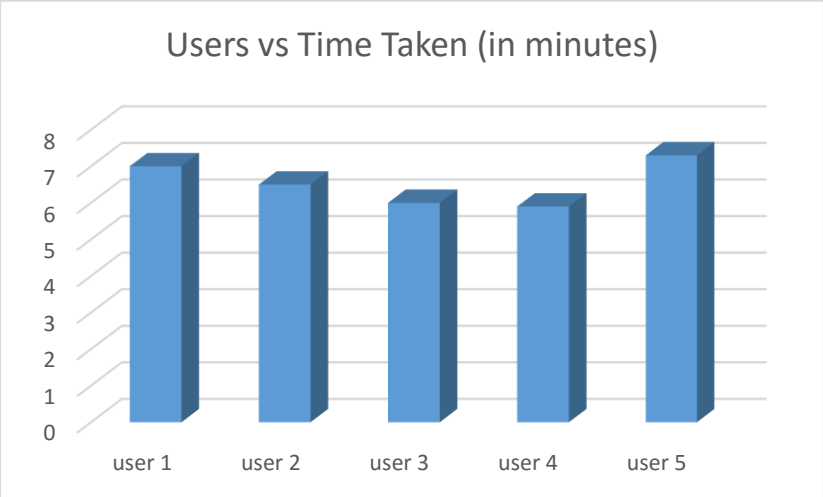
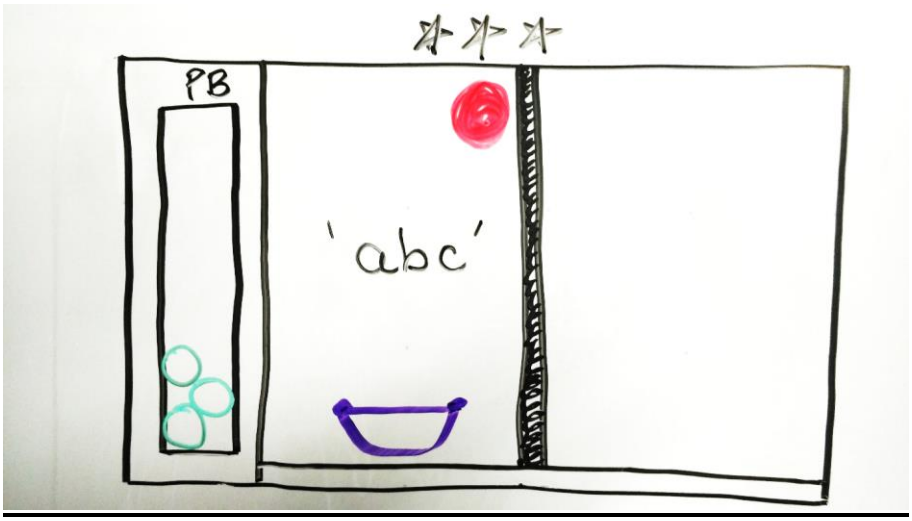


Fig 7: Graph depicting time taken by users in minutes

The average time taken by all the users was 6.54 minutes, which was very high. So we modified our system design to meet our high standards and to decrease the average time taken by users to memorize a password.

