Striking a balance between Password Strength and Memorability to Improve Information Security

By

H.M.S.P.K. Chandrasiri

(2013/IS/005)

H.M.G.C.Herath

(2013/IS/019)

J.N. De Wansa Wickremaratne

(2013/IS/065)

This dissertation is submitted to the University of Colombo School of Computing

In partial fulfillment of the requirements for the

Degree of Bachelor of Science Honours in Information Systems

University of Colombo School of Computing

35, Reid Avenue, Colombo 07,

Sri Lanka

December 2017

Declaration

I, H.M.S.P.K. Chandrasiri (2013/IS/005) hereby certify that this dissertation entitled is entirely "Striking a balance between Password Strength and Memorability to Improve Information Security" my own work and it has never been submitted nor is currently been submitted for any other degree.

……………………………… ………………………………………………..

Date Student's Signature

I, H.M.G.C.Herath (2013/IS/019) hereby certify that this dissertation entitled is entirely "Striking a balance between Password Strength and Memorability to Improve Information Security" my own work and it has never been submitted nor is currently been submitted for any other degree.

……………………………… ………………………………………………..

Date Student's Signature

I, J.N. De Wansa Wickremaratne (2013/IS/065) hereby certify that this dissertation entitled is entirely "Striking a balance between Password Strength and Memorability to Improve Information Security" my own work and it has never been submitted nor is currently been submitted for any other degree.

……………………………… ………………………………………………..

Date Student's Signature

I, Dr. C.I. Keppetiyagama, certify that I supervised this dissertation entitled “Striking a balance between Password Strength and Memorability to Improve Information Security” conducted by H.M.S.P.K. Chandrasiri, H.M.G.C.Herath and J.N. De Wansa Wickremaratne in partial fulfillment of the requirements for the degree of Bachelor of Science Honours in Information Systems.

………………………………………..	………………………………………………………
Date	Signature of Supervisor

I, Dr. Kasun De Zoysa, certify that I supervised this dissertation entitled “Striking a balance between Password Strength and Memorability to Improve Information Security” conducted by H.M.S.P.K. Chandrasiri, H.M.G.C.Herath and J.N. De Wansa Wickremaratne in partial fulfillment of the requirements for the degree of Bachelor of Science Honours in Information Systems.

………………………………………..	………………………………………………………
Date	Signature of Supervisor

Abstract

Text-based passwords have been the most popular form of authentication in last four decades with estimates that around a billion password-based authentications taking place each day. However cognitive limitations restrict humans from being able to remember multiple strong passwords to meet the growing requirement, this results in users generating passwords that they find easy to remember and recall. Such password face major weaknesses primarily in the form of being predictable making them vulnerable to guessing attacks. Further memorability concerns drive users to reuse passwords on multiple sites risking further loss as a result of an attack.

In order to address the problem of password memorability and security in our research, we have presented a three-part model comprising of a password generator, password strength checker, and a memorability module. The system was tested over three iterations and improvements were done based on findings at the end of each iteration.

This system uses a unique approach to address the memorability concerns of by using a user's autobiographical episodic memories to generate phrases which act as the foundation for generating first letter mnemonic based passwords. The password strength checker evaluates generated passwords based on guessability, for this purpose we have used a widely accepted improved version of "zxcvbn" strength checker. Also, the system facilitates an elaborative rehearsal in the memory module to help users better retain the passwords, along with elaborative rehearsal we have also used spaced repetition to aid users to retain the password in their long-term memories.

The research was conducted by following a pragmatic research approach giving the necessary freedom to use both qualitative and quantitative methods since the research deals with both human factors that require a qualitative approach and certain analytical requirements that require a more quantitative approach.

Given the limited time frame we were unable to conduct a full user study when evaluating the system, hence we resorted to obtaining feedback from a limited user sample. The results from the selected sample show an overall positive response to improvements in the balance of password strength and memorability seen over each iteration. Further analysis of user feedback has shown an overall acceptance of the password generating approach.

However, it is important that a full user study be conducted taking a large population covering a broader demography in order to properly validate the effectiveness of the system and its approach.

Acknowledgment

We take this opportunity to express our enormous gratitude towards each and every individual who has offered their time and effort throughout our research.

To begin with, we would like to express our sincere gratitude to our co-supervisors, Senior Lecturer Dr. Chamath Kappitiyagama and Dr. Kasun De Zoysa for their unceasing guidance and support in the course of this study.

We express our appreciation to the external supervisor of our research Mr. Primal Wijesekara, Research Scientist at Computer Science Department, University of California, Berkeley for his expertise domain knowledge and resources provided.

We also express our special thanks to Dr. Nishantha Gunasekera, Consultant Neurosurgeon at the Karapitiya Teaching Hospital Galle for his expertise views on the research amidst his busy schedule.

Last but not least, we would like to acknowledge Dr. T. R. Weerasinghe, for her untiring efforts and all the lecturer, assistant lecturers, instructors our fellow mates of the University of Colombo School of Computing and our families and friends for all the support and motivation they have given.

Table of Content

List of Figures

List of Tables

sList of Acronyms

JTR - John the Ripper

IT1-PG - Iteration 01 Password Generator

IT1-SC - Iteration 01 Strength Checker

IT2-MM - Iteration 01 Memorability Module

IT2-PG - Iteration 02 Password Generator

IT2-SC - Iteration 02 Strength Checker

IT2-MM - Iteration 02 Memorability Module

IT3-PG - Iteration 03 Password Generator

IT3-SC - Iteration 03 Strength Checker

IT3-MM - Iteration 03 Memorability Module

Chapter 01 – Introduction

1.1 Introduction to the Problem

Text-based passwords can be considered as a predominant method of authentication which has a continued lifespan and is used by most users due to its widespread availability and understandability [1]. Information such as banking details, emails, personal and confidential information are protected from unauthorized access through password authentication [2]. Yet, with the rapid development of technology and computing power, the existing textual password mechanism is susceptible to various attacks.

Over time, the need for stronger passwords is crucial. In presence of a strict password policy, users tend to use common passwords, reuse passwords, forget or write the newly created passwords jeopardizing the security of information [3]. On the other hand, in absence of a strict policy, users find it convenient and easy to remember the passwords, consequently making it easy for the hackers to break [3]. It is evident that there exists a tradeoff between password memorability and password strength. While referring to existing studies and the state of art in the field of information security, it was evident that a number of research have been conducted so far by many researchers, organizations etc. with the aim of finding effective methods to make personal information secure.

Our research spreads across the fields of information security in password authentication, human cognition, and memory. Even though memorability and security of human-chosen passwords are two of the most focused and studied areas, still there is no effective mechanism to balance the memorability and password strength [56] which has motivated us to initiate this research. Therefore, our effort is to develop a password generator that will produce passwords which are secure as well as easy for the users to remember.

1.2 Problem Statement

Main problem

Humans have a limited capability of remembering complex passwords with large volumes of alphanumeric and special characters [4]. As a result, humans tend to use passwords that are easy to retain and often repeat the same password for more than one instance to provide authentication. However, these passwords tend to be vulnerable as they are susceptible to various security risks, and may result in compromising overall user/organizational information security.

Sub problems

What impact does various human factors have on password creation?

- Human memory varies on various factors, primarily age, further words and phrases that different people find easy to remember are subjective and varies from person to person based on a broad variety demographic factors such as age, education, culture, background, languages, interest.

How do password policies add restrictions on password creation and support guessability?

- Presence of a password policy can add limitations to the sample space of passwords created by a user. Complex policies cause users an inconvenience to create and remember passwords. As a consequence, users are compelled to create passwords simply to comply with the policy which leads users to use common patterns resulting in passwords being vulnerable to cracking. Furthermore, attackers are compelled to make use of the password policies when initiating a breach against passwords.

How can an easy to follow password guideline be created to support research objectives which described in Section 1.4?

- How can an easy to follow password generating system be created to that can balance password memorability and security.

1.3 Scope & Limitation

In the process of finding the solution to the main problem of the research, attention will be directed towards creating a text-based password generator that creates personalized passwords that are both strong as well as memorable. Alternative solutions such as storing, hashing or encrypting methods are not being taken into consideration.

An extensive literature review will be conducted to obtain the necessary data and information that can be used for this research. The literature review will cover research related to password security, existing research on password generation and human psychology. The findings from the literature review will be used in order to create different password generating methods, furthermore, findings from the literature review will be used to justify research approaches, assumptions, and assertions when appropriate.

For the purpose of developing the password generator and any accompanying development requirements, open source tools will be obtained and modified to fit the requirements of the research. In the absence of a suitable open source program, the development will be done from scratch.

User studies were conducted by using a limited number of consenting students from the University of Colombo School of Computing. Based on the feedback from these studies and literature reviews, required alterations will be made to the password generating methods and the system.

Research Limitations

Since our final solution is easy to use personalized password generating system, we address only the security of the resulting passwords and the memorability of the resulting passwords. While emphasizing on the above-mentioned fact, limitations of the research can be stated as follows,

1. Relying on secondary data in making justifications, assumptions and assertions.
2. Use of limited user testing to evaluate password generating methods.
3. Use of limited user testing to evaluate password memorability techniques.
4. Validity and reliability of the final solution cannot be reasonably concluded until a full user study is conducted.

5. Password storage solutions such as hashing and encrypting techniques will not be considered.

1.4 Research Goals & Objectives

Research goal

The primary goal of our research is to balance the memorability and strength of text-based passwords by developing a system that is able to generate personalized, strong and memorable passwords for the user and aid the user to retain the password.

Objective 1

Perform a full background review of research and surveys in related fields and obtain an understanding of the current state and key problems faced and identify reliable data that can be used as secondary data for the research.

Objective 2

Build a suitable model for password generation combining both established and accepted memorability models and security models that balance memorability and security by addressing the arising trade-offs, based on research findings.

Objective 3

Develop a password generating application that supports both secure password generation and memorability testing based on the developed password generating model.

1.5 Methodology

Research Approach

The research took a pragmatic research approach to meet the main objectives of the project since this approach gives researchers the freedom to use qualitative and quantitative methods. This less formal approach gives the ability to deal better with research participants since the research will have to look into patterns in human behavior hence qualitative techniques need to be employed. Quantitative methods were used to analyze results on the effectiveness of the deliverables. The freedom and flexibility allowed by the pragmatic research approach will allow moving between quantitative and qualitative techniques required to effectively address the objectives of the research topic.

1.6 Outline of Dissertation

- Chapter 02 - Literature Review Chapter comprises of the literature review and analysis of state of the art.
- Chapter 03 - Design Chapter of the research presents the methodology and the research design which we have adopted and the qualitative and quantitative data analysis of the research.
- Chapter 04 - Implementation, Results & Findings Chapter comprises of detailed explanations on the implementation of the password generators, password strength checkers and the memory module, the results, and findings for each iteration which was carried out.
- Chapter 05 - Evaluation and Discussion Chapter discusses about the results achieved in the research, consistency of the results with prior research done in the field and the contribution that we have made.
- Chapter 06 - Conclusion Chapter highlights the importance and the novelty of our research providing a conclusion to the research.
- Chapter 07- Future Work Chapter presents future work to the research and the password generating system.

1.7 Definitions

- ***Mnemonic -*** A system such as a pattern of letters, ideas, or associations which assists in remembering something [5]
- ***Memorability -*** The quality of being easy to remember or worth remembering
- ***Security Model*** - Different approaches and techniques related to security and password authentication
- ***Memorability model -*** Different approaches and techniques related to human memory from human psychology
- ***Memorability Module -*** The component in the proposed system that is responsible for helping users rehearse and memorize the generated password
- ***Password Strength -*** Measure of the effectiveness of a password against guessing or brute-force attacks
- ***Guessability -*** Time needed by an efficient password-cracking algorithm to discover a password [6]
- ***LUDS estimation -*** The Count of Lowercases, Uppercases, Digits, and Numbers
- ***First letter mnemonic password*** - Combining the first letters of each word in a phrase to create a seemingly random password [7]
- ***Candidate password -*** Set of passwords generated by applying mangling rules to a first letter mnemonic password

Chapter 02 – Literature Review

2.1 Security

2.1.1 Introduction

Access control plays an important role information security. It is the means by which valuable resources and sensitive information are protected from unauthorized access and harm. Access control comprises of four main parts [8] namely, Identification, Authorization, Accountability and Authentication. Among various authentication methods text-based passwords are the oldest and most common method of authentication based access control [9][2]. Text-based password authentication is easy to learn by the end user and also quite easy to implement contributing to its popularity [10][11]. However, text-based passwords are notoriously vulnerable to attacks such as brute force attacks and dictionary attacks, mainly due to the fact that user tends to select weak passwords since they are easier to remember and more convenient to use [2]. Furthermore, user tends to share passwords or store passwords using insecure methods (such as writing down passwords) leading to more risk associated with password-based authentication. There are many guidelines available giving users advice on how to create secure passwords however users tend to dislike these guidelines since they make passwords less user-friendly [12]. However, it is important that the security of passwords is not overlooked since secure passwords are what keeps systems safe from unauthorized access and protect sensitive user information

2.1.2 Outlook on Logical Access Control

Access control is the means by which access can be allowed or restricted from either physical assets, locations or systems. This helps protect resources from unauthorized access and abuse and ensures that only persons allowed to use the resources can access them. Access control can be broadly divided into two categories based on the nature of what is being accessed as [8], physical access control which controls access to physical assets and location such as buildings, server rooms, offices, etc. and logical access controls which controls access to operating systems, applications, networks, etc. In most computing environments logical access control plays an important role in ensuring that only authorized persons can access information and perform operations (view, update, delete, etc.) on data and information stored in the system. A proper implementation of access control comprises of four main parts [8] namely, Identification, Authorization, Accountability and Authentication.

The first step of a successful access control enforcement is the implementation of proper identification [8] [13]. Identification is the assertion made by a user, process, or other entity about who they claim to be, this claim is made with the intention of gaining access to resources. The most common identification method currently in use is the username, which can be a user ID, account number, e-mail address, etc., furthermore, identification also includes various bio metric methods such as fingerprints, voice and facial recognition, DNA, etc.

Authorization is a process by which an organization determines which users have access to which resources, in most organizations authorization is determined by job role and when determining the level of access granted it is recommended the adoption of the principle of least privilege, which states that when access is granted only allow the bare minimum of access required to perform necessary functions [13]. Once an authorization policy is in place when users request access to various resources, access controls can enforce the policy rules and determine whether to accept or reject the request.

The principle idea of accountability is to keep track of actions of users and processes when using system resources [8][1]. Accountability is typically implemented by recording users and process activity on log files, which can record login and resource usage history. Accountability plays an important role in the prevention detection and monitoring of system access [8].

Although Identification provides the means to make a claim of the identity of a user or process it does not provide any validation of the claim to be true [13]. In order to do so, systems are designed with a layer of security requiring the establishment of identity known as authentication. There are 3 types of authentication [8] [14] namely knowledge-based authentication, ownership-based authentication and characteristic based authentication.

Knowledge-based authentication is where the user must provide something they know such as a password, PIN number or passphrase in order to access the system. The most common form of authentication in place today is text-based passwords [15], it is estimated that there are over a billion password-based authentications per day [16], despite their poor security and usability text-based passwords remain widely available and the easiest to understand for end users, something that will not change for any time in the near future [1].

Ownership based authentication is where the user can use something they possess such as a smart card, token(synchronous/asynchronous) or badge in order to gain access. A smart card based authentication system will use a smart card that goes into a computers card reader or a dongle that will go into a computers USB drive. Smart cards have their own processing capabilities and store a private key associated with the user and often requires a PIN to sign into the smart card. Although smart cards are considered essential in public key infrastructure environments they have not been deployed widely due to the higher cost of infrastructure requirements [16].

Characteristic-based authentication where the user will identify themselves via a unique characteristic (often physical) such as fingerprint, retina or voice. The oldest, widely researched and most deployed biometric at present is the fingerprint scan [16]. Fingerprint scans are low cost, easy to use since very little training is required, has low error tolerance, fast transaction times and can provide higher level of accuracy by enrolling multiple fingers [16]. However, this technology is not without some significant weaknesses, the use of dummy fingerprints created from latex or manipulating scanners to use latent prints further fingerprint scanners require frequent maintenance, may not be suitable for persons with disabilities such as tremors and missing limbs.

2.1.3 Current Outlook on Popular Authentication Methods

At present text-based passwords also known as alphanumeric passwords are the most popular form of authentication [9][2] which has been in use as a means of authentication for the last 4 decades [11]. Text-based password systems require users to create a password which may consist of letters, numbers and special characters, once the user has created a password it is stored in a database either in plain text, cipher text or as a hash. When a user wishes to be authenticated they will enter their password which is compared with the stored value, and if the values are an exact match the user will be granted access.

The reason for the popularity of text-based password authentication is because they are easy to implement with small associated costs and less technical complications while providing simplicity and understandability for most end users [10][11]. Text-based password is largely used in gaining access to computer operating systems, application and websites, with the rapid development of e-commerce there has been an increase in the number of password protected sites [17] and Forrester research reports that on average web users manage 15 passwords daily [18] for authentication purposes. Although text-based password authentication is very popular they are riddled with many vulnerabilities, which has resulted in many studies directed towards looking for a more secure alternative to replace it.

Two-factor authentication is a method by which two types credentials are used to authenticate a user or process [8], typically two factor authentications is used to authenticate access to high-value accounts such as in banking and finance applications usually as a combination of a password and a system generated security token [19] [20].

The case in support of two-factor authentication is that single factor sign-on is no longer a safe means for authenticating users since if the single factor, which in most cases is a password is stolen it will result in a compromise, in such a case an additional authentication factor acts to enhance the overall security of the authentication process [21]. Security tokens for two-factor authentication can be sent via e-mails and SMS or can be implemented using digital certificates, PIN cards, RSA tokens, USB tokens, etc [20-22]. In a typical system that utilizes mobile phones for two-factor authentication, after a user has successfully entered the password an authentication code will be sent via SMS or to a trusted mobile application which the user must input into complete the authentication process.

In the past few years, Graphical passwords are have received significant attention as a means of authentication and studies have been conducted to see if graphical passwords are a suitable alternative for alphanumeric passwords. Graphical passwords authentication is achieved via the use of one or more graphical images which the user must interact with using actions such as mouse clicks, drags and touch in order to input the password. Graphical passwords are seen as a suitable replacement for alphanumeric passwords because people find it easier to remember and recall graphics as opposed to text which has been established by the Picture Superiority Effect Theory, a substantiated theory in psychology [23].

Graphical passwords are broadly categorized as recognition-based and recall based [23][10][24]. Recognition based systems require users to recognize a previously seen image in order to authenticate themselves. A typical implementation of a recognition based system will get users to select images beforehand and when the user wishes to authenticate themselves the system will show a variety of images from which the user must recognize and select the images they originally selected. Some popular implementations of recall based systems include the Passfaces method by Real User Corporation [25] and the Déjà vu method by R. Dhamija and A. Perrig [26]. Recall based systems are further categorized into the cued recall and pure recall based systems. In cued recall based systems users will select and click on specific points on an image to authenticate themselves, the PassPoints[27] technique is a popular scheme used to implement cued recall based systems. Pure recall based systems require users to draw an image from memory in order to authenticate themselves, a popular implementation of this system is the Draw-A-Secret(DAS) [28] scheme. Graphical passwords have been implemented in authentication of mobile phones, ATMs and certain E-transaction sites.

Biometric authentication is a means by which authentication is achieved by identifying a person using features and characteristics that are unique to that person, which can be either physiological or behavioral. Physiological characteristics are physical characteristics/features of the human body which static in natures and difficult to forge or replicate, examples for these include Iris, fingerprints, retina, DNA, etc. Behavioral characteristics on the other hand are less static and are highly affected by the users present state of mind and body, examples for these include voice recognition, signatures, typing patterns, etc. [29][30][31][16].

Biometric authentication is widely accepted as a more secure form of authentication. In biometric authentication, fingerprints are the oldest and most popular form of authentication implemented [2, 31]. Fingerprint authentication obtains a fingerprint minutiae using a feature extraction software and stores the fingerprint as a template in a database to be used for authentication. The fact that fingerprint-based authentication can be implemented quite easily and relatively cost-effectively along with a False Non-Match Rate (FNMR) of around 2% and a False Match Rate (FMR) of around 0.02% [16] has contributed to its popularity.

2.1.4 Vulnerabilities Associated with Text-Based Password Authentication and how they are attacked

With the wide application of text-based password authentication systems, many attackers have realized the importance of bypassing password security since it acts as the barrier which controls access to important information assets/resources. Alphanumeric passwords face major risk such as being accessible to system administrators, the risk of undetected theft, the risk of undetected sharing, the risk of weakest link which where users repeat the same password across multiple sites, risk of guessing and offline dictionary attacks and brute force attacks, attacks from malware such as keyloggers to name a few [2].

Studies have shown that human has limited cognitive capabilities in their long-term memory to store and recall multiple complex passwords [17] which result in usability issues that eventually leads to various vulnerabilities in user-generated passwords. In human psychology the *Power Law of Forgetting* [32] states that humans forget rapidly in the short term and forget at a slower rate in the long term, this theory can be viewed as an indication as to why users tend to forget the passwords they create. As a result of forgetting passwords, users tend to create passwords using strategies that make passwords easy to remember, but these passwords tend to be less secure when viewed from a security standpoint being easily predictable [8][19][33][9][24].