a. Improved System Design



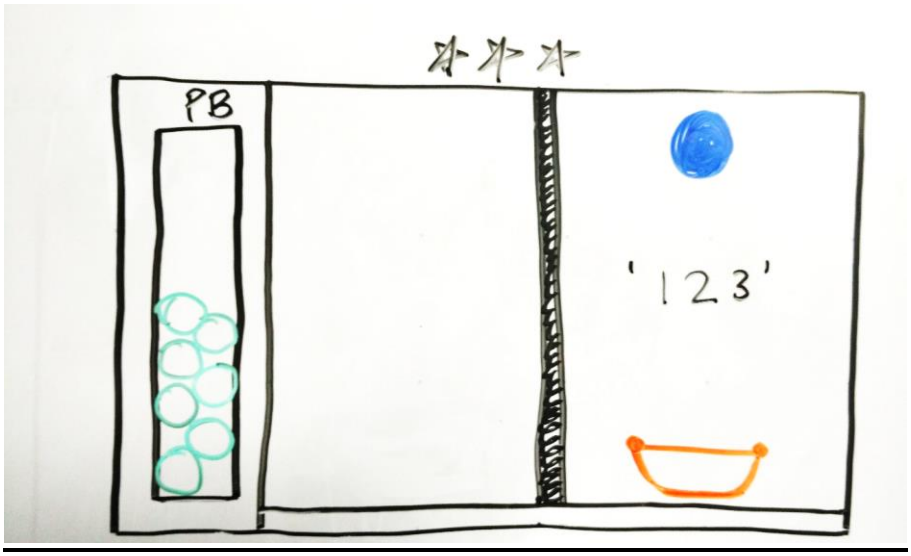


Fig 8: Game chunk 2, Phase 3

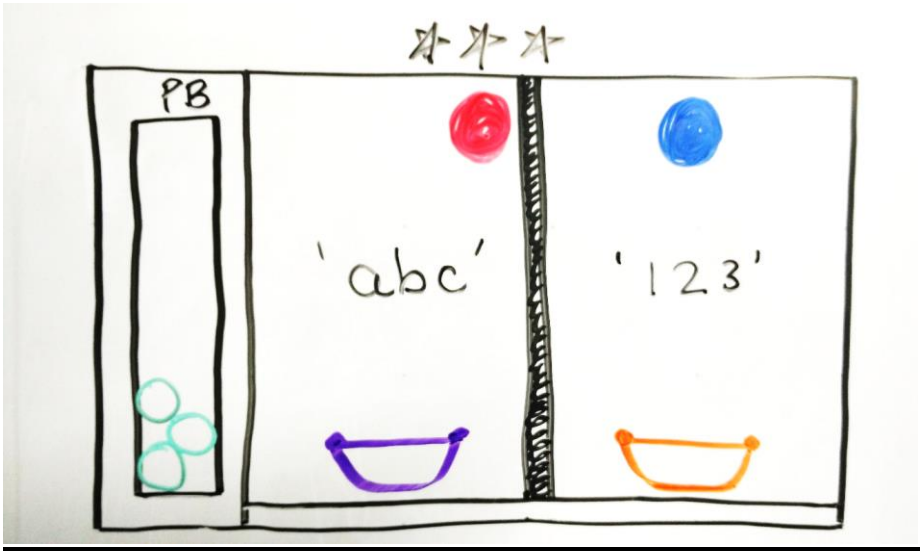


Fig 9: Game level 3, Phase 3

The new system design had the entre screen divided into 2 parts, left for the 1st chunk and right for the 2nd chunk. This plants a psychological concept in users mind that after the first chunk on the left, the other chunk comes on the right and he can visualize both the chunks to better memorize it.

4. Final System Architecture

To implement the entire system along with the front end for the web page to create an account, we designed the system as follows, which is a Client server architecture with a database in the backend:

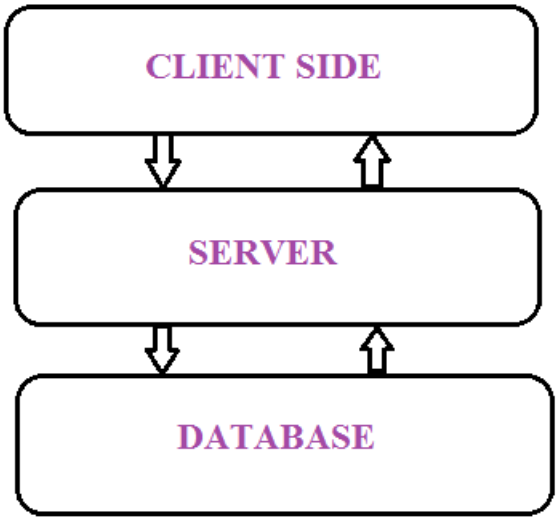


Fig 10: System architecture

The Client side include:

- The front end web page, which was developed using Bootstrap [4].
- The game was developed using Phaser.js, a HTML5 based JavaScript Game framework.[5]

The Server side include:

- UT-Arlington's web server barbie.uta.edu, where we deployed our system.

The database include:

- MongoDB [6], a NoSQL type database to store user's credentials and to log various user data. This database was hosted on Amazon Web Services EC2 instance [7].

5. System Screenshots

1. The following was the front end of the web page for user registration before starting the game.

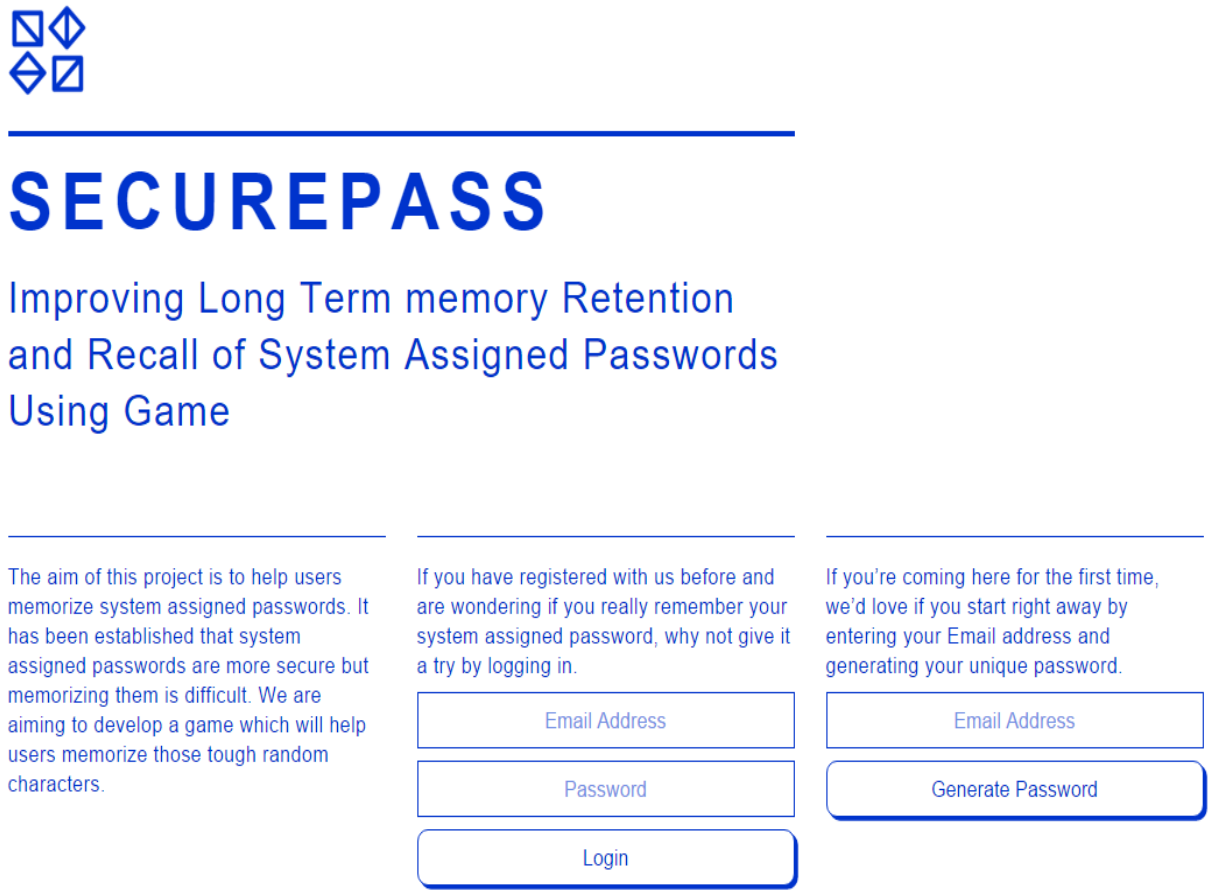


Fig 11: Front end, final webpage of system

2. After the user registers, the system assigns a random 6 character password and displays a button for the user to start playing the game whenever he is ready.

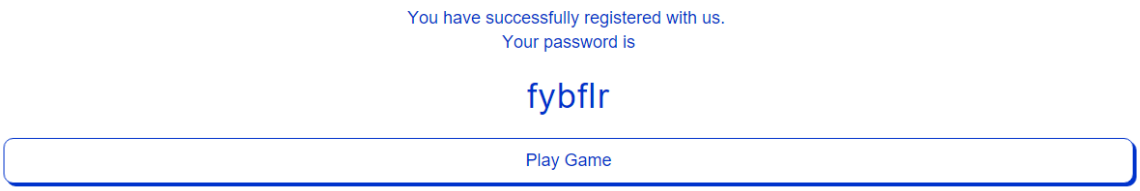


Fig 12: Confirmation page of account registration

3. When the user clicks on Play Game button, the game starts. Initially the user has to play 10 times for the first chunk, as follows:

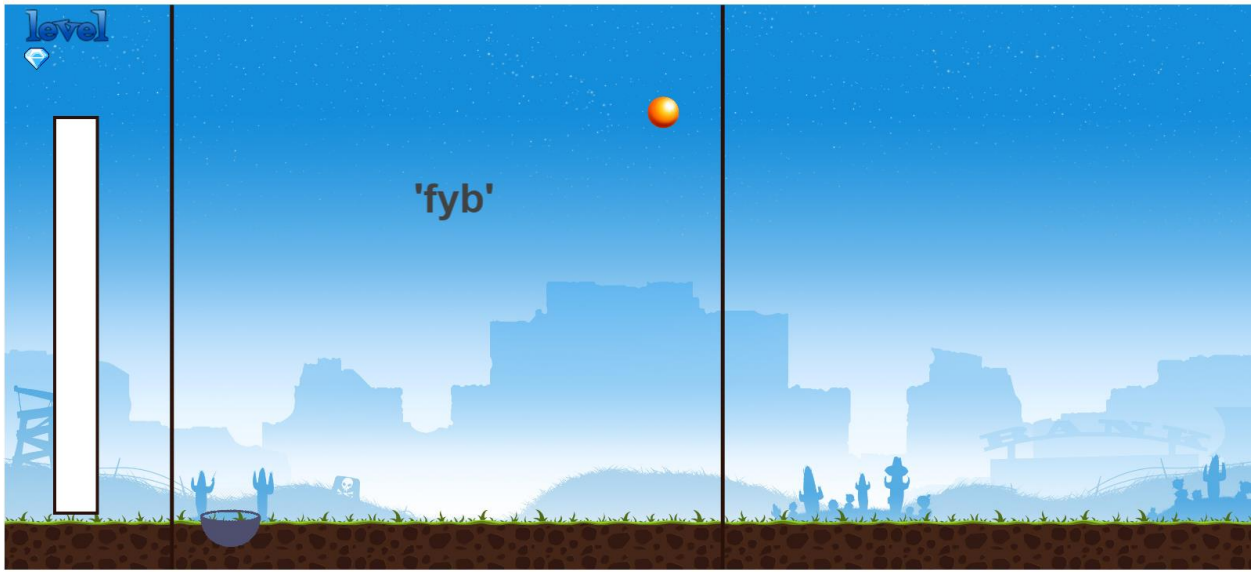


Fig13: Game level 1 with chunk 1

4. After the user finishes the first chunk, the second chunk starts and the same process is continue.

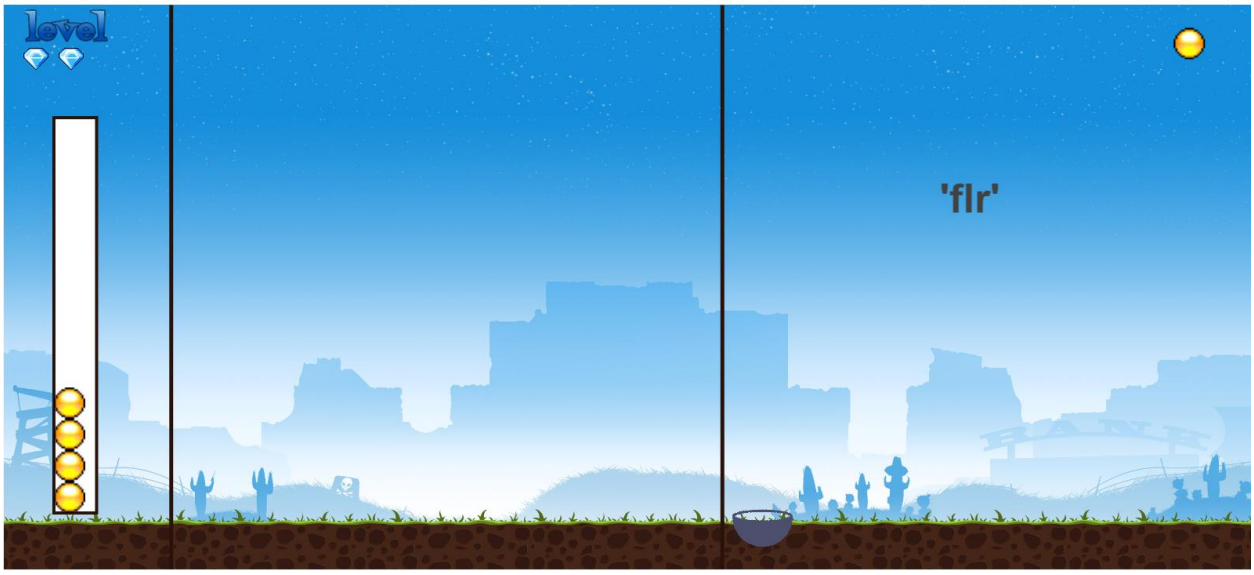


Fig 14: Game level 1 with chunk 2

5. After completion of the first 2 chunks, both the chunks will now appear simultaneously but this time the hints will not be shown. Instead, the hints will appear in order after the ball falls below a certain level.