A study conducted by Carnegie Mellon [8] University [34], with the intent of identifying common password creation patterns of the user and their understanding of password strength. In this study researchers found that participants had their own well-defined process of creating their passwords, where many of these strategies resulted in the creation of predictable passwords, in addition to this most participant had used similar strategies such as using words inspired by the website, words the participant associates with the website, people they associate with the website and common character substitutions among others. Although the passwords generated where exceeding the required character limit the strategies used by participants made the passwords that were generated vulnerable to automated guessing attacks. Furthermore, the researchers found that participant had many misconceptions about what makes a password secure. Participant had little knowledge and fear of larger scale guessing attacks and focused more on attacks directed towards them, leading them to believe information not readily available on social media such as Facebook (example: pets name, birthday) can be used to create a good password. In addition to this participant believed harder to spell words, unpredictable phrases, first letter capitalization, the addition of a single special character or number to the end, using common keyboard patterns where some of the many identifies misconceptions users had generally resulted from misunderstanding currently available security advice.

Even when users create and remember strong passwords they have the tendency to reuse the same password across multiple sites since they find it difficult and inconvenient to create and remember complex passwords [21][23][24]. This results in a domino effect, where when one site is compromised and the password is stolen it puts all other sites that are using the same password at risk, meaning that even the most secure accounts are only as secure as the least secure account the password was reused in. A study on the domino effect of password reuse [17] emphasize the effect of growth e-commerce has on the increased need for passwords resulting in the large-scale reuse of passwords across sites and applications and the severe financial and other loses to both individuals and organizations as a result of password breach.

When it comes to attacking passwords some of the main attacks identified were [8][9][13][33][23][24], dictionary attacks, brute force attacks, keyloggers and phishing attacks. Dictionary-based attack is where attackers use large dictionaries to try and find the users password [8][10]. In a study conducted by Joseph Bonneau [35], the evaluations of results of various dictionary attacks conducted in the past studies concluded that most studies have been successful 20% - 50% of the time when dictionary size range from 20^{20}– 20^{30}.

A brute force attack is an attack in which a large number of combination of alphanumeric and special characters are used exhaustively to try and match the password [10,15]. The more complexity and entropy the password has the harder it is to guess using a brute force attack. [10]. In a study [36] conducted on the crackability of 145 million passwords using 6+ state of the art cracking algorithms concluded that depending on the method used and the amount of training data given to each algorithm they were able to crack passwords at a rate exceeding 55%. The researchers made the recommendation that when creating passwords longer passwords are preferred to shorter passwords and passwords should comprise of a mix of characters with uppercase, lowercase, special and numeric characters in order to be more resistant to attacks such as brute force attacks.

2.1.5 Password Strengthening Techniques

In order to help to users to create strong passwords, various policies have provided different parameters to create passwords. A password can be deemed strong if the password meets characteristics such as containing 12 – 14 alphanumeric characters with both upper and lower case letters with at least one number (0-9) and at least one special character (for example: ! @ $ % * / { } [ ] ( ) < >), free of character repetitions, keyboard patterns, sequences, dictionary words, not containing information that is publicly associated to the user [12][40]. The following of such practices may help improve the entropy of passwords which in turn the overall strength and resistance to guessing attacks such as brute force attacks[35]. The SANS password policy[41] provides recommendation such as having a minimum of 12 characters, having both upper and lower-case characters and at least one numeric and special character. The policy also provides some advice on what not to select as passwords such as any personal information such as birthdays, phone numbers names, etc., passwords should not contain any work-related information such as building names, systems commands etc., avoiding the use of patterns, spelling words backwards and simple passwords such as "password123".

However, studies have shown the use of such passwords can have negative impacts on the users resulting users forgetting passwords, this leads users to follow insecure patterns in creating passwords making them vulnerable as a result [12].

2.1.6 Password Strength Evaluation

Evaluation of the strength of a password is a crucial factor in the password-based authentication. [42] The main objective of strength metric is to predict the guessability of a given password. "Guessability" is understood as the easiness of the predictability of a password [43].

Yet, current methods which have been widely used lack of accuracy due to many reasons such as the inability to capture the complex patterns due to the simplicity of the heuristic rules etc. Different mechanisms used in sites ensure the acceptability of the user chosen-passwords through evaluation of the strength of the passwords. [42]

Password strength evaluation methods can be categorized into three main groups namely, Attacked based methods, Heuristic-based methods and Probabilistic based methods [43].

Attacked based methods: This method estimates the time taken to break a password using a specific mode(s). Longer the time taken, stronger the password is. Most commonly used methods under this category are dictionary attacks, Brute Force attacks.

Heuristic-based methods: These methods make use of heuristic rules to predict the complexity of a password. Few such methods are Shanon's entropy calculation, NIST entropy, LUDS estimation (low-case, upper-case, or digits) etc.

Probabilistic-based methods: Probabilistic based methods exploit the lack of randomness of the user chosen passwords. Statistical evaluations of password datasets have been used to derive the relationship between the password and probabilities and most of these methods are based on Markov models.

Entropy calculation

One of the most discussed approaches of measuring the password strength found in literature is information entropy or the randomness/uncertainty associated with a randomly chosen word or a secret [42]. The notion of entropy was first introduced by Claud Shanon in 1949. [43]. Entropy value for a given password expresses the quantitative value of the unpredictability of a password expressed in terms of bits [44].

The entropy of a randomly generated password is measured using the following equation [44],

$$H = \log_2 (b^l) \rightarrow (2.1)$$

H = entropy in terms of bits

b = number of characters in the password

l = Character space (alphabet) used to create the password

As expressed by this equation if a password of length 8 was generated at random from an alphabet of 94 characters (printable ISO characters on a typical keyboard), the entropy is $94^8 \approx 6.09 \text{ x } 10^{15}$ which is roughly equal to 2^{52}, such that giving entropy of 52 in terms of bits. Entropy calculation has been used by many studies yet, none of these studies have calculated the strength for passwords distributions correctly [43].

The NIST Model of Password Entropy

NIST has introduced a set of entropy calculation guidelines to estimate the password strengths. [42] [44] Entropy calculation is based on Shanon's work and it assigns an entropy value for the password using the following criteria [44].

- The entropy of the first character is taken to be 4 bits
- The entropy of the next characters is 2 bits per character
- For the 9th through the 20th character, the entropy is taken to be 1.5 bits per character
- For character 21 and above the entropy is taken to be 1 bit per character
- A bonus of 6 bits of entropy is assigned to a composition rule that requires both uppercase and non-alphabetic characters.
- A bonus of up to 6 bits of entropy is added for an extensive dictionary check.

In addition, NIST guidelines introduce two levels of security levels which finds the acceptable number of guesses an attacker should carry out to guess the random password based on its entropy.

Level 1: Number of Allowed Attempts = $2^{H(x)}$x 2^{-10} (1 in 1024 chance of compromise)
Level 2: Number of Allowed Attempts = $2^{H(x)}$ x 2^{-14} (1 in 16,374 chance of compromise)

For an instance if we consider a seven-character password with at least one symbol and one uppercase letter the entropy would be = 4 + 2 + 2 + 2 + 2 + 2+ 2 +6 = 22 bits. Therefore, according to the NIST's security level 1 definition, the minimum number of guesses allowed is $2^{22} \times 2^{-10}$ (2^{12} after the simplifying).

However, studies have empirically proved the guideline to calculate the entropy of a password as proposed by NIST is not an effective metrics to be used [42] [43]. it was also proven that the current NIST measurements overestimate the strength of a password.

Markov Models

An alternative metric of password strength is Markov models. This was first introduced by Narayanan and Shmatikov in 2005 which predicts the next occurring character with respect to a probability value which was derived from the previous characters of the password considered. [47] Markov models predict the strength of passwords more accurately than rule-based mechanisms.

The idea behind Markov models is that the adjacent letters of a human chosen password are dependent on each other. (eg: the 2-gram “th” is much more likely than “tq” and the letter e is very likely to follow “th”) Therefore in a n-gram Markov model, the probability of the next element of the password considered is modeled based on a prefix of length “n”. [42]

Many variations of Markov models have been evolved with time [48]. Zero-order Markov model is the simplest form available and it is quite similar to the letter frequency analysis for a given language. Similarly, Markov models can be extended as First order, Second Order, third order and so on, but it is rarely seen models above Second order being used as models for strength evaluation. [45]

Researches by Duermuth et al. and Ma et al. have evaluated these variant models with large sets of leaked password dumps. As per the results of these evaluations, it was found the effectiveness of the guessability for a particular dataset is dependent on the configurations of Markov models adopted [48].

Both john the ripper and Hashcat provide Markov model based cracking modes in their cracking toolkits. [48]. The mode is basically based on the assumption that “*people can remember their passwords because there is a hidden Markov model in the way they are generated*” [93]

In addition to above mentioned methods, “Blacklist Evaluation” approach is another increasingly popular password strengthening metric. In researches conducted by Weir [45] and Schechter et al.[6] suggest a blacklist check can be adapted to rejects weak passwords and may provide more security than specifying password creation policies.

2.2 Human Memory

2.2.1 Introduction

Memory is the ability of the brain to encode, store, retain and consequently recall the information and past experiences from the brain [49]. The human brain has billions of neurons where each neuron forms about thousand connections with each other adding up to about trillion connections overall [50]. The interconnected web of neurons will increase the memory capacity thus creating the possibility of remembering many memories in your brain at a time [50]. Investigations and research have been carried out to learn how the brain works, how much memory storage a human brain can possess, how humans recall information and past events etc. in order to unveil the mechanisms and the potential of the brain.

2.2.2 Mechanics of Human Memory

Information that we capture and store by our brain can have a number of forms and the type of memory to which this information falls depends on how long we retain the information in our brain. Human memory can be mainly categorized as follows,

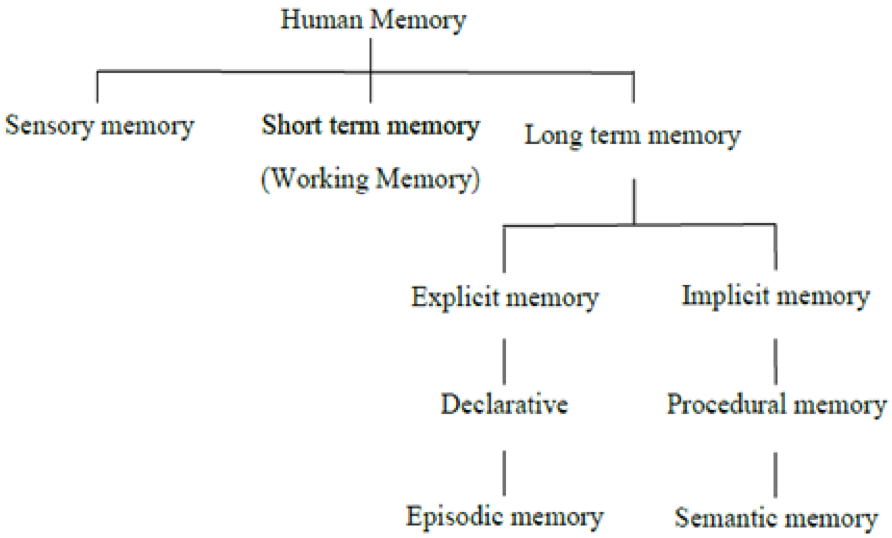


Figure 2.1 *- Types of memory*

When a person senses a stimulus (person, image, event etc.) as important, an electrical message is sent by the neurons in your brain. This process is called as encoding [51]. Once encoding is done, information captured by the brain is stored for retrieval.

Retrieval of stored information from the memory is highly influenced by how information is encoded by the brain. Few factors that influence the encoding process are the level of processing pertaining to an item, timing of practice, person's reference at the time of self-learning of the event or information, organizing the structure of information by the person, the level of distinctiveness of information encoded by the brain etc. [52].

The levels of processing are classified as deep processing and shallow processing. The levels of processing of information will range between these two levels based on the instructions given or the level of elaboration. In shallow processing, the brain tries to remember the physical features such as length, color, shape of the item or the event to be remembered rather than its meaning. As an example, we see coins every day yet we find it difficult remember each and every finite information written in the coin. Repetition of such physical information of an event through shallow processing will not support the human's memory to remember information for a long period of time [52]. In contrast, deep processing will create logical reasons to the information that is to be remembered with the existing knowledge of the person. A meaning is created by the brain using the new and old information to elaborate the on the information. When memorizing a new word human tend to remember the word by associating the word with something that you already know.

An individual may remember information for a longer period when it is studied repeatedly in multiple times spaced out in time rather than trying to memorize the information in one or two crammed sessions that are longer and exhausting [52].

Encoding information and elaborating them around one self's experience and knowledge makes it easier to access the information fast from the memory as it creates elaborative and salient cues to information that has to be remembered [52].

In a lake with an uncountable number of white swans, if a black swan was found among them, it will be remembered by anybody as it is distinct and unique compared to other items found among it. Similarly, if an item or event is significant and prominent to an individual, such information is retained in the memory for a longer period of time [52].

Cues can be created to recall information by categorizing information and organizing them under different topics. These topics will act as cues to the information that is stored under the given topic which facilitates easy memorization and easy retrieval of information [52].

Conway and Pleydell-Pearce's concept of event-specific knowledge which is also known as an episodic memory for authentication is salient and is an ideal approach. Episodic memory is easy to be recalled by the user and on the other hand, hard for strangers to discover or guess. [53]

2.2.3 Stages of retrieval

In a general idea, information retrieval from the human brain involves three stages. These stages are producing the retrieval cues as per the stimulus, retrieving information based on the cues and finally verifying the retrieved information [54]. These three stages may follow an interactive process rather than being a single cycle.

Long-term memory of a human is a vast collection of episodic memory traces. For each and every episodic memory created by an individual will have a separate trace disregard of its similarity to other episodic memories. When retrieving information from the long-term memory to working memory, two elementary operations are activated. A retrieval cue which is called a “probe” is created by the working memory and is sent to the long-term memory with respect to the information that is to be retrieved from the memory. Once the probe is received by the long-term memory, an “echo” is created by the long-term memory and is sent back to the working memory. An echo consists of the collection of all the memory traces which has the highest similarity to the probe sent by the working memory. The selection of traces is done through simultaneous matching of the probe with all the other memory traces in the long-term memory and based on the degree of similarity memory traces are combined parallel to make the overall contribution to the echo sent by the long-term memory to the working memory [55].

2.2.4 Strategies for Memorization and Recall of Phrases & Words

The study of human memory is more or less a study of a black box which is a limiting factor in designing memory models [54]. However, from general studies of human memory Peter W. Foltz [54] suggests that information retrieval from the human brain involves three stages. These stages are producing the retrieval cues as per the stimulus, retrieving information based on the cues and finally verifying the retrieved information. These three stages may follow an interactive process rather than being a single cycle.

A paper by Wijesekara et al. [56] suggests that humans tend to recall information or words quite easily when this information are blended with autobiographical episodes of an individual. When an individual uses episodic memory to recall information, the so called personal landmark acts as the retrieval cue which activates the memory traces of the event or the experience of the individual which ultimately increases the recalling ability of information.

Chunking of information is a technique used by chess players, waiters in restaurants to remember information they are dealing with. Chunking is the process of organizing information into small chunks or units of familiarity which are also manageable and memorable [52]. When a chess player is given five seconds to memorize the arrangements of a set of chess pieces, they nearly remember all the chess pieces and their arrangements. Yet, once when the arrangements are created with a meaningless and in a random manner, despite being a chess expert, every chess player fails to remember those arrangements [52].

Also, people tend to remember images more than words [56]. This finding is named as picture superiority effect. Nelson et al. suggest in their paper, that image-based mnemonics can be used improve the memorability of the passwords, thus increasing the security of the passwords used for security [56].

Words or phrases generated by oneself are more memorable than the words that are already found in the vocabulary [57]. This effect is known as the “generation effect”. For an example, when a team is asked to come with their own team name for a given teamwork, they come up with their own creative team name by combining words that are most relevant and represents their team mostly. Such words or phrases will last in their memory for a longer period as they appeal to themselves and to the team.

Words or phrases are likely to remember when they are more elaborative and fall under deep processing levels. When the words are remembered with a deeper and a logical meaning, these words tend to retain in the memory for a longer period of time [56].

Strategies of mnemonics also can be used in memorizing words or phrases. Mnemonics are images, events or any other object which creates a landmark for the user to remember information. Therefore, mnemonics activates deep level processing levels ultimately making the humans to remember words and phrases easily [7]. One mnemonic strategy used in password creation is a first-letter mnemonic method. A sentence is created by an individual to which has a personal meaning and the first letter of the sentence is used as the password for the user. Using a first-letter mnemonic method to create passwords will improve the memorability of the passwords by the user and motivating them to create strong passwords that are easy to remember.

2.2.5 Forgetting Passwords

In the study conducted by Brown et al. [58] to gather information about how often the passwords are forgotten or mixing up of passwords across different accounts, out of 212 participants, 31.1% of participants have forgotten their password and password mix-ups have been experienced by 22.5% of the participants. The password mix-ups were most to occur between the email address and their computer sign in.

In almost every scenario the passwords are generated by users under a hurried situation created by the policy setters and forcing the users to develop their passwords which lack meaningfulness and relevancy. This situation perfectly resembles the perfect scenario of people hiding their jewelry and valuables right before going on a trip and once they return, they have already forgotten the place where they hid their valuables. This paradox is clearly described by A. S. Brown and T A. Rahhal [59] in their study. When a person is successful in hiding something at the spur of moment irrelevant to the object they are planning to hide, it is likely to un-recall that information after some time. Similarly, the password users are contemplating between the factors of convenience in remembering the password and its strength against being hacked in the process of creating the password.

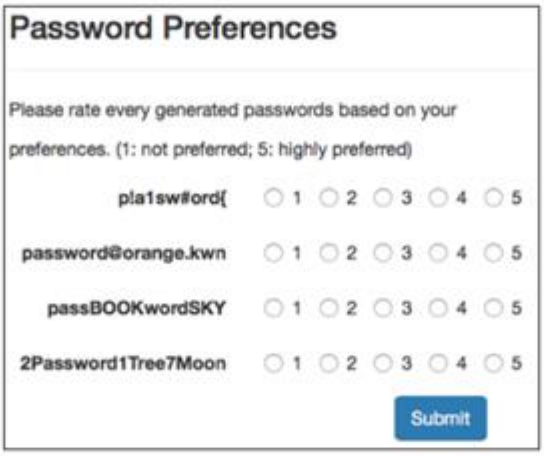
The strength of the passwords generated can be improved by composing them with numbers, special characters, uppercase lowercase letters etc. thus making it hard for the intruders to break the password as well as making it hard for the users to remember too [60]. On the other hand, memorable passwords can be generated by integrating meaningful life events or by using the knowledge that the user already knows. But retrieval of such meaning content will not be sufficient for the authorization process since passwords need to be entered in verbatim. Therefore, the process of password generation followed by users should have the characteristics of having the ability to retrieve detailed information about password and to remain in the human memory for a longer period of time.

As per Pilar et al [60], the research study conducted by the team assumed that the difficulty in remembering the passwords will be comparatively higher for adults unlike for the younger generation. But surprisingly, the research results concluded that regardless of the age; the major factor that affected the memorability of passwords is the number of unique passwords used by the user at a time. It was proved that having a number of passwords in use will increase the difficulty in retaining the information in the human memory as it increases the cognitive load associated with passwords in the brain.

2.2.6 Password Memorability Evaluation

Password security prior research are often addressed the memorability as well as the strength of the password. Most of the prior research evaluate it in short-term wise and long-term wise. According to the research of Juang et al [1], they have evaluated the memorability of the password in short-term as well as long-term. Initially, users need to participate in creating accounts and the completing some tests which are NASA Task Load Index & System Usability Scale[1]. Then they are directed to the distracted task which relates to mental arithmetic problems and then users need to authenticate to their accounts. Each user needs to create three accounts according to the research and needs to log into those accounts. The order of the login is not the order that the accounts were created. It is random. And each user has 5 attempts to log if they fail and all the attempts' details are recorded. In this way, they need to log into their all three accounts. Then users are requested to come back after a week and they should log into their accounts as the second session. Considering the records which are creation time, recall time and binary metric of either eventual success or failure logins, memorability was evaluated for proposed password mechanism.

Lyanstani et al. [61] have evaluated the ability to recall the password with a user test on the Amazon MTurk and it was large-scale online user test. Many researchers used this mechanism. In their case, users need to select the more memorable password from 4 candidate passwords and its implementation of 4 type of passwords is described in Section 2.4. And users are advised not to write down or store the password in any form. To improve the memorability of the generated password, users have the opportunity to enter password few times and then they are directed to distraction task. Also, users are requested to provide the preferences about the passwords by using Likert scales as seen in Figure 2.2 in order to identify the most used mangling rule. Also, the user has a second part that they have to log into the web site one week later and re-enter the selected password. Using these recording details and their failure records, the ability to recall the password has been evaluated.



Password Preferences

Please rate every generated passwords based on your preferences. (1: not preferred; 5: highly preferred)

p!a1sw#ord{ ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

password@orange.kwn ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

passBOOKwordSKY ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

2Password1Tree7Moon ○ 1 ○ 2 ○ 3 ○ 4 ○ 5

Figure 2.2: *Likert Scale for users*

2.3 Human Behavior & Password Selection

User behaviors for the passwords in information systems, have a straight forward influence on the level of security [62]. As demonstrated in [63], using the password mechanism was considered as "*the front line of defense against intruders*". Researchers have identified that a lot of passwords breaches and attacks occur frequently since users show the weak security behaviors [63].

Some computer users are not proficient with password practices, guidelines and proper security measures while some users may proficient with those. Therefore, users have different levels of password performance and it is influenced by a number of aspects. McCloy et al. [64] have proposed a function that can assist to measure the password performance that associated with knowledge of facts, rules, principles and procedure of a task, capability and motivation [63] According to [63], there are three determinants of a user's password performance based on above performance function. They are, knowledge which refers as the knowledge and education regarding password practices, a capability which refers the competency level of users to combine password knowledge with knowing the approach and ability to apply well password practices and motivation which refers to the driver of user's password behavior.

R. Butler and M.J Butler [63] have performed a research by applying a model to determine the password practices to targeting the South African user group. They have identified that South Africans should improve the password security by addressing all aspects of password performance and it was affected by the qualities of incompetence, ignorance and indifference. Also, they suggested that can be enhanced by providing attention to the human-computer interface, relevant education and awareness programs.

System generated passwords are secure, but those are often unusable and difficult to remember. Since it includes the usability issue, people tend to select a password by their own to increase the usability with applying the personal related details. But they are not good to provide better security for their accounts [65][1][56]. Considering general password security, they direct users to have unique and random passwords. But Duggan, Hilary and Beate [66] have found that password security has a mutual relationship with the sensitivity of the task. Users who mostly related to computer science concerned about the password security more than other users. Most users' main goal is to remember the password instead of considering the security. Mazurek et al. [67] also have conducted a study targeting Carnegie Mellon University and have identified that students who are in science and technology make passwords 1.8 times as strong as those of students who are in business schools.

Das et al.[33] have identified 43-51% of users who use internet service, reuse the same password across the websites. Blase et al. [34] have identified several reasons for reusing the same password, such as most users believe that the password is strong enough and reusing it is not a problem, difficult to remember several different passwords, some users haven't experienced negative consequences by reusing password and some of the users knew that reusing the same password is a poor idea, but they do it anyway. But above self-reported reason did not provide clear idea whether it is a wishful thinking or actual behavior of the users. Therefore, Wash, Radar and Berman [68] have done some studies connect users' password related attitudes and intention to theirs real behavior. From their studies, they have identified, users re-use complex passwords for accounts which are accessed frequently, because frequent access to the account improves the memorability.

Existing password meters for account creating process provides the representation of strength level of passwords. Also, system accounts can be divided into two major types which are important accounts and non-important accounts. Serge et al. [69] have done a study to identify whether these password meters have an impact on password selection for above two types of accounts. They conclude that users reuse weak passwords for non-important accounts and password meters do not have an influence on that behavior. The research team identified that there is a likely marginal impact of password meters for important accounts when users are forced to change existing password.

Although convenient it is recommended that users avoid practices such as password reuse and writing down passwords as they pose significant security risks. Elizabeth and Robert [70] have done studies on user behavior in managing passwords and have identified some of the major points regarding writing down passwords. Users have to manage many accounts and it is expected to have a separate password for each account. Also, they are forced to have complex passwords with policies and forced to change the password at fixed intervals. Considering these factors users tend to write down their passwords. Since it can be a simple explanation for their behavior and there can be another story behind that. Therefore, the research team has done studies to identify important patterns in user behavior. Writing passwords down is considered as to be insecure. But some security experts think it is better to do it if they can be stored and kept in a secured physical location. Many users do write down and store their password without considering a secure location. According to their analysis, most of the users have stored their passwords in their email, Dropbox and mobile phones or saved on their computer desktop [70].

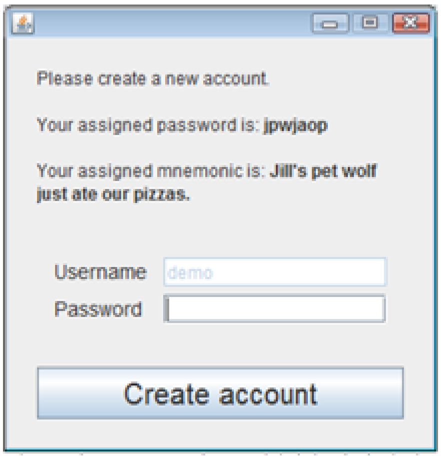
Another one of the behaviors of people that try to avoid to maintain multiple accounts with separate login is using the single sign-on. Elizabeth and Robert [70] have identified that people tend to use it without having adequate knowledge about how it works. Furthermore, they suggested having single-sign-on the service provider to provide single sign-on service only rather than sites like Facebook, Google which maintain a lot of personal information, because users feel more comfortable with using a service that does not have direct ties to their personal life and social activities.

The most systems use password-based authentication mechanism instead of many sophisticated and viable security alternatives. Kay et al. [71] have examined user password composition and security practices of email accounts and study were conducted for the business faculty in an Australian University. According to findings, they have identified all participants use two or several email accounts and also a host of computer-based software which includes password-based authentication. Users reuse the password for different email accounts and other computer-based software. One of the major issue is, users haven’t identified the risk of such weak password practices. Also, they haven’t identified the consequences related to breaches in security. The majority of the users have shown poor password composition practices. Users choose their passwords that are based on personal details that can be easily guessed by others. But they have identified employees that are working in an organization is minimizing this issue and it may be due to organizational policies. But younger participants have shown poor password practices in their study.

Furthermore, use of passwords can be affected by different age and educational background of individuals. Therefore Pilar et al. [60] have conducted a study by focusing on above concern and they have chosen ages range from 18 to 93 years and education range from grade school to graduate degree. Even though they assumed that effects of cognitive function due to aging will cause to forgetting passwords or mixed up, it was not the actual cause of it. The number of passwords is the reason for the password forgetting and the mixed up. Furthermore, findings brought out that younger educated users manage more passwords rather than old uneducated users. Furthermore, Mazurek et al. confirmed that men's passwords are stronger than women's passwords [67].

2.4 Password Generation Mechanisms & Implementations

There are several mechanisms that researchers have followed to generate the passwords to increase the strength and memorability. One of the mechanism is the use of mnemonics to generate the password and Wijesekara et al [56] have used this concept and presented a mechanism to generate the password that increased the strength and memorability. They suggested to select the fully random password first and then generate a text that can be used as a mnemonic to the password. To improve the better recalling that text phrase will be based on the user's background information. According to the [1], the research team has implemented a password generator for their research that evaluates the strength and memorability. For the generating password, they also have used the mnemonic concept and the system constructs the mnemonics from given passwords by using a small word list. The research team has applied for wordlist and character positions with all possible combinations to create the meaningful mnemonic and, for that, they have used the simple grammar and vocabulary. As seen in Figure 2.3, the assigned password is "jpwjaop" and assigned mnemonic for it is "Jill's pet wolf just ate our pizzas". Furthermore, by default, it opens the paint program and the web browser with the result of generated mnemonic and user needs to draw a visual graphic that can be used as a hint for the mnemonic in order to improve the better recalling as seen in Figure 2.4.



Please create a new account.

Your assigned password is: **jpwjaop**

Your assigned mnemonic is: **Jill's pet wolf just ate our pizzas.**

Username: demo

Password:

Figure 2.3: *Password generator*

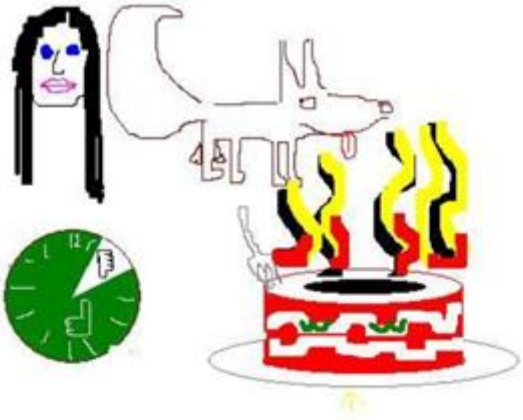
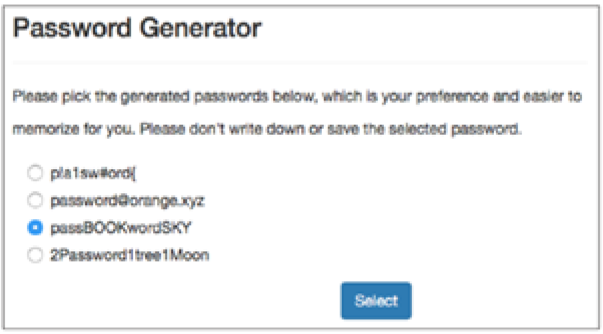


Figure 2.4: *Visual Image for generated password*

Lyanstani et al. [61] also have proposed a password generating mechanism with an implementation that based on the mangling rules. Mangling rule transforms a given text into another based on a rule. From their system, they have followed 4 rules to transform the password and enable the user to select the more memorable password. The system is developed as a web system by using JavaScript and HTML. Initially, the user needs to select a prime password from a large dictionary. That password is the input for the mangling rule. They have used following mangling rules to transform the prime password;

- Insertion of random 4 characters or symbols or digits at random positions
- Generate the password as email address form by adding “@” with 3 random characters and end with “.”.
- Given password is divided into two parts at a random hyphenation point. Then a dictionary word is appended in uppercase at the hyphenation point as well as another dictionary word in uppercase is appended at the end of the password.
- Generate the password which is structured as baking recipes.

As seen in Figure 2.5 and Figure 2.6, it displays the generated passwords based on the above mangling rules for the prime password of “password”.

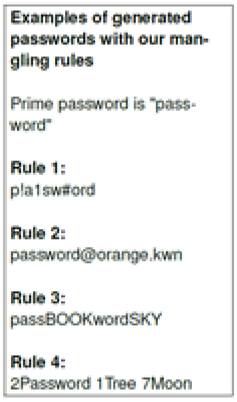


Password Generator

Please pick the generated passwords below, which is your preference and easier to memorize for you. Please don't write down or save the selected password.

○ p!a1sw#ord{
○ password@orange.xyz
● passBOOKwordSKY
○ 2Password1tree1Moon

Figure 2.5: *Password generator*



Examples of generated passwords with our mangling rules

Prime password is "password"

Rule 1:
p!a1sw#ord

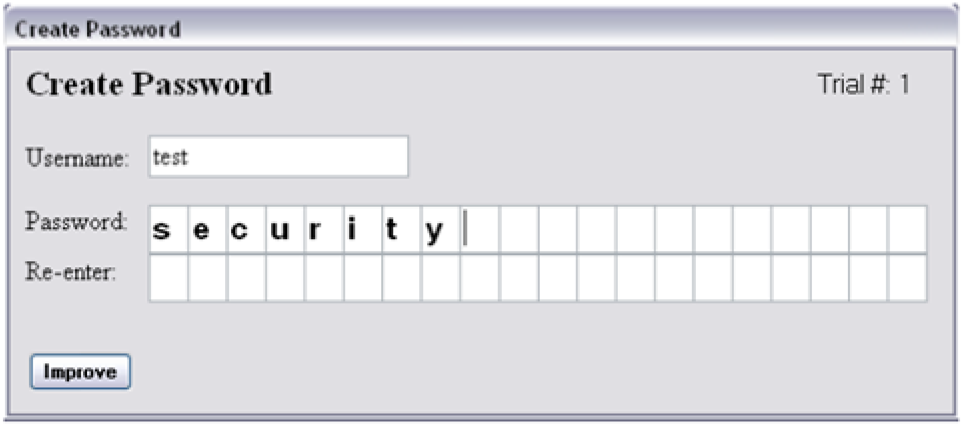
Rule 2:
password@orange.kwn

Rule 3:
passBOOKwordSKY

Rule 4:
2Password 1Tree 7Moon

Figure 2.6: *Examples of generated passwords with mangling rule*

Forget et al. [72] have conducted a research to evaluate the security and memorability of generating the password by applying the randomly selected characters in random places in a given password. They named this password generating mechanism as "Persuasive Text Passwords (PTP)". Therefore, the input is the user given password and its output is improved persuasive text password. Also, user has chance to shuffle the output password to generate another combination in order to have memorable password. As seen in Figure 2.7 describes user given the password before apply the persuasive improvement and Figure 2.8 shows the output password with the persuasive improvement.



Create Password

Create Password

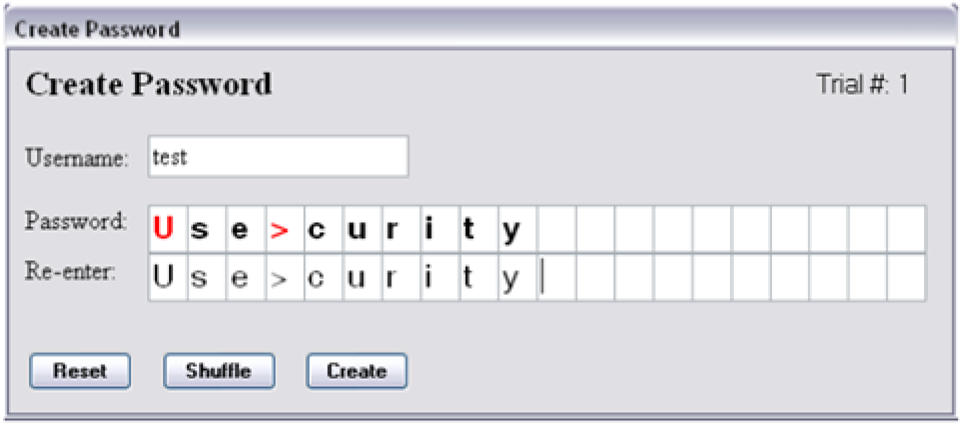
Trial #: 1

Username: test

Password: security

Re-enter:

Figure 2.7: *User given password before apply the persuasive improvement*



Create Password

Trial #: 1

Username: test

Password: U s e > c u r i t y

Re-enter: U s e > c u r i t y

__Figure 2.8:__ Output password with the persuasive improvement

2.5 Data Breaches & Financial Implications

Whether it be a single individual or a large multinational organization a data breach would likely result in some serious repercussions if or when data is leaked and falls into the wrong hands. A report for the year 2017 published by IBM Security and Ponemon Institute [73] sampling 419 companies in 13 countries report that the average total cost of a data breach to be 3.62 million dollars. In calculating the cost this report takes into account the cost of churned customers as a result of the breach, cost of a number of records stolen, the time taken to identify and contain the breach, detection and escalation of the data breach incident and post data breach cost such as costs to notify the victims.

Losing the goodwill of customers can have serious consequences. The IBM report shows that losing just less than 1% of a company's customer base had an average total cost $2.6 million and if the churn rate is greater than 4% the average total cost may exceed $5.1 million. Industries such as Finance (churn rate= 5.7%) Health Care (churn rate= 5.5%) and Services Sector (churn rate=5.2%) face the greatest impact resulting in higher churn rates, adding to which in the United States the highest price for losing a customer was as high as $4.13 million.

The average total cost of a breach and loss of records have a significant positive correlation where the cost ranges from $1.9 million for less than 10000 stolen records to around $6.3 million for 50000 or more compromised records. Furthermore, the cost associated with detection and escalation range from $0.43 million to $1.46 million and post-breach response costs range from $0.44 million to $1.56 million.

The IBM report categorizes 3 root causes for data breaches, namely malicious or criminal attack, system glitch and human error. Out of the 3 root causes malicious and criminal attackers cause 47% of data breach incidents and also the most expensive of the 3 to deal with.

When attacks are conducted with malicious or criminal intent the most favored method is to exploit vulnerabilities in password authentication. In a report titled “2017 Data Breach Investigations Report” published by Verizon [73] it states that 62% of confirmed data breaches featured hacking of which 81% of the hacking related breaches were executed leveraging weak, default or stolen passwords usually obtained through some form of social engineering. This report goes on to point out that no system is 100% secure however organizations not putting into place basic security measures such as measures to improve password security can be quite costly. Given below are some details regarding the financial repercussions of some recent data breaches.

The major Yahoo data breach that resulted in the leak of information related to 3 billion user accounts resulted in a major blow on the sale price of the company. Yahoo which was to be acquired by Verizon for $4.8 billion was later revalued to a sale price of $4.48 billion, which was a price reduction of $350 million, a direct result of the huge data breach resulting in a huge loss for the company shareholders [75].

In 2014 Sony Pictures computer network was hacked and taken over by attackers who proceeded to steal information such as social security numbers of around 47000 employees and films from the network. The attack resulted in a drop in share price of 10% and ended costing Sony Pictures $35 million, as a result, to repair and compensate for damages [76].

In October of 2015, a UK broadband company named Talk Talk was attacked by a group of hackers resulting in the loss of close to 157000 customers data. This resulted in Talk Talk having to pay two fines of £400000 and £100000. In the aftermath of the data breach, it was estimated that a total of 101000 customers left the organization, the share price of the company dropped by 7% and the total estimated cost of the breach was estimated to be around £60 million [15].

Although it must be noted that these breaches were not solely the result of weak passwords, given the statistics obtained through studies such as the report by Verizon it is quite likely that poor passwords would have likely aided the attackers to become successful in their endeavors.

Chapter 03 – Design

Following Figure 3.1 represents the graphical representation of the top-level research design process.

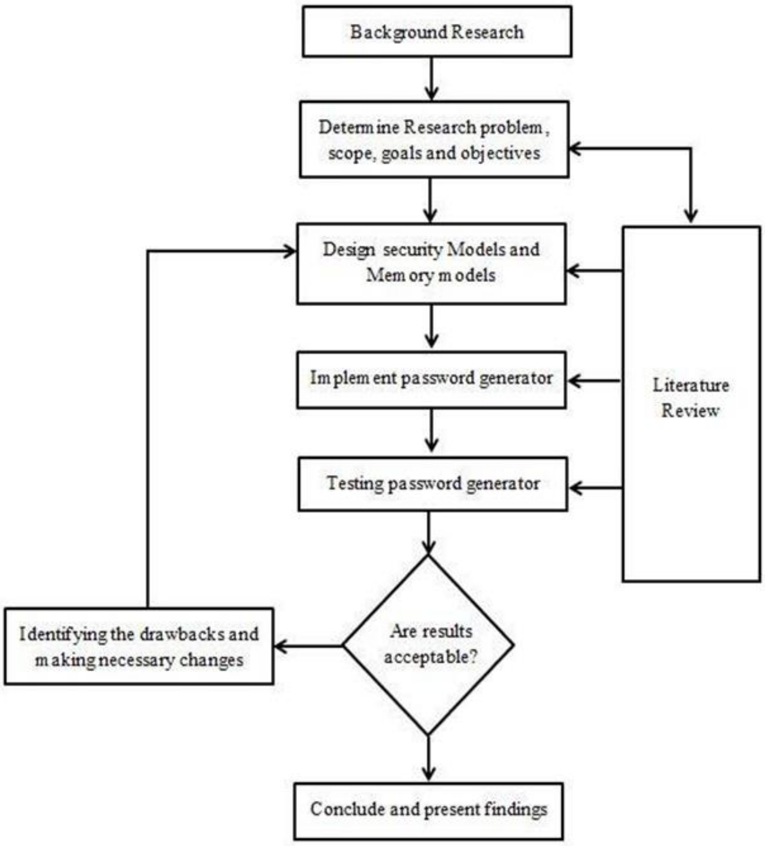

Background Research
Determine Research problem, scope, goals and objectives
Design security Models and Memory models
Implement password generator
Testing password generator
Literature Review
Are results acceptable?
Identifying the drawbacks and making necessary changes
Conclude and present findings

Figure 3.1: *Abstract view of the research design*

The research will be continued in iterations and enhancements will be done subsequently analyzing the results and findings that were gathered in the previous iterations combined with new literature reviews and findings to produce a complete package of the best feasible password generating system consisting of the password strength checker and a rehearsal module at the end of the final iteration.

Background Research: As the initial step of our research we conducted a preliminary study of the background in the field of information security in order to understand the current state of related areas, nature of work carried out by previous research and other related studies, with the aim of obtaining a better understanding of unclear areas and formulating a suitable research question.

Determine Research Problem, Scope, Goal and Objectives: Once a preliminary understanding of the research area was obtained through the background research, we were able to formulate a proper research problem and subproblems (which we hope to address through our research). We were able to determine the scope and limitations clearly stating what the research hopes cover and what areas it will not address and the primary research goal and objectives ***which will be accomplished in order*** to achieve the research goal. This was conducted in parallel with the next phase which is "Literature Review" and our research goals and objectives were altered and fine-tuned ***as required***.

Literature Review: A more thorough literature review was conducted to obtain a deeper understanding of the current situation and the studies in the field. Our efforts in this phase are focused on comprehensively learning and determining the need for authentication and how it's done, vulnerabilities associated with text-based password authentication and the work carried out on strengthening text-based password authentication, the psychology in text remembering and recalling, factors that cause a user to forget passwords and the human's behavior upon password selection, studying the significant traits and behavior of crackers and ultimately finding the gaps and loopholes in current authentication systems that crackers manipulate to cause data breaches. Upon completion of the literature review phase, we have made suitable adjustments to our research problems, scope, goals and objective to be more meaningful and relevant. Furthermore, we used this review to identify possible secondary data sources and the knowledge gathered from this section was used in creating our initial security and memory models for "Iteration 01".This phase was carried out in parallel with the other phases of our research design and with new findings and knowledge that we have gathered in this phase, required changes were made to the security models and memory models in each Iteration with the intention of achieving the objectives and consequently the main goal of our research.

Design Security and Memory Models: For the purpose of this research, we developed and have combined both security models and memory models to be used as design models to develop the password generator. A security model is developed based on accepted password security requirements and best practices in order to identify the strength of the generated password from the different password generation mechanism. Similarly, a memory model is created by referring concepts in psychology related to human memory that can be applied to generate memorable passwords and as well as to train users to retain and recall the passwords in the long term. Based on our understanding and knowledge from the literature review, we designed and evaluated multiple security and memory models and a more detailed understanding and explanation on the implementation of these models has been presented in Chapter 4.

Implementation of password generator: Based on the security and memory model, various password generators have been designed and implemented. Each implementation changes made to the password generator in terms of security and memory aspects were carried out in iterations which were based on new findings and learning discovered in the "Literature Review" phase. Three such iterations were carried out in our research and a technique with the best solution for the password generation was achieved in "Iteration 03". More details on the implementation of the password have been presented in chapter 4.