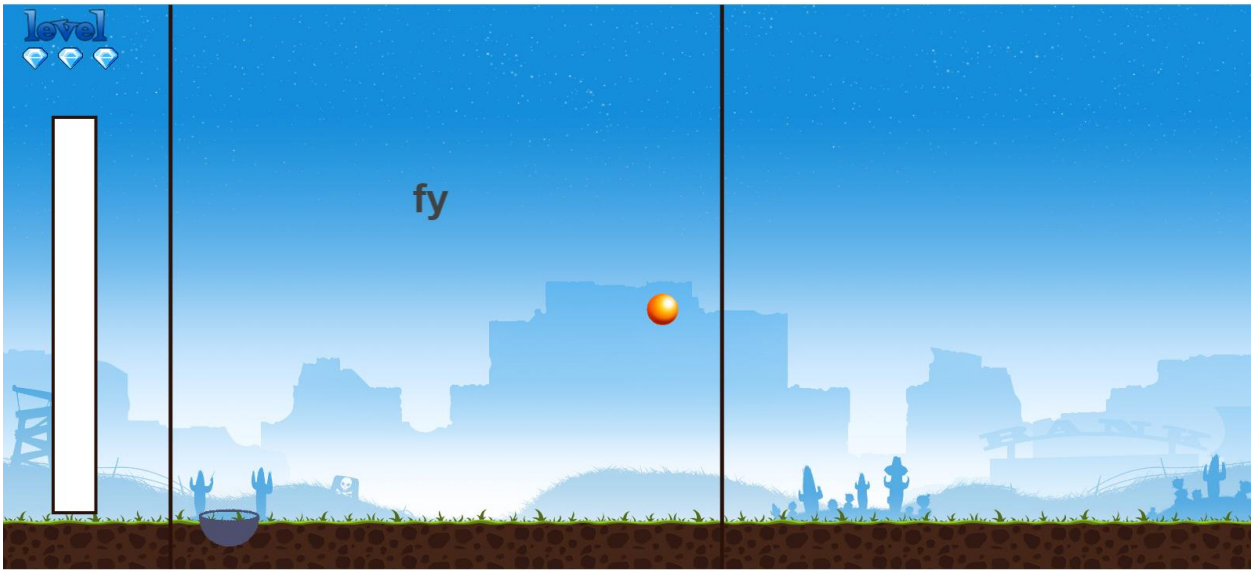


Fig 15: Game level 2 with 1st chunk and hint

6. After the game is completed, the system checks if user memorized his password or not and prompts the user to enter the entire password.