Testing the password generating System: Since our goal is not to generalize any findings to the public and considering the time limitations for the research, our tests have so far been done on a limited number of small user groups having samples chosen at random from fourth-year undergraduates from University of Colombo School of Computing. For the time being, we have used the verbal feedback from the user tests and our own observations along with further literature findings to make necessary changes to improve the password generators. In addition to these tests, in order to check the sensibility/appropriateness of the memory model adopted, an expert validation was taken and additionally, a set of rehearsal activities were done to improve the recall ability of the passwords generated. Finally, a feedback form (Appendix A) was generated using google forms and was given to the participants of iterations 02 and 03 in order to obtain an overview on the usability aspects of the entire process of password generation used in the two iterations. More details on the evaluation process of each implementation in each iteration will be discussed in detail in chapter 4

3.1 Research Methods

During the course of our research work, we have used both qualitative and quantitative methods in order to gather and analyze data.

Qualitative data gathering and analysis

Qualitative data were collected by reviewing existing literature and studies. Through analysis of this data, the following facts were extracted for the commencement of the study,

- Various security models defined and security considerations studied by researchers which play a crucial role in formulating an enhanced security and psychological model in order to develop a password generator.

- Multiple avenues and design approach available which could be adopted in finding an optimal solution for the problem that is addressed by the research.

In addition to analysis of existing literature, another qualitative data which will be dealt with throughout the research is the feedback taken from the users and observations and problems encountered during the rehearsal testing.

- At the end of each user test, direct user feedback was collected in order to obtain a general idea on the usability of the system. Based on this user feedback the implemented system and the overall process was enhanced.

- Finally, a feedback form was given to all the participants of iteration 02 and 03 to compare and contrast the usability of the processes adopted to generate passwords in these iterations.

Furthermore, we obtained a validation from an external expert on the overall approach to address the psychological aspects related to human memory in our implementation.

Quantitative data gathering and analysis

The strength of the passwords which were generated by the password generator in each iteration will be evaluated using an excepted password strength checker. These password evaluation results will be used to derive an overall performance measure for the password generator and modifications are carried to enhance the password generator and to overcome the existing shortcomings.

Chapter 04 – Implementation, Results & Findings

4.1 High-Level Implementation Design of the System

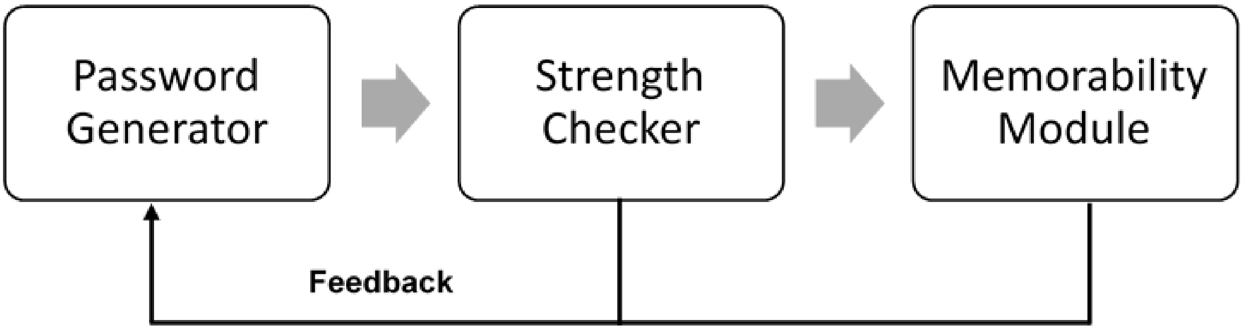


Figure 4.1: *High level implementation design of the system*

The proposed system included 3 major components which were integrated as in Figure 4.1. The generated password was directed into the strength checker and it evaluated the strength of the given password. Then the memorability module was used to rehearse the password and to evaluate the ability to recall a password. After considering both results and feedback from the password strength checker and memorability module, the password generator was evaluated and modified iteration wise.

4.2 Iteration 01

4.2.1 Password Generator – (IT1-PG)

The password generator in our first iteration named IT1-PG was designed and developed with the intention of obtaining a preliminary understanding of implementing a system to address the problem of balancing the password strength and memorability. IT1-PG generated “Singlish” phrases which used both user inputs and a list of predefined words for phrase generation. IT1-PG was developed using Python 3.6 with our understanding of some fundamental requirements for making passwords both strong and memorable. The IT1-PG generates a password in the following format:

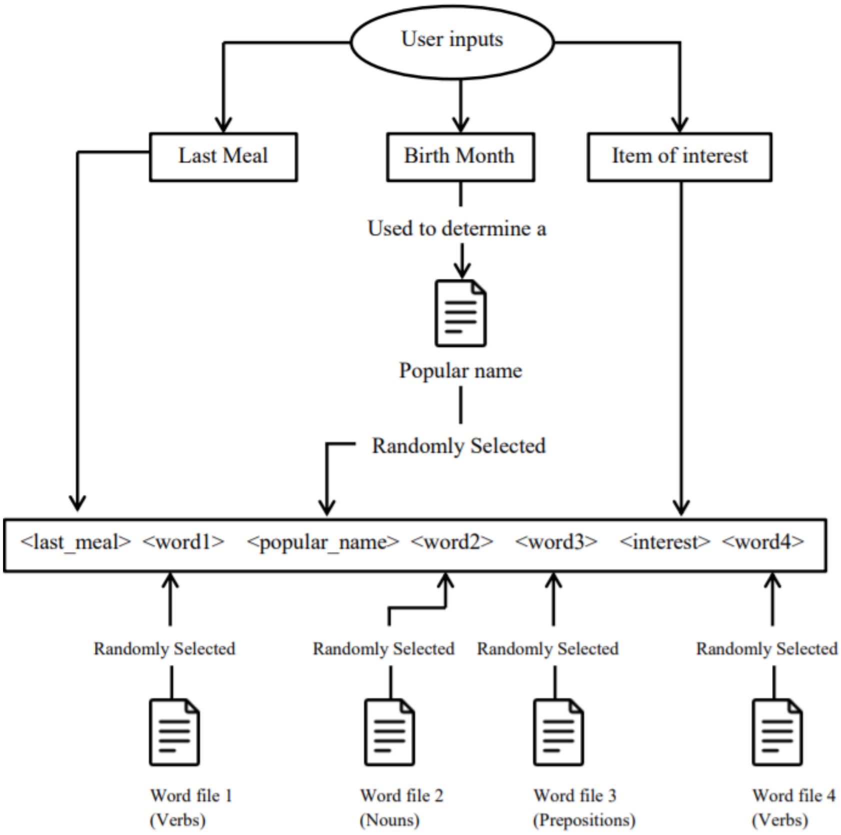


***Figure 4.2**: IT1-PG abstract password generation process*

The generator obtains 3 inputs from the user, which are as follows:

- Last meal the user had
- Users birth month
- An item of interest

The last meal a user had is a piece of personal information that user can remember and will vary based on the time and date the password was generated as well as which item of consumed food the user wishes to take into consideration for the purpose of generating the password, making it difficult for an attacker to guess unless they are very closely acquainted with the user.

Once the user enters the birth month, the generator will select a random name based on the entered value from a text file which contains names of popular personalities born on the same month as the user to be incorporated to the phrase. The user is given an explanation on how the name in the phrase was selected, when the password is generated. one such example is given below:

For the password: bath ussapu John ira pennala aba yaaluwo gaththa

The explanation displayed: John Kotelawala was born on the same month as you
that’s how we got John

The user will finally be prompted to enter an item of interest this can be anything such as a song, drama, movie, book, play, sport, etc. This adds a personal interest of the user to the phrase making it easier for the user to retain.

Once the user’s inputs are taken in above order, the generator randomly selects 4 words from the 4 text files in order to generate the phrase with respect to the format in Figure 4.2. The details related to the contents of these word files are given below.

File name	Word classes used	Total number of words in file	Examples
<word1>	Verbs	15	dekapu, kaapu, deepu, gaththu
<word2>	Nouns	10	Kanda, gedara, midula, gaga, pokuna
<word3>	Prepositions	13	Udin, yatin, dige, lagin
<word4>	Verbs	8	Beluwa, kiyewwa, liwwa, gaththa

Table 4.1: *Word files content summary*

By taking random inputs from the above files and combining them with the information from the user inputs, IT1-PG generates 5 phrases. The generated phrases are not always meaningful phrases. However, they had sufficient syntactical integrity for a user to make some sense. The user will select the phrase that they are most comfortable with as their password. Examples of some IT1-PG generated phrases are given below:

Input			Output Phrases
Last Meal	Birth Month	Item of Interest	
paan	4	aba yaaluwo	Paan wisikarapu Banda muhuda udin aba yaaluwo gilla
			Paan ussapu Lester pokuna penala aba yaaluwo kiyewwa
			Paan wisikarapu Lester ira dige aba yaaluwo liwwa
			Paan hedapu Lasantha pokuna behela aba yaaluwo gilla
			Paan kaapu John ira udin aba yaaluwo kewa

Table 4.2*: Sample output of IT1-PG generated passwords*

4.2.2 Strength Checker – (IT1-SC)

For the purpose of this iteration, password strength was evaluated using 4 online strength checkers. The sites used along with accompanying features of each strength checker are as follows:

Strength Checker	**Creator**	**URL**	**Features**
How Secure Is My Password	Dashlane Password Manager	https://howsecureismypassword.net/	a) Display password strength based on estimated years to crack b) Provides feedback on strong points of the entered password c) Provides feedback on weaknesses of the entered password
Kaspersky Lab Secure password check	Kaspersky Lab	https://password.kaspersky.com/	a) Display password strength based on estimated years to crack using a variety of platforms for estimation. (Example: Mac Book Pro (2012), Conficker botnet, Tianhe-2 Supercomputer) b) Provides feedback on weaknesses of the entered password
LastPass How Secure is Your Password	LastPass	https://lastpass.com/howsecure.php	a) Display password strength as a rating ranging from weak - very strong b) Provides feedback on weaknesses of the entered password
The Password Meter	Jeff Todnem	http://www.passwordmeter.com/	a) Display password strength as a rating ranging from Very weak - very strong and a score ranging from 3% - 100%

			b) Provides a rating based feedback on strong points of the entered password c) Provides rating based feedback on weaknesses of the entered password

Table 4.3: *Password strength checker site details and features*

4.2.3 Memory Module – (IT1-MM)

Once the users had selected a password they were comfortable with, they were asked to memorize the phrase until they felt that they were confident enough to retain the password.

The participants were instructed not to write down the generated password. After 3 days, participants were requested to recall and write down the phrase that they had memorized.

4.2.4 Results

Results from the IT1-PG

Below table shows the phrases generated for each participant from the password generator. Detailed output created from the system for each participant is shown in Appendix B.

Participant 01	Participant 02	Participant 03
paan wisikarapu lester kanda udin aba yaluwo kewa	bath rasawetuna nanada kale hangala sarigama wikka	kadala gaththy Asnaka gama harala saara bumi gilla
paan john midula balala aba yaluwo liwwa	bath allapu athula gaga behela sarigama baluwa	kadala wage Asanka midula penala saara bumi wikka
paan wage malini muhuda eliyen aba yaluwo baluwa	bath beepu henry kale lagin sarigama wenasuwa	kadala hedapu Asanka midula hangala saara bumi liwwa
paan hadapu lester geadara lagin aba yaluwo gaththa	bath kapapu harry pokuna lagin sarigama beluwa	kadala wage Asanka muhuda dige saara bumi wikka
paan wage john kanda behela aba yaluwo kiyewwa	bath kaapu harry muhuda eliyen sarigama kiyewwa	kadala wisikarapu Asanka pokuna langin madolduva liwwa

Table 4.4: *Results from the password generator for iteration 01*

Results from the IT1-SC

IT1-PG generated phrases with an average character length of 30+ making the password generated by IT1-PG quite resilient to brute-force attacks. Furthermore, the use of "Singlish" phrases also made it quite resilient to dictionary attacks. The table below illustrates the strength score generated from each site for password selected by users in the user study.

Phrase	Password	Scores			
		How Secure Is My Password	**Kaspersky Lab Secure password check**	**LastPass How Secure is Your Password**	**The Password Meter**
paan wage Malini muhuda eliyen aba yaluwo beluwa	paanwageMalinimuhudaeliyenabayaluwobeluwa	18 sexdecillion years to crack	10000+ centuries on Tianhe-2 Supercomputer	Very Strong	100% ; Very Strong
bath kaapu Harry muhuda eliyen	bathkaapuHarrymuhudaeliyensarigamawenasuwa	935 sexdecillion years to crack	10000+ centuries on Tianhe-2 Supercomputer	Very Strong	100% ; Very Strong
kadala wisikarapu Asanka pokuna langin madolduva liwwa	kadalawisikarapuAsankapokunalanginmadolduvaliwwa	18 vigintillion years to crack	10000+ centuries on Tianhe-2 Supercomputer	Very Strong	100% ; Very Strong

Table 4.5: *Password strength scores from online strength checkers*

As shown, each site rated the passwords to be of very high strength primarily due to the long length of each password. However, the feedback from these sites highlighted that despite the length, the passwords lacked complexity as a result of only using alphabetic characters. A summary of identified strengths and deficiencies of tested passwords are given below.

Strength Checker	Strengths	Deficiencies
How Secure Is My Password	a) Password contains a large number of characters	a) The password contains only letters, recommended that numbers and symbols be added to increase complexity
Kaspersky Lab Secure password check	Site does not offer this feature	Did not highlight any deficiencies
LastPass How Secure is Your Password	Site does not offer this feature	a) The password contains only letters, recommended that numbers and symbols be added to increase complexity
The Password Meter	a) Contains a large number of characters	a) Password contains only letters and password does not contain numbers, symbols b) Password contains repeated characters and consecutive lower-case letters

Table 4.6: *Highlighted strengths and weaknesses of passwords from online strength checkers*

Results from the IT1-MM

Of the 3 participants, none were able to correctly recall the password. However, they could recall it partially. The following table shows the original phrase that participants chose along with the recalled phrase after 3 days.

Participant	Original Phrase	Phrase Remembered
Participant 01	paan wage Malini muhuda eliyen aba yaluwo beluwa	paan wage ___ muhudu ___ aba yaaluwo beluwa
Participant 02	bath kaapu Harry muhuda eliyen sarigama wenasuwa	bath kaapu Harry ___ ___ sarigama ___
Participant 03	kadala wisikarapu Asanka pokuna langin madol duva liwwa	kadala ___ ___ pokuna lagin madol duva liuwa

Table 4.7: *Results from the memorability module for Iteration 01*

4.2.5 Findings & Observations

Different users followed different spellings when writing “Singlish” phrases which could contradict with system generated phrases. For an example, participant 03 spelled the system generated word “liwwa” as “liuwa”. Therefore, use of “Singlish” phrases have made the participants to employ more effort and concentration towards memorizing the spellings of the words that are used in the phrase. It was also observed that users struggled to memorize and recall the phrases since they were long and lacked meaning. However, the results showed that users were able to successfully recall the words input by them into the system.

Results from the memorability modules showed participants were able to partially recall the password and failed to recall the entire password correctly and most of these forgotten words are the words that were given by the system.

Passwords generated by the system had issues related to password complexity which lacked meaning and the use of the Singlish scheme. These indicate the need for a more robust approach for generating a memorable and secure password.

Furthermore, due to the limited feedback and the lack of control over the online strength checkers, well-established methods are required to evaluate the password strength which were used in prior research.

4.3 Iteration 02

Considering findings from Iteration 01 and research objectives, a system comprising of a password generator, strength checker and rehearsal module was developed for Iteration 02. Furthermore, a simple login website was developed in order to aid evaluation of the memorability of the password.

4.3.1 Password Generator – (IT2-PG)

The prior research [56], [1] have stated that generating a mnemonic based password with user's background information will trigger a better memory and user's publicly available data can be used to achieve the above consideration. Therefore, a system is developed called IT2-PG which uses publicly available data from Facebook to generate a first letter mnemonic password. Since first letter mnemonic password is composed of the first letter of each word in the phrase, it makes the password resistant to dictionary attacks [15]. Major drawbacks that were identified in Iteration 01 were the use of different spellings when recalling the Singlish phrases and the lack of meaning in the Singlish phrases which reduced the recall ability of the password created. Therefore, in order to address the above problems, first letter mnemonic password was created using English templates and extracted data.

Figure 4.3 shows the process of generating a first letter mnemonic password in IT2-PG.

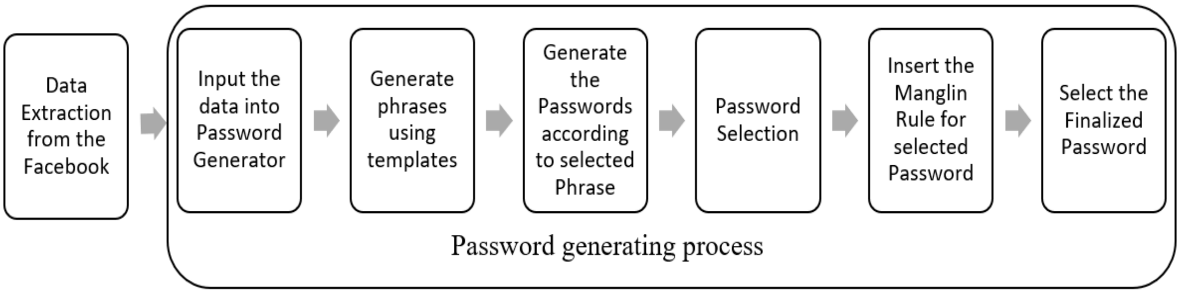

Data Extraction from the Facebook
Input the data into Password Generator
Generate phrases using templates
Generate the Passwords according to selected Phrase
Password Selection
Insert the Manglin Rule for selected Password
Select the Finalized Password
Password generating process

Figure 4.3: *First Letter Mnemonic Password Generating process*

Data Extraction Process of Publicly Available Data

As “Facebook” is one of the most popular social media services it was chosen as the source for user public data extraction [56]. Facebook offers information of users’ such as profile details, employment history, locations visited, user interests, status, their feelings as public data. Facebook public data can be queried simply by obtaining an access token along with the ID of a user who has logged in, using the Facebook Graph API. The access token represents the permissions for which data can be accessed using the API.

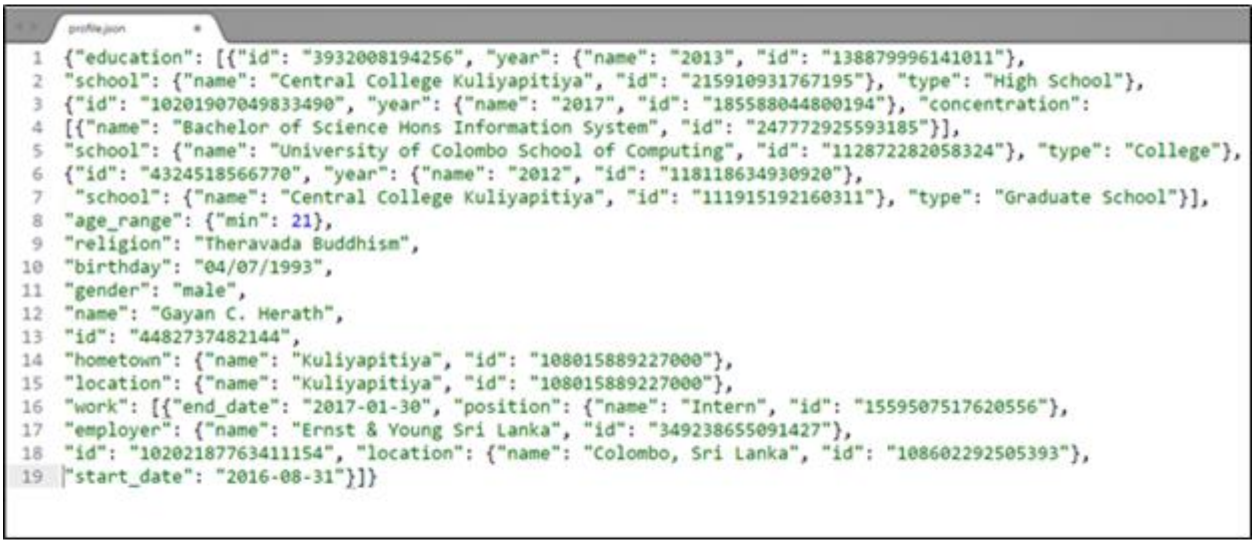
A Python 3.6 based script is used to extract the user’s profile details, friends’ names, posted locations, feeds and ratings for locations into five JSON files. The script uses the user’s access token and the user ID to extract above data. Appendix C represents the permissions which are used to extract the data from participants’ Facebook profile. Also, Appendix D represents the generated token, Facebook username and its ID according to above permissions. To address the ethical considerations, a consent form (Appendix E) was given to all the participants before the data extraction process.

Following table shows the libraries which used for the script and the purpose of it.

Library	**Purpose**
facebook	Support to Facebook Graph API and implement Facebook authentication
requests	Allows to send the HTTP requests
simpljson	Support to encode and decode the JSONs

Table 4.8: *Libraries which used for the Facebook data extraction script*

Figure 4.4 represents the sample JSON file which includes the profile information of a user.



```
{"education": [{"id": "3932008194256", "year": {"name": "2013", "id": "138879996141011"},
"school": {"name": "Central College Kuliyapitiya", "id": "215910931767195"}, "type": "High School"},
{"id": "10201907049833490", "year": {"name": "2017", "id": "185588044800194"}, "concentration":
[{"name": "Bachelor of Science Hons Information System", "id": "247772925593185"}],
"school": {"name": "University of Colombo School of Computing", "id": "112872282058324"}, "type": "College"},
{"id": "4324518566770", "year": {"name": "2012", "id": "118118634930920"},
 "school": {"name": "Central College Kuliyapitiya", "id": "111915192160311"}, "type": "Graduate School"}],
"age_range": {"min": 21},
"religion": "Theravada Buddhism",
"birthday": "04/07/1993",
"gender": "male",
"name": "Gayan C. Herath",
"id": "4482737482144",
"hometown": {"name": "Kuliyapitiya", "id": "108015889227000"},
"location": {"name": "Kuliyapitiya", "id": "108015889227000"},
"work": [{"end_date": "2017-01-30", "position": {"name": "Intern", "id": "1559507517620556"},
"employer": {"name": "Ernst & Young Sri Lanka", "id": "349238655091427"},
"id": "10202187763411154", "location": {"name": "Colombo, Sri Lanka", "id": "108602292505393"},
"start_date": "2016-08-31"}]}
```

__Figure 4.4:__ Sample JSON file which includes the profile information a user

This data extraction process is independent of the rest of system. JSON files are the input for IT2-PG.

Password generating process

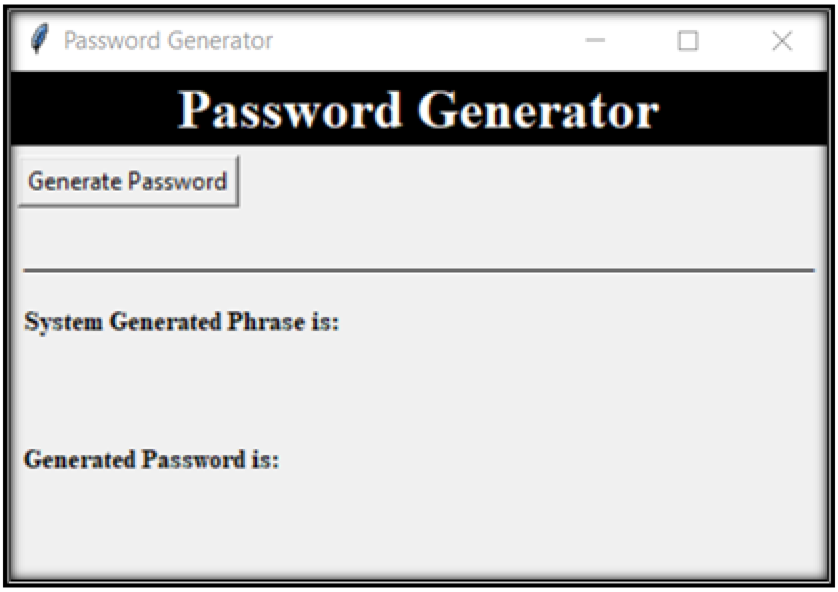
The IT2-PG was developed using the python 3.6. Following Table 4.9 shows the libraries used in the implementation and their purpose.

Library	**Purpose**
json	Supports to encode and decode the JSON
tkinter	To implement the Graphical User Interface
subprocess	To initiates a new process
random	Provide the random phraseas output
datetime	To get assist of dates and time for templates
os	To support for command line execution

__Table 4.9:__ Libraries which used for the Password Generator

Implementation has a graphical user interface in order to improve the usability of the password generator. It reads the extracted data from the five JSON files. Using this data, it generates multiple phrases according to a set of predefined templates and those generated phrases are presented to the user one by one. The number of templates generated depends on the amount of public data extracted from Facebook in the data extraction process. Since users have multiple phrases, they have the freedom to select the most comfortable phrase which can be used to generate the password using first letter mnemonic strategy.

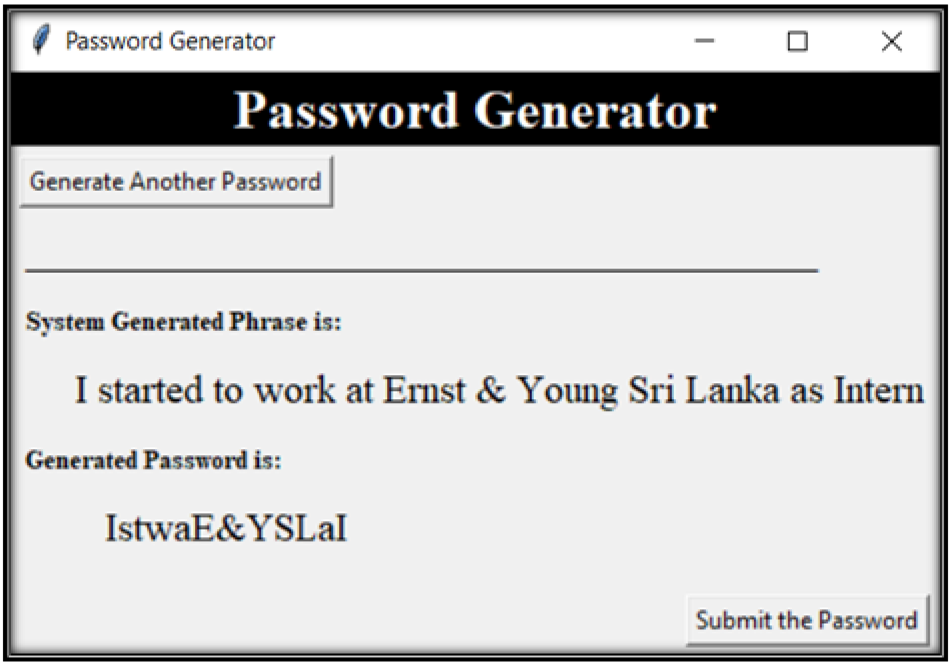
Figure 4.5 represents the initial graphical user interface of IT2-PG and the user can generate the phrase and its password based on his/her data by clicking the “Generate Password”. This phrase is picked by the IT2-PG randomly. Figure 4.6 represents a generated phrase and its password based on one of the user’s employee history data. In this case key variables that were taken from JSON files are “Ernst & Young Sri Lanka” and “Intern” and rest of the words come from the default template. Also, it shows that user has the ability to generate another password or submit it. Figure 4.7 represents the submitted password.



System Generated Phrase is:

Generated Password is:

Figure 4.5: *Initial Graphical User Interface of IT2-PG*


Password Generator

Password Generator

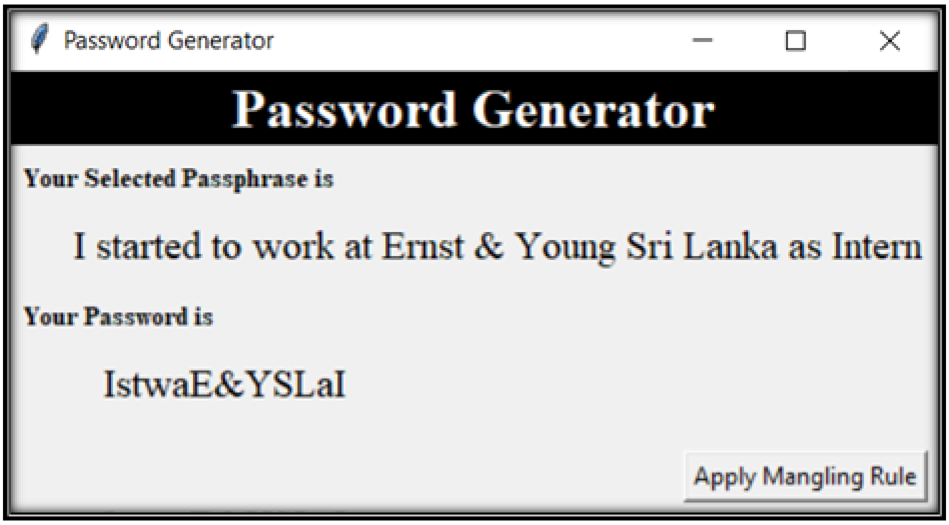
System Generated Phrase is:

I started to work at Ernst & Young Sri Lanka as Intern

Generated Password is:

IstwaE&YSLaI

Figure 4.6: *One of generated password and its mnemonic based on employee history data*


Password Generator

Password Generator

Your Selected Passphrase is

I started to work at Ernst & Young Sri Lanka as Intern

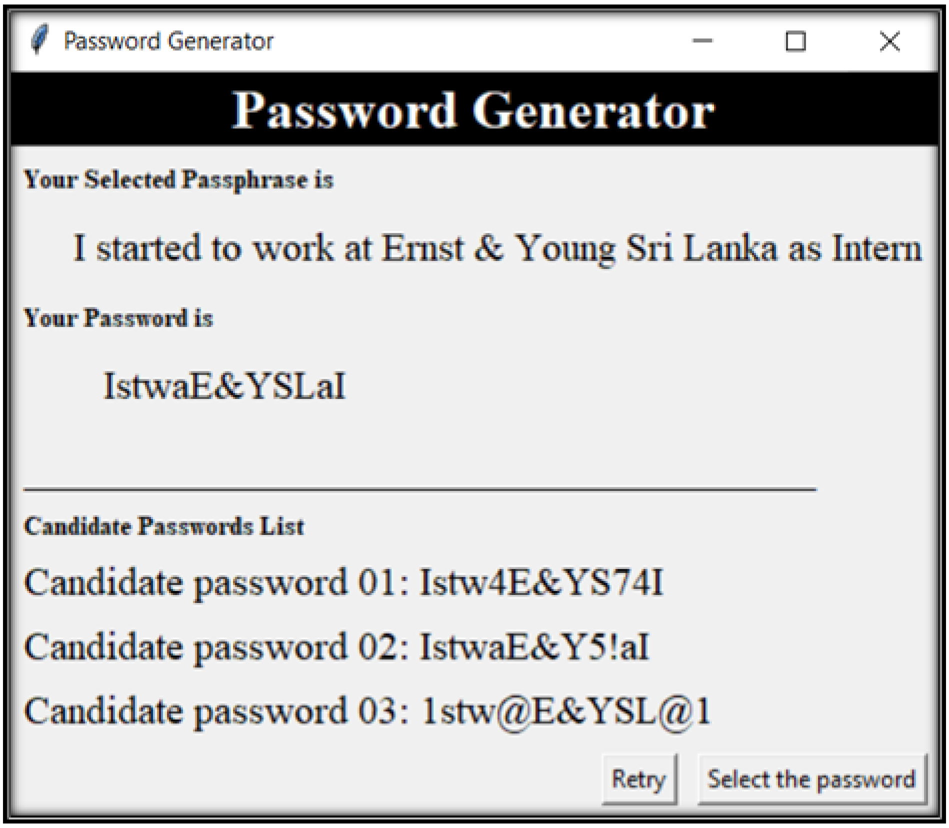
Your Password is

IstwaE&YSLaI

Figure 4.7: *Graphical User Interface of submitted password*

This generated password is not the finalized password. Password’s some characters are substituted with a similar character such @ for a, ! for l, 3 for E using the default mangling rule set which is packaged with the John the Ripper password cracker. By applying these mangling rules, it increases the randomness of the generated password and it transforms the password to have different character types of digits, uppercases, lowercase and symbols.

As seen in Figure 4.7 user can apply the mangling rule by clicking the button “Apply Mangling Rule”. Figure 4.8 represents the output results after applying the mangling rule and only 3 candidate passwords are showed to the user. The user has the freedom to pick a comfortable password from this set of candidate passwords or he/she can generate another 3 candidate passwords if he/she is not comfortable with them. In some cases, IT2-PG does not generate a set of candidate passwords which means passwords generated from the first letter mnemonic cannot be transformed to have all the different character types as described above. Then user needs to retry with another phrase and its password. After user has submitted the most comfortable password, IT2-PG provides the phrase, its password and selected password from the candidate password list. Figure 4.10 represents the summary window for a selected password.



Password Generator

Your Selected Passphrase is

I started to work at Ernst & Young Sri Lanka as Intern

Your Password is

IstwaE&YSLaI

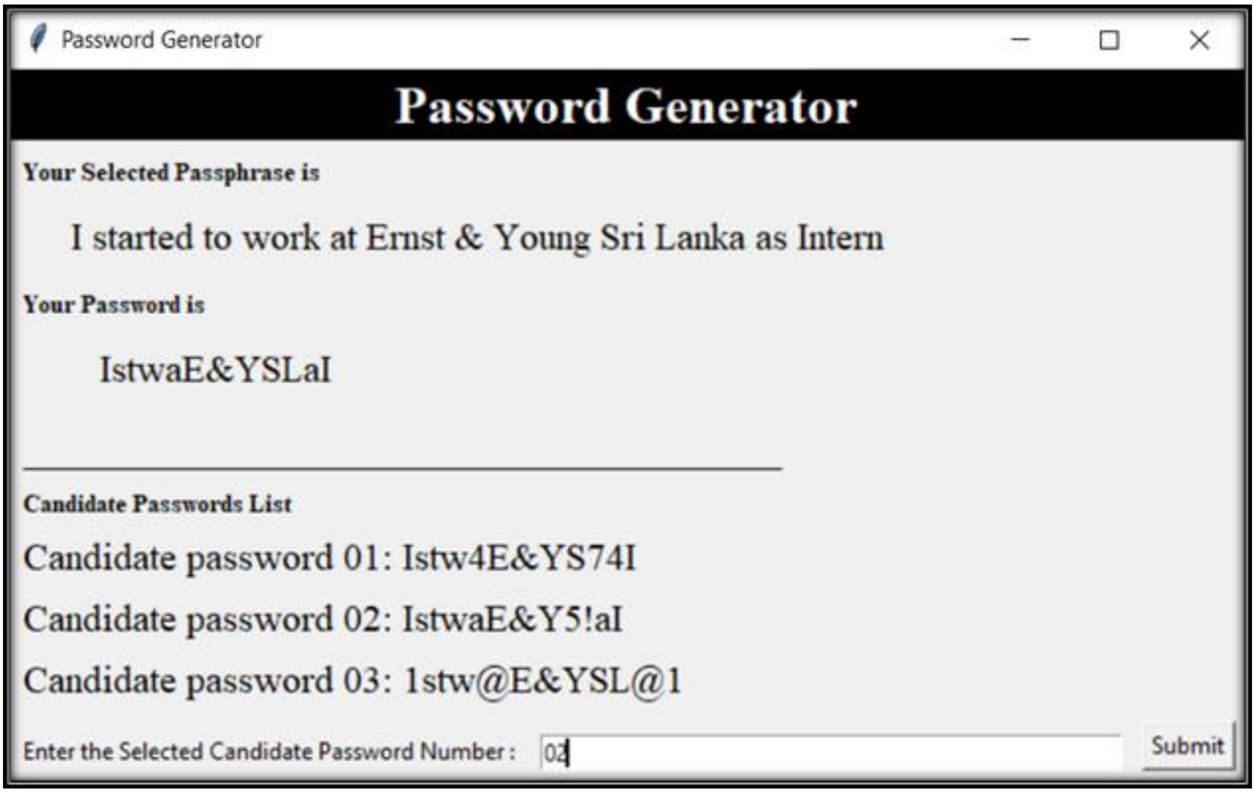
Candidate Passwords List

Candidate password 01: Istw4E&YS74I

Candidate password 02: IstwaE&Y5!aI

Candidate password 03: 1stw@E&YSL@1

Figure 4.8: *Three candidate passwords from mangling rule applied passwords*



Password Generator

Your Selected Passphrase is

I started to work at Ernst & Young Sri Lanka as Intern

Your Password is

IstwaE&YSLaI

Candidate Passwords List

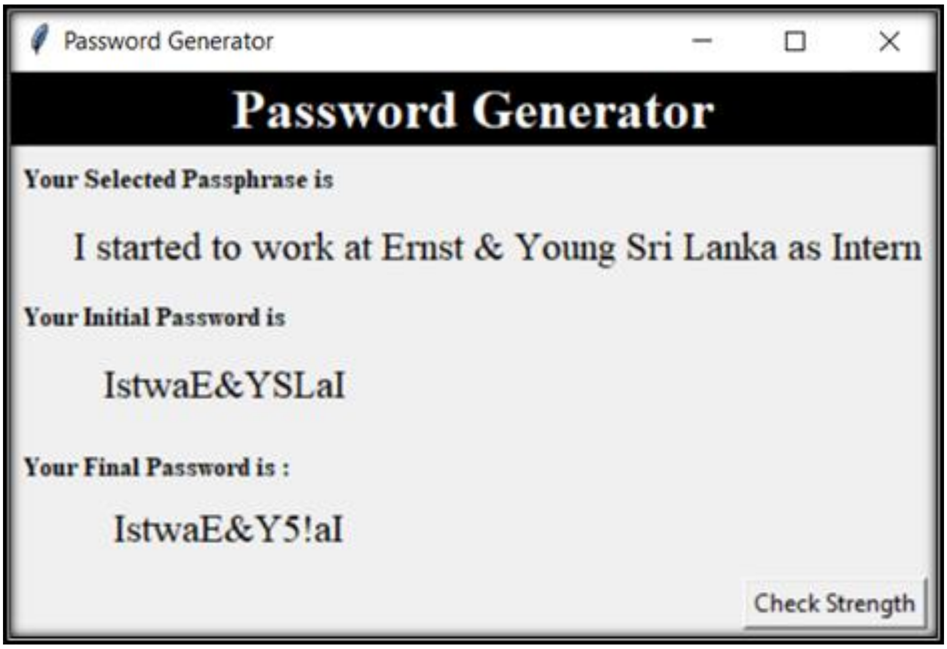
Candidate password 01: Istw4E&YS74I

Candidate password 02: IstwaE&Y5!aI

Candidate password 03: 1stw@E&YSL@1

Enter the Selected Candidate Password Number : 02

Figure 4.9: *Select the 2nd Candidate password as comfortable password*



Password Generator

Your Selected Passphrase is

I started to work at Ernst & Young Sri Lanka as Intern

Your Initial Password is

IstwaE&YSLaI

Your Final Password is :

IstwaE&Y5!aI

Figure 4.10: *Summary window selected password*

In this phase, we advised user not to give any hard effort to remember it since memory module helps user to rehearsal the generated password.

4.3.2 Strength Checker – (IT2-SC)

Strength checker is the component which measures the strength of a given password and to provide feedback on the password strength. In implementation 2, multiple candidate solutions were used to measure the strength of the passwords. They were Hashcat, entropy calculation and improved version of "zxcvbn" password estimation with LUDS estimation. Among them, improved version of zxcvbn" with LUDS estimation was the selected solution for our 2nd iteration. Figure 4.11 represents the selection process of the password strength measurements that we have followed in this iteration.

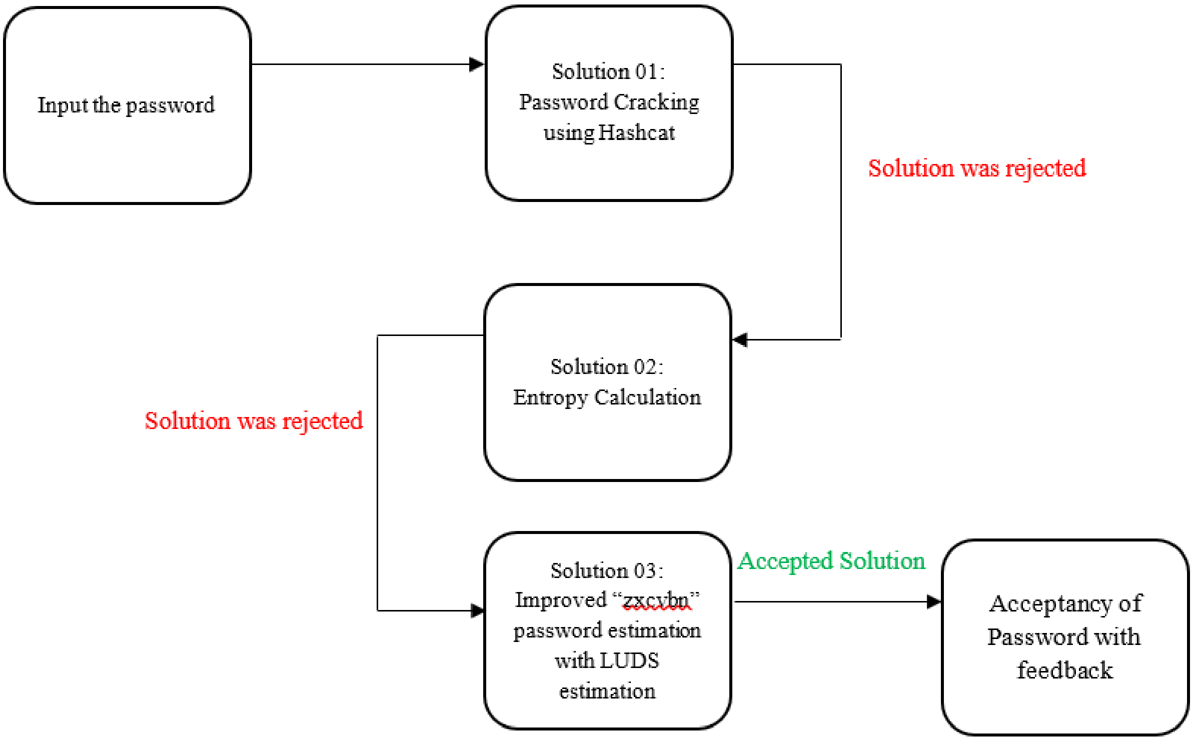

Input the password
Solution 01: Password Cracking using Hashcat
Solution was rejected
Solution 02: Entropy Calculation
Solution was rejected
Solution 03: Improved "zxcvbn" password estimation with LUDS estimation
Accepted Solution
Acceptancy of Password with feedback

Figure 4.11: *Candidate solutions for password strength measures and the selection process of the password strength measurements*

Candidate Solution 01: Password Cracking Using Hashcat

Initially, password generator was integrated with a GPU based password cracker called Hashcat to check the password resistance to cracking, equating its resistance to strength. Even though John the Ripper is another password cracker, Hashcat was selected as it includes more performance and benchmark results than John the Ripper.