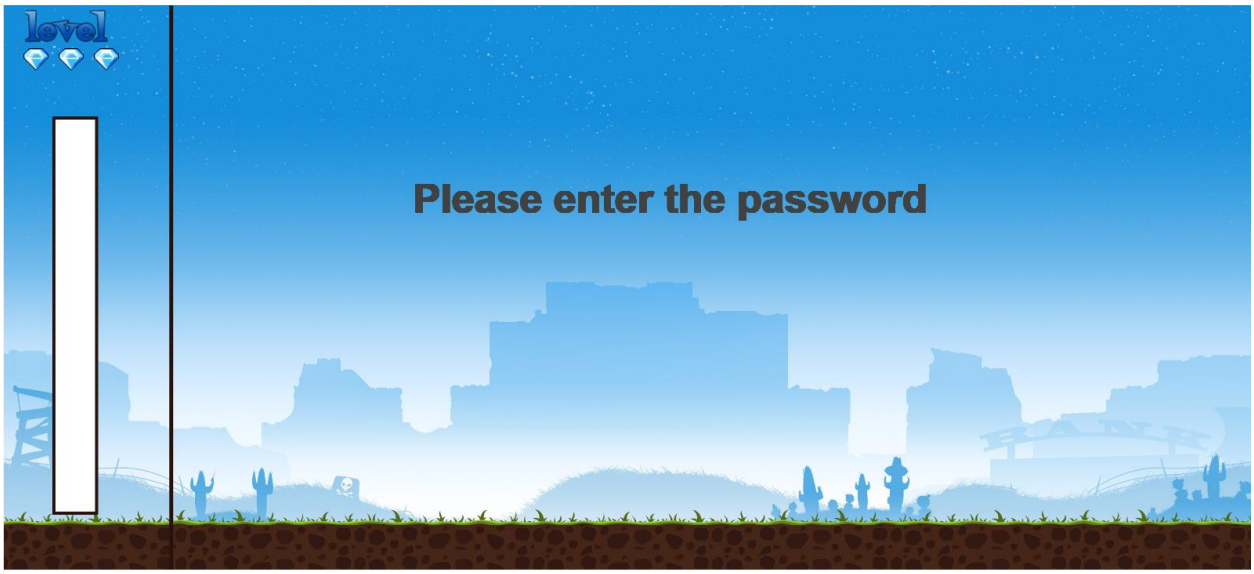


Fig 16: Password prompt in the game

6. Analysis

We tested this game on 7 participants. Our study involved 2 phases:

1. 1st week for system registration and playing the game for memorization.

2. 2nd week for simply logging in to the system with your registered email address and system assigned password allotted to user in week 1.

We gathered several data from the users such as number of errors committed while playing the game, time taken by users to complete the entire game and feedback from them about the system. We found that the most of the errors committed by the users was during the 3rd level, where the hints were not displayed. The analysis we did was as follows:

Fig 17: Chart depicting errors committed in each level

We saw a decrease in time taken by users to complete the entire game as compared to Phase 3 Pilot study. So our plan to improve the game design from Phase 3 worked. The analysis of the time taken by users is as follows:

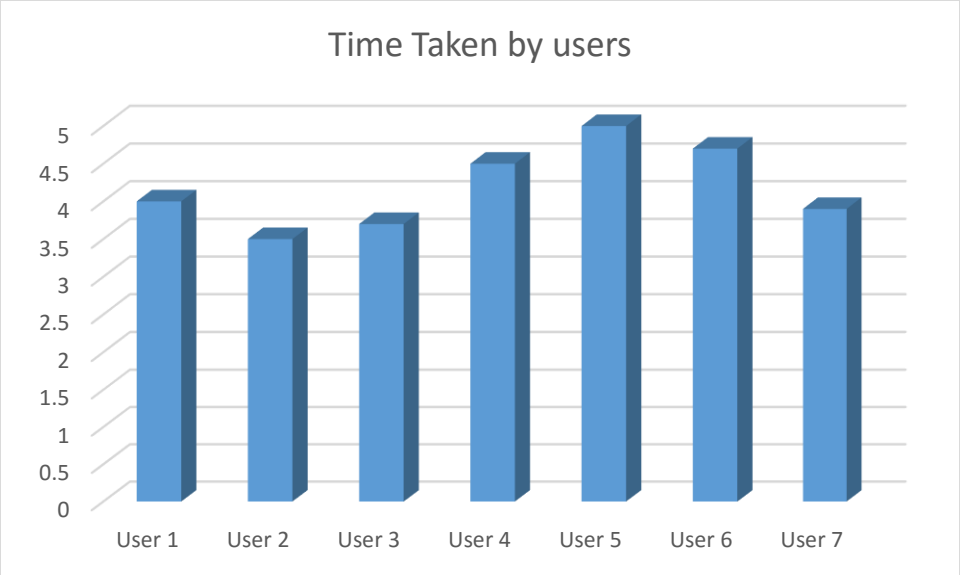


Fig 18: Chart depicting time taken by users in final study

All of our participants were able to correctly recall the system assigned passwords after 1 week.

7. Conclusion

After performing several changes in our system design and by performing user studies, we came to a conclusion that system assigned passwords can be memorized by users by letting them play a suitable game. It's also possible for the users to recall these passwords 1 week later.

8. Future Work

In future we plan to extend our system to support system assigned passwords of length 12 which not only includes alphabets but also alphanumeric characters and numbers.

9. Acknowledgement

We are pleased to acknowledge the valuable guidance provided by Dr. Filia Makedon for this project. She has motivated us and has been a driving force for our project.

We are also thankful to Michalis Papakostas, GTA, for his feedback throughout the semester to improve the project. The class's contribution in giving feedback is also much appreciated

10. References

1. Jermyn, I., Mayer, A. J., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999, August). The Design and Analysis of Graphical Passwords. In Usenix Security.

2. https://news.usc.edu/87361/does-poetry-hold-the-key-to-more-secure-passwords/

3. Al-Ameen, Mahdi Nasrullah, and Matthew Wright. "A comprehensive study of the GeoPass user authentication scheme." arXiv preprint arXiv:1408.2852 (2014).

4. http://getbootstrap.com/

5. http://phaser.io/

6. https://www.mongodb.com/

7. https://aws.amazon.com/ec2/