Hashcat Vs John the Ripper *(*JTR*)*

Users of popular hacking tools who utilize the power of a computer's GPU to crack password hashes have reported about the performance of various GPUs' specifications against different hashes. Two notable high-end GPU's here are the Nvidia GTX Titan X from the year 2015 and the Nvidia GTX 1080 from the year 2016. The Titan X is able to crack MD5 hashes at a rate of 16904.6 MH/s (million hashes per second) & sha256 at a rate of 2113.0 MH/s in comparison the newer GTX 1080 was able to crack MD5 hashes at a rate of 25246.4 MH/s & sha256 at a rate of 2905.7 MH/s. This shows an improvement of approximately 49% for the MD5 cracking rate and an approximately 37.5% improvement in the sha256 cracking rate in the span of just a 1 year [78].

Both JTR and Hashcat are two most commonly used hacking tools. Hashcat utilizes the power of the computer's CPU as well as the GPU to crack passwords for all types of hashes, whereas JTR supports GPU cracking only for selected kinds of hashes. Analyzing the performance charts of Hashcat from 2012, Hashcat tool possesses the ability to crack passwords with a very high speed in comparison to other cracking tools [79] [80]. One other positive point which compliments Hashcat over John the Ripper cracking tool is its rapid updates released by the developer. The latest version of Hashcat v3.6.0 which was released on 9th June 2017 comprises of new set of algorithms, bug fixations and improvements spanning across many feature requirements [81] [82].

In first candidate solution, Hashcat aids to crack the given password in brute force attack, mask attack or dictionary attack and save the cracked password and the time taken to crack in a text file. Appendix F and Appendix G represent the cracking options and the saved text file with the information that was taken to crack the password "WaIf2" within the mask attack. Furthermore, GPU that used to crack it was Nvidia GEFORCE 940M and the CPU is Intel Core i7 6500U.

But this solution was infeasible due to following drawbacks.

Drawbacks

- Cracking time depends on the GPU performance
- It doesn’t provide any feedback except the cracking time

Candidate Solution 02: Entropy Calculation

Entropy is a measurement of the unpredictability of a password which can be used as a metric for password strength measured in terms of bits. Entropy value for a given password represents the quantitative value of the unpredictability of that password. A descriptive introduction on entropy calculation is stated in Chapter 02, Section 2.2.6.

The entropy value generated solely depends on the password length and the character space and it is independent of the physical specifications of the computer/device that we are using to obtain the measurement [46].

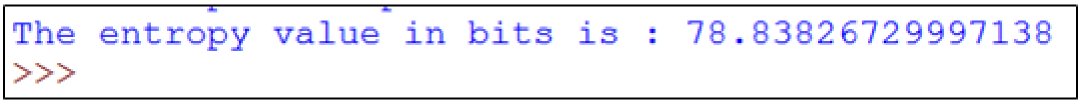
Using the equation **(**2.1**)** mentioned in Chapter 02, Section 2.1.6, the entropy of the mnemonic based password was generated using a python 3.6.1 code. Following example represents the entropy value for the password “IstwaE&YSLaI”. Figure 4.12 represents the system representation of the entropy value for the generated password.

Example:

Passphrase: I started to work at Ernst & Young Sri Lanka as Intern

Mnemonic based password: IstwaE&Y5!aI

Entropy Value: 78.837267



```
The entropy value in bits is : 78.83826729997138
>>>
```

Figure 4.12*: Results of the entropy calculating program for the password “IstwaE&Y5!aI“*

Drawbacks

Even though entropy value provides a quantitative measurement for the password strength, it was difficult to find standard reference values to identify the meaning of different entropy values or a cutoff value to verify the acceptability of the passwords whether it is resistant to guessability attacks. Even though it has been mentioned that higher entropy values are better, yet no proper source of justification was found to represent the meaning of the entropy values for a given password. However, KeePass has provided an entropy cut off values (Appendix H) in order to measure the password strength [94]. But prior research has stated, that Keypass overestimates the password [91]

Even though this is a common approach to evaluate the password strength, prior research have shown that entropy value is not a proper representation of password strength [94].

Entropy calculation solely depends on the password length and the character space and it fails to address the effects on the overall strength of the password when repeating characters or sequences are introduced to the password.

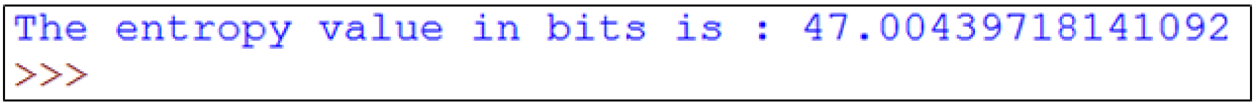
Consider the following password examples and the entropy results.

Example 01:

Password: aaaaaaaaaa

Password length (l) = 10

Character space = 26 (Only lowercase English letters)



```
The entropy value in bits is : 47.00439718141092
>>>
```

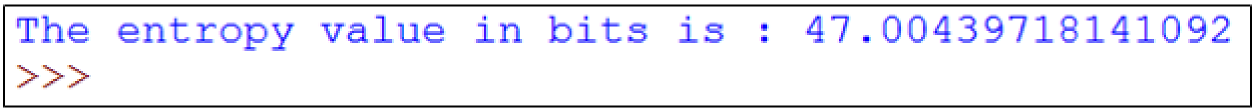
Figure 4.13: *Entropy Value for "aaaaaaaaaa"*

Example 02:

Password : asjcnfhtos

Password length (l) = 10

Character space = 26 (Only lowercase English letters)



```
The entropy value in bits is : 47.00439718141092
>>>
```

Figure 4.14: *Entropy Value for "asjcnfhtos"*

Considering above two passwords and their results, password of example 01 is highly vulnerable to brute force attacks and the entropy values for both above examples are same which implies both passwords have the same strength. This above scenario expresses the inaccuracy of entropy measurement given by the entropy calculation. Therefore, considering the drawbacks this solution was considered as infeasible to be used and a new technique or a tool needed to be used to measure the password strengths.

Candidate Solution 03: Improved version of “zxcvbn” password estimation with LUDS estimation

Prior research have stated that password strength depends on the attempts that attackers use to guess the password [95]. Also, literature stated that there are two common approaches to quantify the effectiveness of the password. They are using the entropy such as NIST and guessing tools against the password composition [94]. Considering the prior research which have been conducted recently, have used the guessing technique to evaluate the password composition and its strength [94] [95] [91].

The improved version of “zxcvbn” password strength estimator is a password strength measurement tool related to the above guessing concept and it provides the strength of a password in several aspects. Also, this improved version was released in 2016 and earlier version was released in 2012 that was presented by the Dropbox tech blog [[91]]. Therefore, iteration 2 strength checker (IT2-SC) was implemented using the improved “zxcvbn” password estimation along with its default features and LUDS estimation. In here, LUDS estimation provides the counts of lowercase and uppercase letters, digits and symbols.

IT2-SC was developed using the Python 3.6 and it includes the graphical user interface. One of the advantage was that improved “zxcvbn” password estimator is an open source estimator which is available as a python library called “zxcvbn” under MIT license.

The improved version of “zxcvbn” Password Estimation

The “zxcvbn” password estimator follows a 3-stage process to estimate the password strength in guessability perspective. Figure 4.15 shows the process that it follows to determine the strength measurements [91].

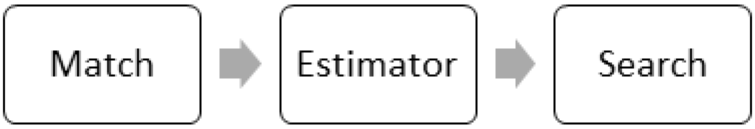


Figure 4.15: *Process of determining the password strength measurements*

This estimation works by assuming the attacker knows the password and then they determine how many guesses must be encountered to recover the password using the ranked dictionaries. The following table shows the dictionaries and the counts of data set that they use to assist for the password estimator.

Dictionary / Source	**Word counts**
RockYou	32M
Yahoo	450k
Xato	10M
Wikipedia	Have generated word list by using Wikipedia database dump that dated 2015-10-02. (Include all the Wikipedia articles without previous revisions, edit history, templates or metadata)
Wiktionary	40k
USCensus	10k

Table 4.10: *Source of words that aided to the password estimator*

Match: This is the initial stage that identifies the all possible patterns included in a given password. The pattern could be an either one of these types as shown in the following table.

Pattern	**Explanation**	**Example**
Reversed	Reversed text of a text	drowssap
L33t	Substitutions	@ for a, ! for 1
Sequence	Texts that represented with sequential form characters	1357, xyz
Repeat	Text includes the repetitions	aaaaa, cdcdcdcdcd
Keyboard	Keyboard words	Qwerty
Date	Text represents the date format	7/4/1993, 741993, 7493
Brute-force	Texts that do not present in dictionaries.	Z$hQ7tj

Table 4.11: *Type of patterns that can exist in a text.*

Furthermore, this estimation has the ability to identify the sequences of Cyrillic and Greek.

As an example, here we stated the same example that was used by the Daneil Lowe Wheeler (Dropbox inc.) in 25th USENIX Security Symposium [91].

Example:

Input word: lenovo2222

Possible patterns:

- Lenovo (password)
- eno (surname)
- no (English)
- no (Reversed)
- 2222 (Date – 2/2/2022)
- 2222 repeat

Estimation: Here, it determines the guessing attempts for each identified pattern.

Example:

Input word: lenovo2222

Possible patterns:

- Lenovo (password) →11007 guesses
- eno (surname) →3284 guesses
- no (English) →11 guesses
- no (Reversed) → 18 guesses
- 2222 (Date – 2/2/2022) →2190 guesses
- 2222 repeat→48 guesses

Search: This stage finds the simplest non-overlapping matches in order to construct the original password from the full set of possible matches.

Example:

Input word: lenovo2222

Possible patterns:

Lenovo (password) →11007 guesses
eno (surname) →3284 guesses
no (English) →11 guesses
no (Reversed) →18 guesses
2222 (Date – 2/2/2022) →2190 guesses
2222 (repeat) → 48 guesses

Considering above example Lenovo (password) and the 2222 (repeat) are the simplest non-overlapping matches in order to generate lenovo2222. Through the production of their guesses, it calculates the total guesses. For above example, it takes 10^6 guesses.

Considering above search section, it derives the count of guesses which will take to guess the original password. Dropbox has given a score value in the range of 0-4 for a password, considering the guesses count in order to measure the password strength. Recommended strength score for password is the 3 or 4 [91] [83] [84].

Following Table 4.12 shows the score and its meaning.

Score	Description
0	Too guessable: risky password (Guesses < 10^3)
1	Very guessable: protection from throttled online attacks (Guesses < 10^6)
2	Somewhat guessable: protection from unthrottled online attacks (Guesses < 10^8)
3	Safely unguessable: moderate protection from offline slow-hash scenario (Guesses < 10^10)
4	Very unguessable: strong protection from offline slow-hash scenario (Guesses >=10^10)

Table 4.12: *Scoring system for the password based on guesses*

Furthermore, this password estimation provides feedback for the given password in order to generate a stronger password if it is weak. Therefore, suggestions and warnings are given when the score is less than or equal to 2. Suggestion provides help to create more unguessable passwords while warning shows the mistakes that have been done such as "this is a top-10 common password". Additionally, we included the meaning of the score in the feedback.

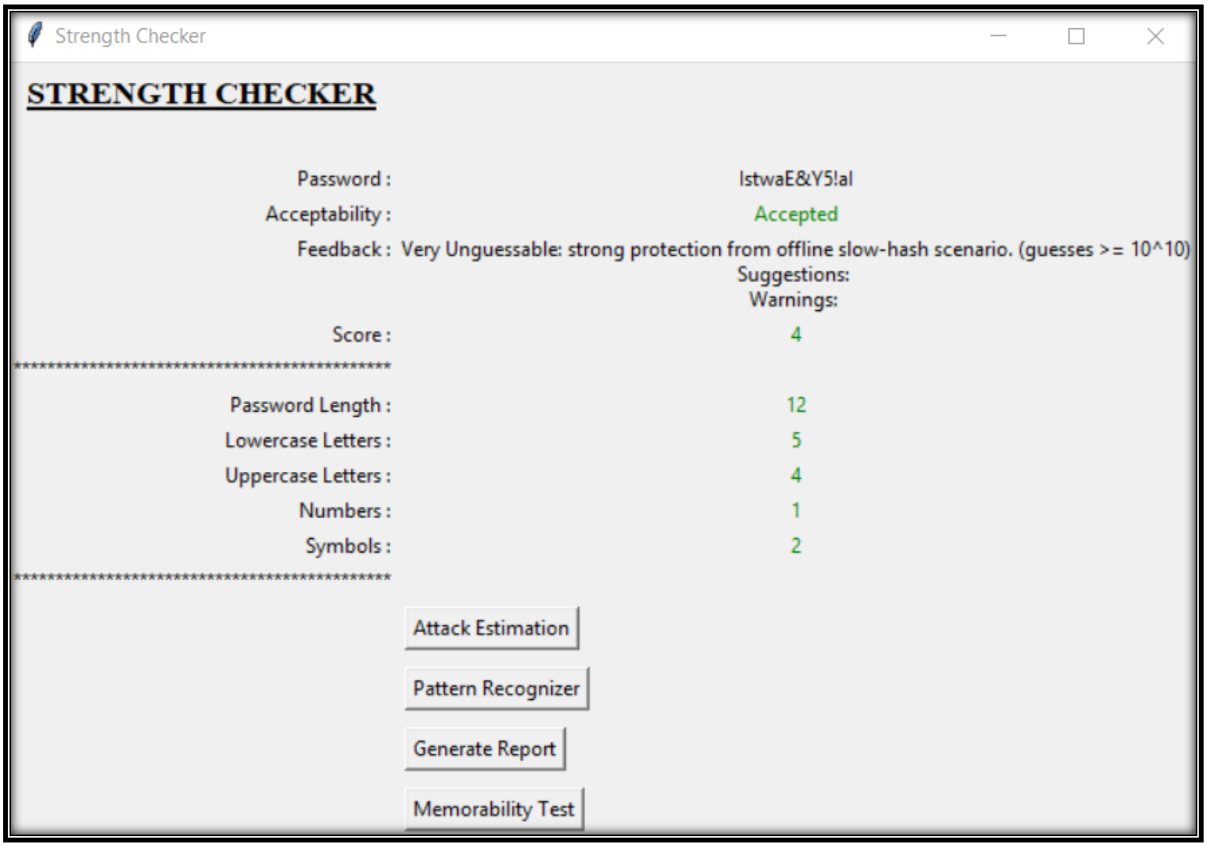
According to [91],

- Accuracy experiments for password estimation is done using four modern guessing attacks which are order-5 Markov model, Probabilistic Context-Free Grammar, Mangled Dictionary (Hashcat) and Mangled Dictionary (John the Ripper)
- Training data set is wide (Table from the top)
- Possible to add our own dictionaries
- Since this was released in 2016 by considering situations in that time, it includes more accuracy considering than other estimators available in research
- The checker ranks the most common passwords found in dictionaries and these passwords are identified as weak passwords
- For the experiments, entropy-based NIST, KeePass algorithms have been used

Considering above mentioned facts, it showed more robustness than candidate solution 1 and 2. Since it is the selected candidate solution as the password strength checker, we added following features as security considerations for our implementation.

- LUDS estimation: Count of Lowercases, Uppercases, Digits, and Numbers
- Overall score for a password in range on 0-4
- Pattern Matching: Information of identified patterns such as repeat, sequence, brute-force, existence of dictionaries
- Feedback on the password: Suggestions and Weaknesses
- Acceptance of the password according to the overall score and the LUDS estimation.

Figure 4.16 shows the basic view of strength checker that includes the LUDS estimation, overall score, feedback and acceptance of password. Figure 4.17 shows the identified patterns type for given password. It shows the pattern type, guesses that were required and the token that was considered for a particular pattern.

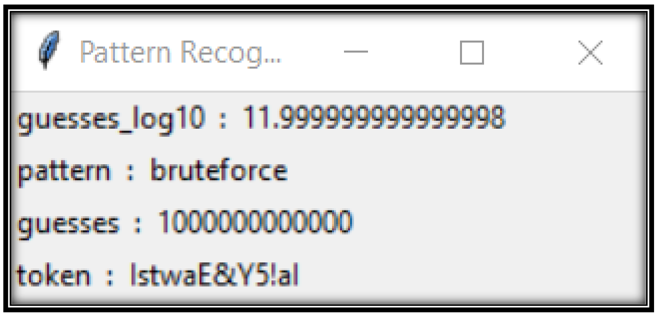


STRENGTH CHECKER

Password : IstwaE&Y5!aI
Acceptability : Accepted
Feedback : Very Unguessable: strong protection from offline slow-hash scenario. (guesses >= 10^10)
Suggestions:
Warnings:
Score : 4

Password Length : 12
Lowercase Letters : 5
Uppercase Letters : 4
Numbers : 1
Symbols : 2

Figure 4.16: *Basic view of the strength checker for password "IstwaE&Y5!aI"*



```
guesses_log10 : 11.999999999999998
pattern : bruteforce
guesses : 1000000000000
token : IstwaE&Y5!aI
```

Figure 4.17: *Identified patterns for "IstwaE&Y5!aI"*

According to the results of the strength checker, the user will proceed to the rehearsal module of the system.

4.3.3 Memory Module – (IT2-MM)

The simplified approach of IT1-MM memorability module did not sufficiently support users to move the password from their short-term memory to their long-term memory. This lead to impaired retention and recall of passwords resulting in poor memorability results.

To address this issue in Iteration 02 a password rehearsal module named IT2-MM was designed in order to aid users move the new password from their short-term memory (STM) to their long-term memory (LTM) through a process of elaborative rehearsal. The password rehearsal module offered a graphical user interface (GUI) developed using Python 3.6 and the Tkinter library, for users to rehearse their newly selected password so that it can be retained in the users LTM.

The rehearsal process was broken down into stages in such a way that users were able to rehearse and recall their password in an incremental and repetitive manner. The rehearsal strategy we employed gets users to perform an elaborative rehearsal. Users recall characters in the password by linking them to the initial phrase that was generated using an autobiographical memory.

Rehearsal Strategy

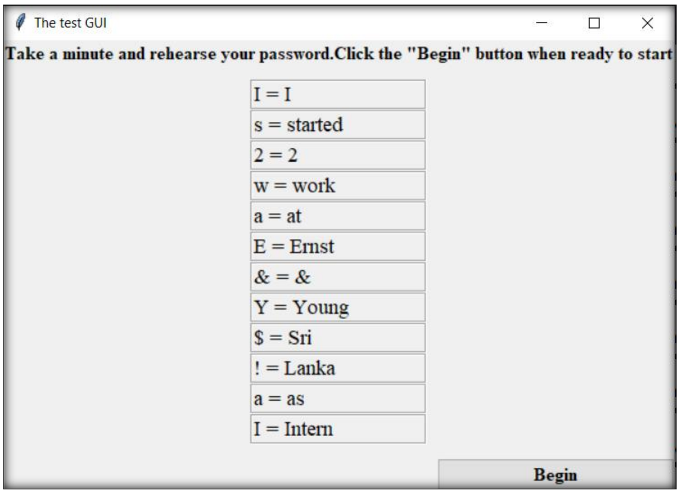
In psychology, rehearsal is the "cognitive process in which information is repeated over and over as a possible way of learning and remembering it" [85]. The two main memory rehearsal strategies in psychology are maintenance rehearsal and elaborative rehearsal. For the purpose of meeting our research goals, we took an elaborative rehearsal approach since it is better at transferring information into the long-term memory as opposed to maintenance rehearsal which is better at maintaining information is the short-term memory [85].

This rehearsal strategy cannot be directly coded into a program but instead can be facilitated by design. The approach to facilitate elaborative rehearsal in our design is to help the user link each character of the mangled password to the generated autobiographical memory phrase when rehearsing, this adds meaning to what is being rehearsed making it easier to retain in the users LTM. To achieve this, we present the password characters and the words of the autobiographical phrase at each point of rehearsal.

At the successful completion of each chunk rehearsal, the user is presented with a small distraction task, that involves the user solving a logic or mathematical problem. The reason for presenting these distraction tasks is to help prevent users from performing any clear memorization of the chunks. It is not important that the user gives the correct answer to the distraction tasks, mistakes won't have any impact on their assessment on the memorability of the password.

The Rehearsal Process

Before starting the rehearsal process the users were instructed on how to elaborately rehearse the password. Users were shown each character in their password linking them to the words in the users' autobiographical passphrase and asked to recall the password by linking each character to the autobiographical phrase. The user was instructed to take as much time as needed to study the password in this manner. Once the user feels comfortable the rehearsal process was initiated.



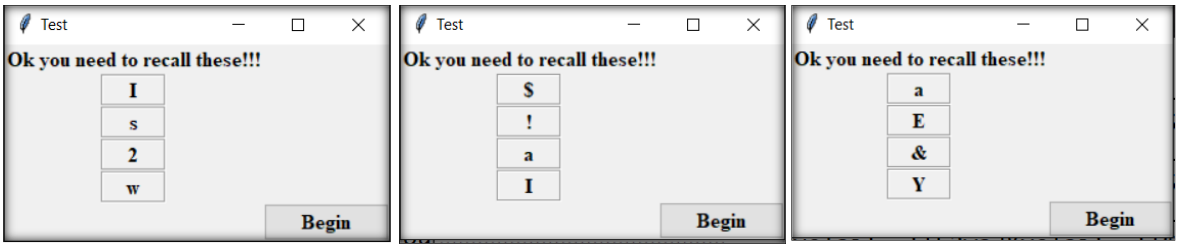
Take a minute and rehearse your password.Click the "Begin" button when ready to start

I = I
s = started
2 = 2
w = work
a = at
E = Ernst
& = &
Y = Young
$ = Sri
! = Lanka
a = as
I = Intern

Figure 4.18: *Linking password characters to the autobiographical phrase*

The rehearsal module divided the password into chunks, in order to break the larger password into smaller manageable portions. The user then rehearsed each individual chunk separately and once successful the rehearsed chunks were gradually amalgamated together so that the user gradually reached towards recalling the full-length password in an incremental fashion.

When dividing the password into chunks the rehearsal module segregated the password into chunks of 4-5 characters. The average chunk was 4 characters each, and by design at no point was a chunk allowed to be smaller than 2 characters or larger than 5 characters.



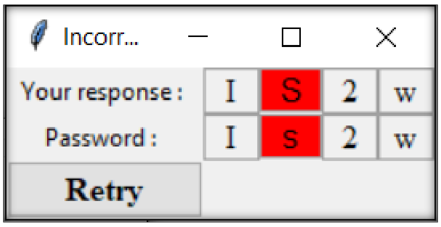
Ok you need to recall these!!!
I
s
2
w

Ok you need to recall these!!!
$
!
a
I

Ok you need to recall these!!!
a
E
&
Y

Figure 4.19: *Chunked segments of Is2waE&Y$!aI*

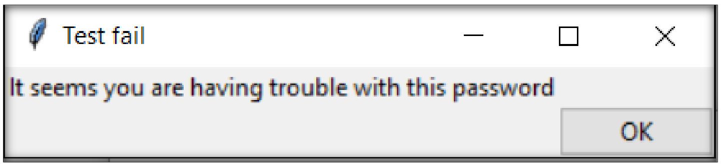
Once the password was chunked the user was presented with the first chunk, which the user has to recall successfully 3 times. If the user makes any mistakes when recalling the chunk, the rehearsal module pointed out the mistake and ask the user to try again.



Your response :	I	S	2	w
Password :	I	s	2	w

Figure 4.20: *Incorrect response*

If a user continuously made more than 3 erroneous attempts at recalling a given chunk the rehearsal module determined that the user is unable to retain the selected password and requested the user to go back and generate a new password.



It seems you are having trouble with this password

Figure 4.21: *Password rehearsal failure*

Upon successful completion of a rehearsing the first two chunks, the user was presented with a larger chunk which was an amalgamation of the first two chunks. The user will have to recall this chunk 3 times to be successful and will only be allowed 3 erroneous attempts. This process continues with the user rehearsing a new chunk and upon successful completion of the rehearsal, the rehearsed chunk was amalgamated to the previously rehearsed chunks and presented to the user for rehearsal.

Given below is a diagrammatic summary of the rehearsal process

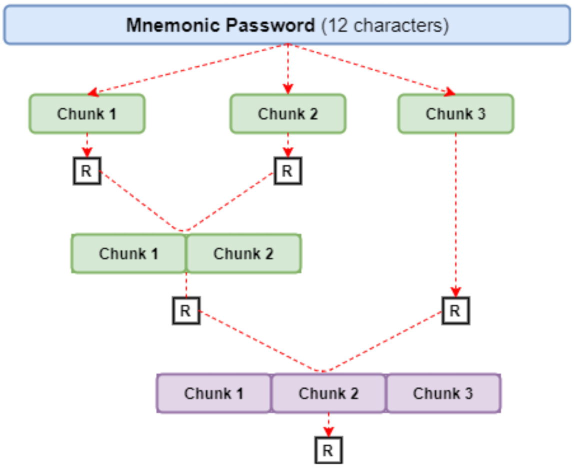


Figure 4.22: *Summary of the rehearsal process*

Web Site for evaluation

In order to test the memorability of the passwords generated by the system, a simple login site was created using php, html and mysql and the page was hosted in Amazon web services (http://18.220.242.157/research/index.php).

The initial registration of the user is done by one of the research team to avoid the risk of registering into the system using a wrong password as the registration process is not a part of memorability process.

The database of the system saves the respective emails, rehearsed password and the phrase used to generate the password along with basic information provided in the registration step with respect to each user. The passwords of the users are saved in plain text in order to identify the failed logins and to analyze the character mismatches done by the user by comparing the plaintext password saved in the database and the incorrect password input by the user. Figure 4.23 represents the registration form.

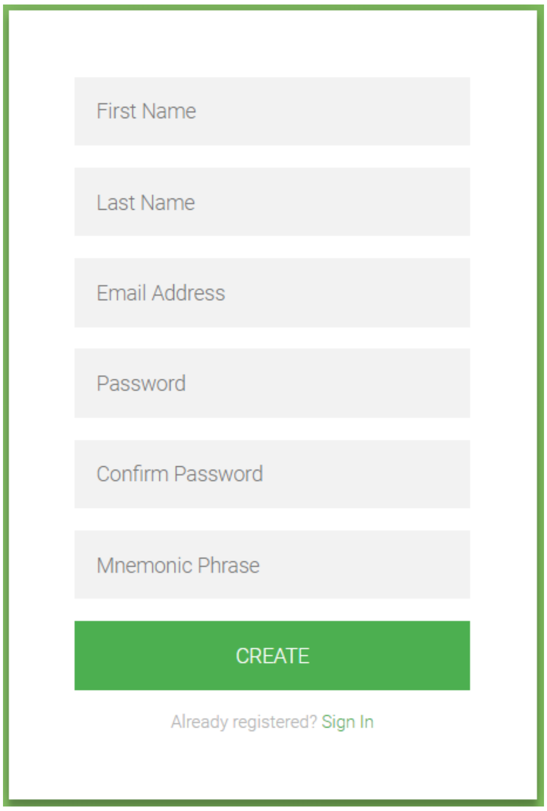
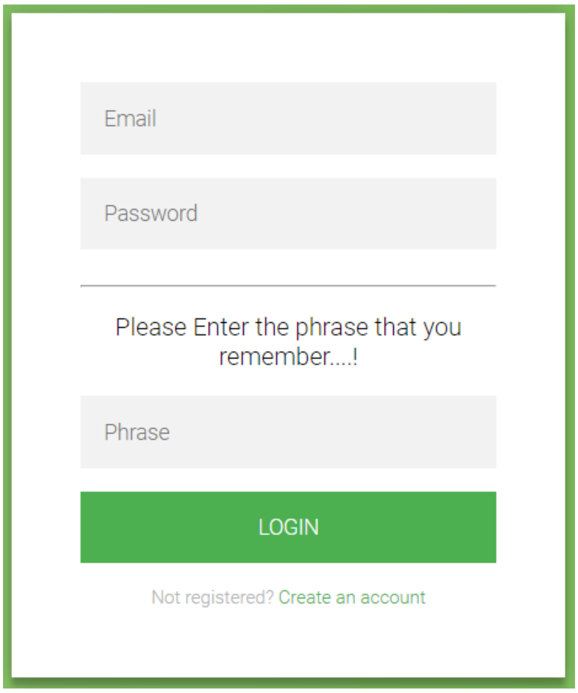


Figure 4.23: *Registration form to be filled by one of the researchers*

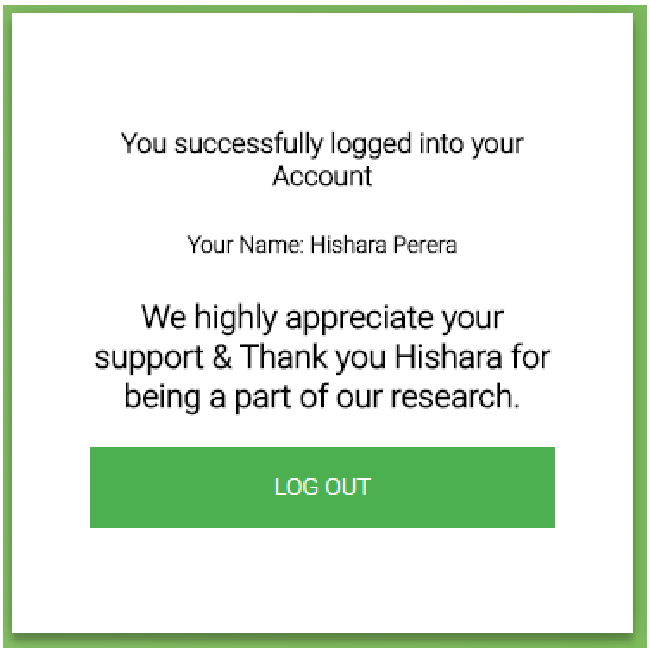
Once the user was registered and upon completion of the rehearsal module user is asked to login to the system using the provided email address and the password that was rehearsed during the rehearsal module along with the mnemonic phrase. Figure 4.24 shows the login page for user.



Please Enter the phrase that you remember....!

Figure 4.24: *Login page*

If the user successfully logins to the system within five attempts a message which indicates a successful login will be shown. If the user fails to sign in successfully, failure information is stored in the database for every incorrect login. Information that stored are the user details along with correct and incorrect passwords, and the phrase that user has used to recall the inserted password. Figure 4.25 shows the successful login message and Figure 4.26 shows the failure log entries.

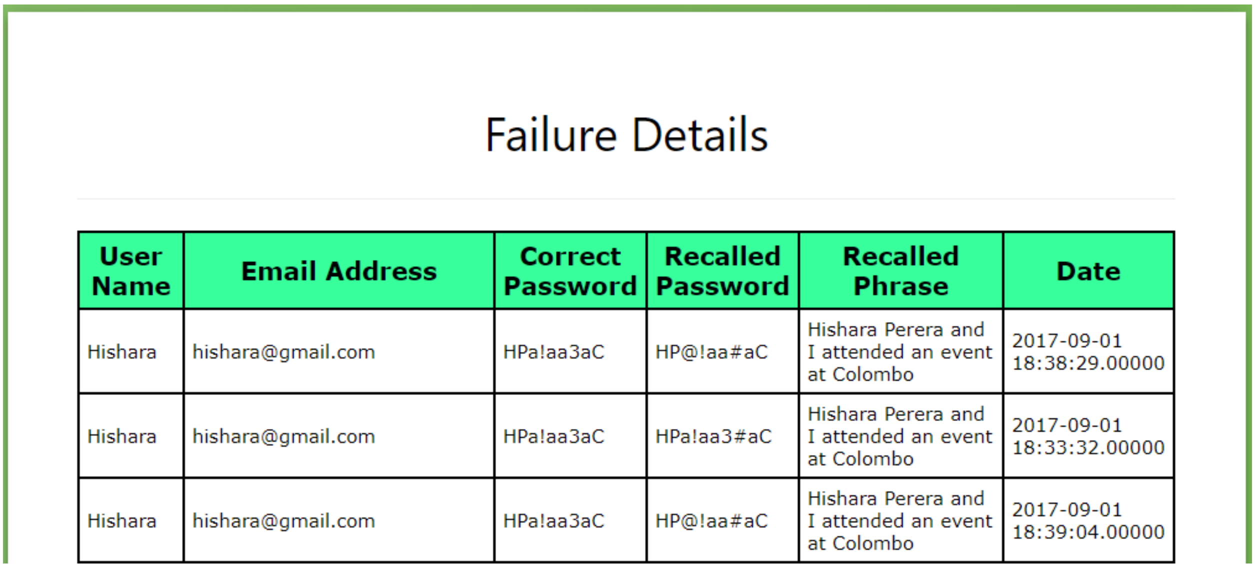


You successfully logged into your Account

Your Name: Hishara Perera

We highly appreciate your support & Thank you Hishara for being a part of our research.

Figure 4.25: *A successful login message*



Failure Details

User Name	Email Address	Correct Password	Recalled Password	Recalled Phrase	Date
Hishara	hishara@gmail.com	HPa!aa3aC	HP@!aa#aC	Hishara Perera and I attended an event at Colombo	2017-09-01 18:38:29.00000
Hishara	hishara@gmail.com	HPa!aa3aC	HPa!aa3#aC	Hishara Perera and I attended an event at Colombo	2017-09-01 18:33:32.00000
Hishara	hishara@gmail.com	HPa!aa3aC	HP@!aa#aC	Hishara Perera and I attended an event at Colombo	2017-09-01 18:39:04.00000

Figure 4.26: *Login entries written for every failed attempt*

Furthermore, the access log is stored in the database which records the users' each successful and failed attempt. In order to ease the analysis process, a summary of access information and failure information can be queried individually. Appendix I shows the access information for users and Appendix J shows the summary of one user.

4.3.4 Results

Results from the IT2-PG

Passwords generator was tested with 5 participants and summary of the results of the passwords created for each participant is shown in Table 4.13 shown below. Furthermore, Appendix K represents all the results of phrases generated by the system, candidate passwords generated for the selected phrase of each participant in a comprehensive manner.

Participant	Passphrase chosen	First Letter Mnemonic password	No. of Candidate passwords generated with mangling rules	Password chosen
Participant 01	You Nathaliya Jayawardena born on a Monday in 1993	YNJboaMi1	50	Ynjbo@m!1
Participant 02	Hishara Perera and I attended an event at Colombo	HPaIaaeaC	14	HPa!aa3aC
Participant 03	I started to work @ UCSC Mozilla Club from 0000	Istw@UMCf0	46	I$tw@UMCf0
Participant 04	You Lochana Thathsarani Batuwitage born on a Thursday in 1992	YLTBboaTi1	108	Yltbbo4ti!
Participant 05	I started to work @ Ceylon Electricity Board from 2016	Istw@CEBf2	79	Istw@c37f2

Table 4.13: *Results of the password generator for iteration 01*

Results from the IT2-SC

Table 4.14 shows the security results for above 5 participants’ selected passwords. Appendix K shows all the candidate passwords pertaining to the selected phrase by a participant.

Name		**Participant 01**	**Participant 02**	**Participant 03**	**Participant 04**	**Participant 05**
Password		Ynjbo@m!1	HPa!aa3aC	Istw@UMCf0	Yltbbo4ti!	Istw@c37f2
Acceptability		Accepted	Accepted	Accepted	Accepted	Accepted
Score		3	3	3	3	3
LUDS Estimation	**Password Length**	9	9	10	10	10
	Lowercase	5	4	3	6	5
	Uppercase	1	3	4	1	1
	Digits	1	1	1	2	3
	Symbols	2	1	2	1	1

Table 4.14: *Results of Security Checker in iteration 01*

Since all the password scored more than 2, they were considered as strong and the system did not provide any suggestions or warnings as feedback.

Below table shows the patterns identified in the passwords of participants while the score is estimated. The mark of “✓” represents a presence of a pattern type and “X” represents the absence of a pattern type.

	Brute-Force Attacks	**Available in Dictionary**	**L33t**	**Keyboard**	**Repeats**	**Sequence**	**Date**
Participant 01	✓	X	X	X	X	X	X
Participant 02	✓	**X**	**X**	**X**	**X**	**X**	**X**
Participant 03	✓	**X**	**X**	**X**	**X**	**X**	**X**
Participant 04	✓	✓ *	**X**	**X**	**X**	**X**	**X**
Participant 05	✓	**X**	**X**	**X**	**X**	**X**	**X**

Table 4.15: *Identified patterns types for each participants' passwords*

*IT2-SC identified the existence of dictionary word in the 4th participant's password. The word which matched with the dictionary word was the "bo4t" for the word "boat" found in the dictionary named "us_tv_and_film". IT2-SC has identified that letter "a" has been transformed into digit "4" indicating the l33t conversion to the letter "a".

Following table shows that count of each participants' candidate password list after the mangling rule was applied and the scores received from IT2-SC.

Name	**Candidate Passwords Count**	**Score**
Participant 1	50	All passwords received score 3
Participants 2	14	All passwords received score 3
Participant 3	46	All passwords received score 3
Participant 4	108	All passwords received score 3
Participant 5	79	All passwords received score 3

Table 4.16: *summarized results for the candidate passwords from the password strength checker for iteration 02*

Results from the IT2-MM

Following table represents the summary of the attempts taken by each participant to login to the website for IT02-MM.

Furthermore, Appendix L consists of the detailed results of the attempts taken by each participant in recalling test. An attempt represents the number of tries which a participant has used to successfully login to the system. For eg: 2-Attempts represents the participant has failed to login on the first try and have successfully logged into the system on the second try.

Participant	0 hours (Initial Login) (Attempts)	24 hours (Attempts)	15 days (Attempts)	45 days (Attempts)
Participant 01	1	1	3	1
Participant 02	1	4	2	2
Participant 03	1	4	2	1
Participant 04	1	4	4	2
Participant 05	1	2	2	1

Table 4.17: *Results from the memorability module for iteration 02*

4.3.5 Findings & Observations

When considering the results from the IT2-PG, an average number of generated phrases were 7 to 10 per participant, even if 15 default templates were added to the IT2-PG. And the reason was the number of phrases that generated were dependent on the public data made available by a user.

Furthermore, results from the feedback form showed that the wordings used in the templates by the system to create the phrases were familiar to the participants and the selection of a phrase from the list to create a password by the participants was easy.

Results from the feedback form showed that first letter mnemonic strategy which was used for password creation in this iteration was a comfortable option to be used in creating a personalized and seemingly random password for a given participant.

Mangling based substitutions were applied and the system had generated a large set of candidate passwords from the first letters of the phrase except for participant 02 giving the freedom to select a password as the participants wish.

When analyzing the candidate passwords generated for participant 02 using mangling rules (Appendix K), it was observable the default mangling rules set in John the Ripper applies the same conversion to repeated letters in the first letter mnemonic and not in a random manner. In consequent, this resulted in generating a lesser number of candidate passwords in comparison to the rest of the participants. (eg: all the “a”s in the first letter mnemonic “HPaIaaeaC” is replaced by “@” thus creating “HP@I@@e@C”). However, this did not have any negative impact on the strength of the generated password as shown in results in Results from the IT2-SC in Section 4.3.4.

Results from the feedback form shows that all the participants found it easy to select a mangled password from the candidate list, yet 40% (2 participants) of the participants were intimidated when these passwords were first introduced to them by the system.

When analyzing the results from “zxcvbn”, all the passwords selected by the participants have received a score of 3 implying that these passwords are safely unguessable providing protection from offline slow-hash attacks.

Also, in generating above score, IT2-SC showed that all the selected passwords’ compositions are accounted to the brute force pattern type. But only the 4th participant’s password composition included the dictionary word which is “bo4t” with l33t substitution. But IT2-SC showed that password can be used since it scored as 3. And all the selected passwords were not matched with any of other pattern types that make the password weaker which are l33t, keyboard, repeat, sequence and date.

According to the Table 4.16, all the candidate passwords for each participant received a score of 3 from IT2-SC. This implied that any candidate password created by IT2-PG has an acceptable level of strength.

Even though the memorized passwords were resilient to dictionary attacks, there is a risk that one might derive these candidate passwords computationally using the default templates available in IT2-PG along with the application of reverse engineering techniques to the default mangling rules which were used in IT2-PG.

By observing the number of failed logins over time (Figure 4.27) we can see a clear decline in the number of failed attempts over time.

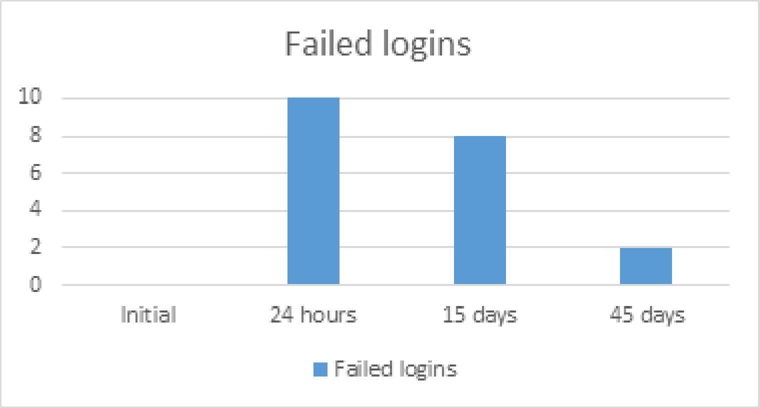


Figure 4.27: *Failed login attempts*

In the analysis of login errors four main categories of logins were noted:

- **Missing characters:** Where users failed to input a password character.
- **Incorrect character substitutions:** Where users incorrectly input mangled characters (example: ‘a’ instead of ‘@’)
- **Incorrect character:** Where users input an incorrect character.
- **Extra characters:** Where users input an extra password character.

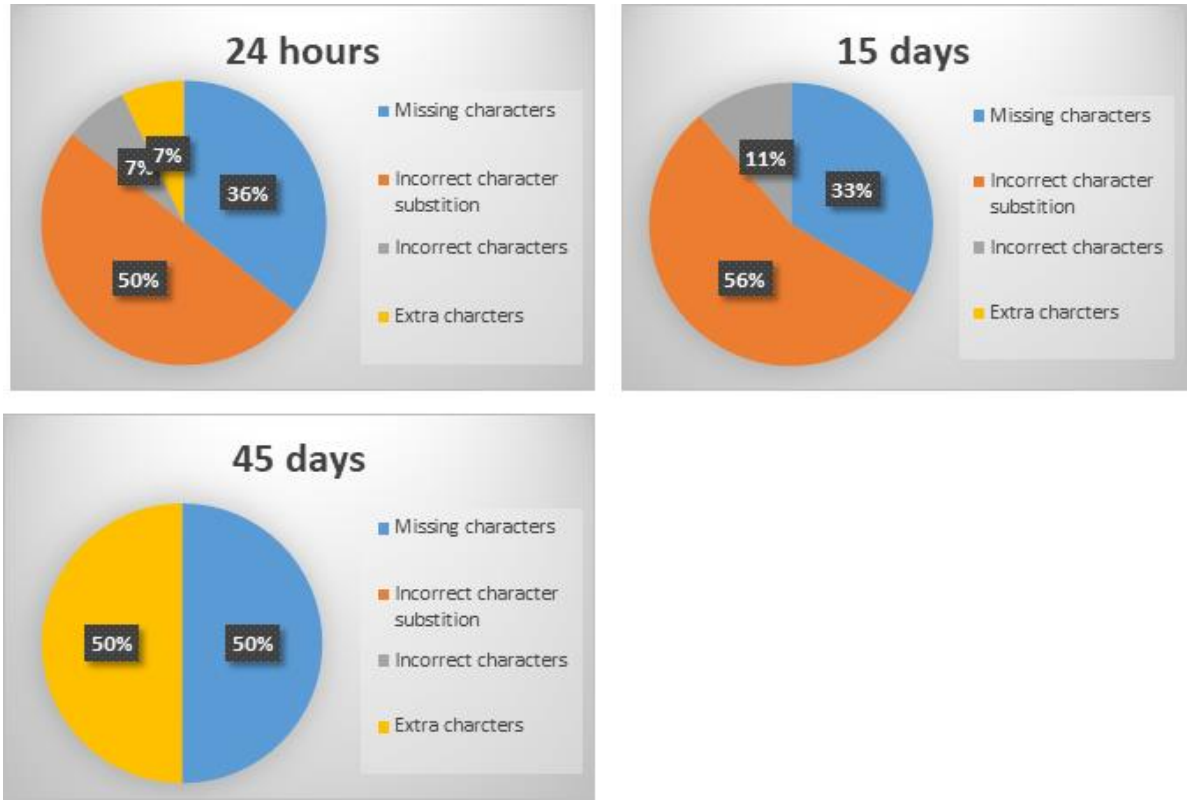


Figure 4.28: *Login error breakdown*

The analysis of error logs shows that users did not make any login errors in their initial login attempt, with all users being successful in their first attempt.

In analyzing failed login attempts after 24 hours and 15 hours we can see the majority of the errors at 50% and 56% respectively where as a result of incorrect character substitutions. When inquiring with the participants regarding this matter it was revealed that two major reasons contributed for making mistakes in character substitution. 3 of the 5 participants stated that they intended to input the special character but mistyped. While the remaining participants stated that they could only vaguely recall if the special character was needed in a certain position and had to guess.

Furthermore, at the 24 hours and 15 hours logins missing characters where the second largest contributor to failed logins with 36% and 33% respectively. Similar to character substations 3 of the 5 users stated that this error was due to mistyping and others stated that they made this mistake as a result of incorrectly recalling the phrase. This was observed when analyzing the phrase collected at each login attempt.

At the 45-day mark errors made where the result of extra characters and missing characters, further users have not shown any difficulty in character substitution at this point and all participants claimed these errors were due to mistyping the password.

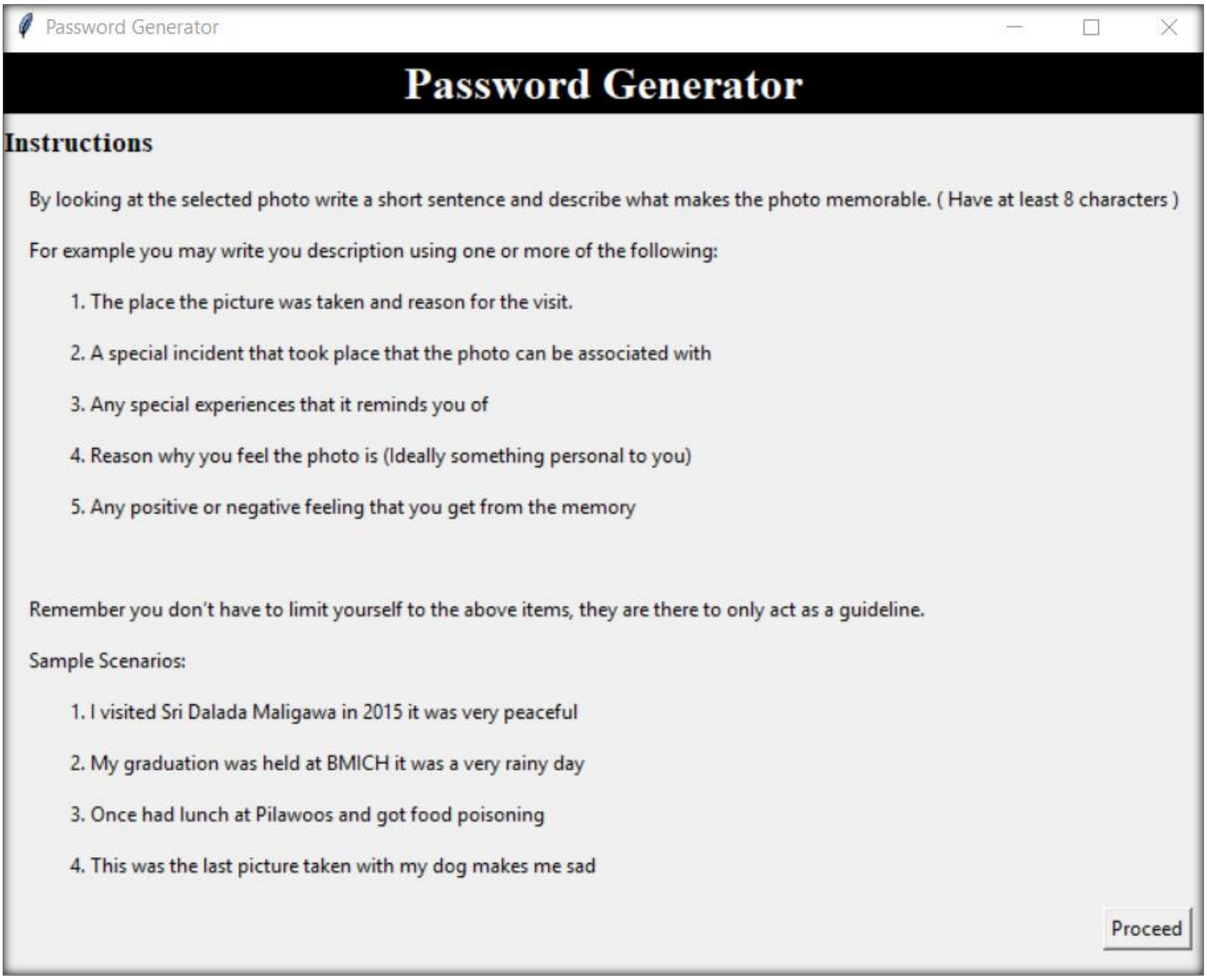
4.4 Iteration 03

4.4.1 Password Generator – (IT3-PG)

In the 3rd iteration, we didn’t change or replace the password generating strategy which was first letter mnemonic and the mangling rule applying process as iteration 2 has showed positive results with respect to these two approaches. Yet, the use of default templates for passphrase generation was replaced by a different approach as the candidate passwords generated through these templates can be computed using reverse engineering techniques.

Initially, users need to choose one of their images which has a specialty and significance to them. That image can be taken from any source. Therefore, it can be from mobile or any other storage medium or social media sites like Facebook, Instagram etc. Then users need to build up a phrase about that image based on what makes more significant and memorable the chosen image which can act as a mnemonic for the password generation and recall process. For an instance, it could be a description of what makes the image special or any associated feelings with the image etc. In the implementation IT3-PG, instructions are provided about the generation process of the mnemonic phrase along with a condition with respect to the length of the phrase created. The user has to input a sentence/s which has words more than 8 and if the user fails to match that condition, a warning is shown asking the user to meet this requirement. Prior research has shown that password creation policies which considers only about the length results in the creation of passwords that are highly resistant to guessing attacks [51]. Moreover, the newest release of NIST guideline states the minimum character length of a password is 8 for a user-chosen password[15]. Considering these factors, a condition on the length of the created sentence is added to IT3-PG.

Figure 4.29 shows the instruction window for users. Furthermore, users can use their own grammar and style that they are comfortable with to generate the phrase. Figure 4.30 shows the window that user has to insert the phrase with a sample phrase and Figure 4.31 shows the submitted window. It displays the user’s submitted phrase and its password. From this point onward, the same process that was used in iteration 2 is performed.



Instructions

By looking at the selected photo write a short sentence and describe what makes the photo memorable. (Have at least 8 characters)

For example you may write you description using one or more of the following:

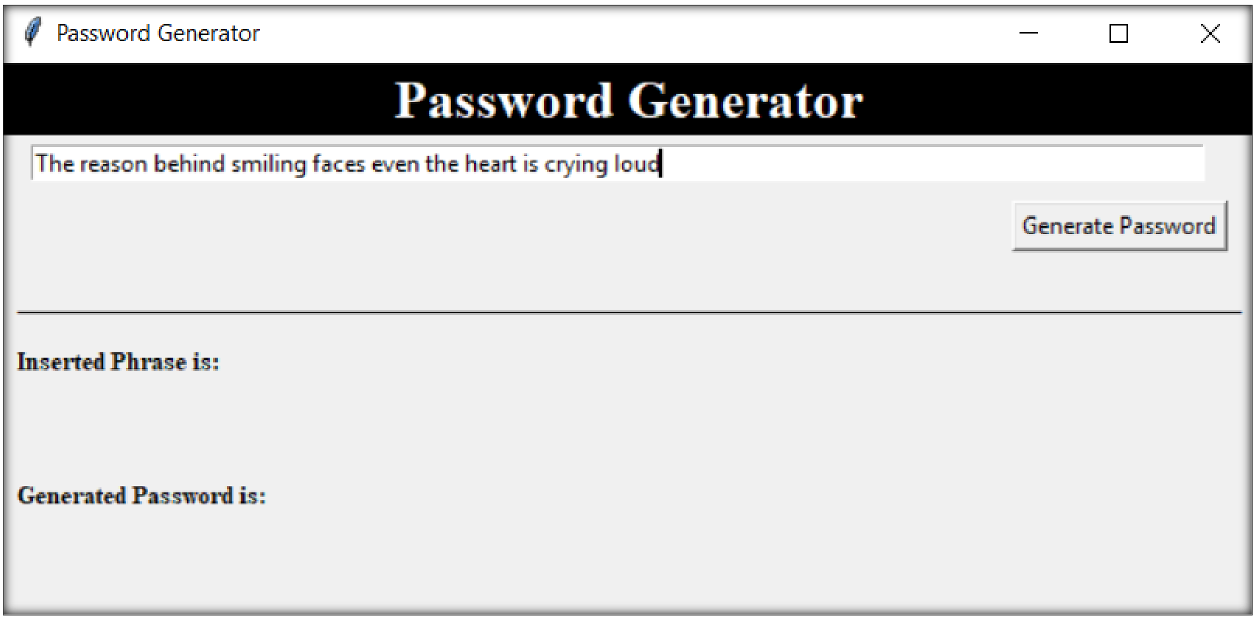
1. The place the picture was taken and reason for the visit.
2. A special incident that took place that the photo can be associated with
3. Any special experiences that it reminds you of
4. Reason why you feel the photo is (Ideally something personal to you)
5. Any positive or negative feeling that you get from the memory

Remember you don't have to limit yourself to the above items, they are there to only act as a guideline.

Sample Scenarios:

1. I visited Sri Dalada Maligawa in 2015 it was very peaceful
2. My graduation was held at BMICH it was a very rainy day
3. Once had lunch at Pilawoos and got food poisoning
4. This was the last picture taken with my dog makes me sad

Figure 4.29: *Instructions to generate the mnemonic phrase which makes more memorable*

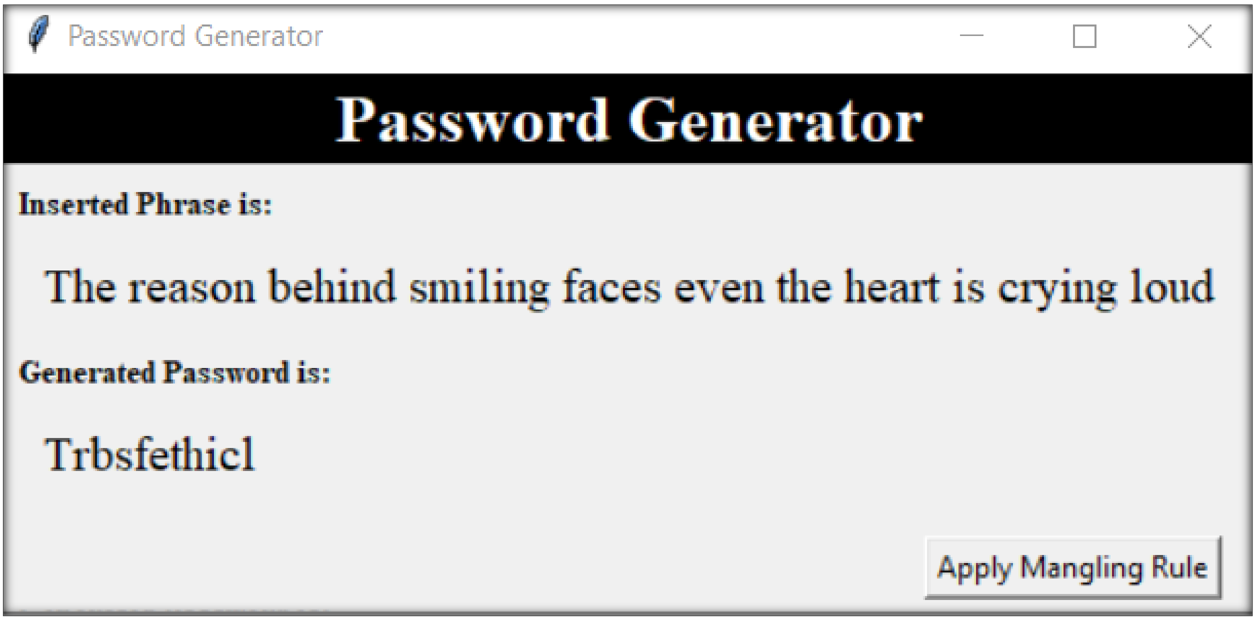


The reason behind smiling faces even the heart is crying loud

Inserted Phrase is:

Generated Password is:

Figure 4.30: *The window that user can insert the mnemonic phrase*



Password Generator

Inserted Phrase is:

The reason behind smiling faces even the heart is crying loud

Generated Password is:

Trbsfethicl

Figure 4.31: *Submitted window of the mnemonic phrase- Summary*

4.4.2 Strength Checker – (IT3-SC)

We used the exact password strength checker which we used in Iteration 02.

4.4.3 Memory Module – (IT3-MM)

As an improvement to IT2-MM it was decided to take a spaced repetition approach in IT3-MM. Studies have shown [86 – 88] that a spaced repetition approach can improve the long-term memorability and recall. In IT3-MM after the initial login, users must login to the system using the rehearsed password at some predefined incremental time intervals, the first login from the initial login will after a 12-hour interval, and in 1.5x increments from there on until space between two logins reach 40.5 hours. This results in a total of 4 logins within a period of 4 days from the initial login. Other aspects of the rehearsal process of IT2-MM remains the same in IT3-MM.

4.4.4 Results

Results from the IT3-PG

5 participants were taken for this iteration as well and the summary of the results is presented in Table 4.18 as shown below. The user study for the third iteration was done with same participants that we have taken in the second iteration and this was done in order to obtain a comparison of the results between the second and the third iterations.

Appendix M represents all the passwords generated by the system after applying mangling rules for each participant's passphrase.

Participant	Passphrase Created using the photograph	First Letter Mnemonic password	No. of Candidate passwords generated with mangling rules	Chosen password after applying mangling rules
Participant 01	I went to Siri pada with MTG 18 last February	IwtSpwM1lF	66	Iwt$pwm11f
Participant 02	My sister's big day at royal grand ja-ela with massina's brother	Msbdargjwmb	8	M5bd@rgjwmb
Participant 03	Sightseeing at Deniyaya was a wonderful memory in my life	SaDwawmiml	44	Sadwawm!m7
Participant 04	The reason behind smiling faces even the heart is crying loud	Trbsfethicl	28	Trb5feth!cl
Participant 05	school days are the best days in life, I love that time.	sdatbdilIltt	75	$dat8dilIltt

Table 4.18: *Results generated from the password generator for iteration 03*

Results from the IT3-SC

Table 4.19 shows the security results for above 5 participants' selected passwords. Appendix M shows all the candidate passwords pertaining to the selected phrase by a participant.

Name		**Participant 01**	**Participant 02**	**Participant 03**	**Participant 04**	**Participant 05**
Password		Iwt$pwm11f	M5bd@rgjwmb	Sadwawm!m7	Trb5feth!cl	$dat8dilIltt
Acceptability		Accepted	Accepted	Accepted	Accepted	Accepted
Score		3	4	3	4	4
LUDS Estimation	**Password Length**	10	11	10	11	12
	Lowercase	7	8	7	8	9
	Uppercase	1	1	1	1	1
	Digits	1	1	1	1	1
	Symbols	1	1	1	1	1

Table 4.19: *Results from the strength checker for iteration 03*

Since all the password scored more than 2, they were considered as strong and the system did not provide any suggestions or warnings as feedback.

Below table shows the patterns identified in the passwords of participants while the score is estimated. The mark of "✓" represents a presence of a pattern type and "X" represents the absence of a pattern type.

	Brute-Force Attacks	**Available in Dictionary**	**L33t**	**Keyboard**	**Repeats**	**Sequence**	**Date**
Participant 01	✓	X	X	X	X	X	X
Participant 02	✓	**X**	**X**	**X**	**X**	**X**	**X**
Participant 03	✓	**X**	**X**	**X**	**X**	**X**	**X**
Participant 04	✓	**X**	**X**	**X**	**X**	**X**	**X**
Participant 05	✓	**X**	**X**	**X**	**X**	**X**	**X**

Table 4.20: *Identified patterns types for each participants' passwords*

Following Table 4.21 shows the count of each participants' candidate password list after mangling rule was applied and the scores received from IT3-SC.

Name	Candidate Passwords Count	Score
Participant 1	66	All passwords received score of 3
Participan 2	8	All passwords received score of 4
Participant 3	44	All passwords received score of 3
Participant 4	28	All passwords received a score of 3 except password "Trb$f3thic". Password "Trb$f3thic" received score of 4
Participant 5	75	All passwords received score of 4

Table 4.21: *summarized results for the candidate passwords from the password strength checker for iteration 03*

Results from the IT3-MM

Furthermore, Appendix N consists of the detailed results of the attempts taken by each participant in the spaced repetitive process. An attempt represents the number of tries which a participant has used to successfully login to the system.

Participant	0 hours (Initial Login) Attempts	12 hours (Attempts)	18 hours (Attempts)	27 hours (Attempts)	40.5 hours (Attempts)
Participant 01	2	1	1	1	1
Participant 02	1	1	1	1	1
Participant 03	1	1	1	1	1
Participant 04	1	1	1	1	1
Participant 05	1	4	4	1	1

Table 4.22: *Results from the memorability module for iteration 02*

4.4.5 Findings & Observations

Similar to iteration 02, the password generator created a large set of candidate passwords after applying mangling rules except for participant 02, thus giving more freedom to the user in selecting a password.

The first letter mnemonic “Msbdargjwmb” generated for participant 02 which has 11 characters had created only 8 candidate passwords. When analyzing the candidate passwords generated for participant 02 (Appendix M), the default mangling rules set has not applied substitutions to the characters for the entire chunk of “rgjwm”. Even though a limited number of candidate passwords were created from the default mangling rules, all the candidate passwords generated were accepted by IT3-SC giving a score of 4.

The results from the online feedback form with respect to Iteration 03 suggested that on average, the creation of a phrase on their own by a participant was easy to some extent. Also on average, the participants find it comfortable to use the password created using the photograph that they have selected.

According to the Table 4.19 and Table 4.21 selected passwords and their all candidate passwords had a score 3 or 4 from the IT3-SC and these results implied that any passwords created by the IT3-PG has an acceptable level of strength. Also, any composition of selected passwords was not matched with the pattern types of l33t, keyboard, repeats, sequence and date and none of passwords' composition existed in dictionaries that were included in IT3-SC. The only type of pattern that IT3-SC gave as positive is the brute-force type.

Results show that IT3-PG had generated much stronger passwords in comparison to Iteration 02 giving a score of 4 to some candidate passwords. In order to evaluate the acceptability and the practical usability of the passwords memorized by the participants in Iteration 03, acceptability and the feedback given for these passwords were evaluated using strength meters integrated in few popular websites.

Comprehensive details about the results of the acceptability and the feedback given by these websites are shown in Appendix O.

Results from the evaluation show popular websites amazon, alibaba.com, ebay and other websites that were considered in the evaluation accepted all the passwords memorized by the participants in Iteration 03 to be used as user login passwords. Furthermore, it was significant that one of the popular password managers, LastPass had accepted these passwords to be used as a master password for their system. Therefore, by taking all these results in to consideration, it can be stated that the passwords selected and generated by the participants in Iteration 03 are acceptable and can be used practically by a user in the cyberspace.

When analyzing the results of the failed attempts in iteration 03, it was noted that there was a rise in a number of failed attempts up to the 18-hour mark (30 hours after initial login) and a drop to no erroneous logins.

Upon further analysis, it was noted that the failed attempts only belonged to one participant and the reason for the error was as a result of incorrect recollection of the phrase. Given below is a sample of incorrect phrases the participant recalled to the original phrase "school days are the best days in life, I love that time." and password "$dat8dilIltt".

Phrase	Password
school days are the best time in life, I love that time.	$dat8tilIltt
school life is the best days of life, I love that time.	$lit8dolIltt
school life is the best thing in life, I love that time.	$lit8tilIltt
school life is the best thing in life, I love that time.	$lit8tilIltt

Table 4.23: Sample of incorrect phrases that participant 05 used

It is clear that the participant had no issues recalling the overall idea of the phrase, but rather seems to have trouble with the wording.

This implies that there is a possibility that users will retain the overall idea but mistype the password as a result of not recalling the phrase they created in the correct wording.

4.5 Expert Validation on Psychological Approach

Given our limited experience and knowledge regarding theories related to human psychology, we decided to contact an external expert in a field related to the study of human memory and obtain their comments on the approach we have adopted in our research.

We were able to get in touch with Dr. Nishantha Gunasekera who is a Consultant Neurosurgeon at the Karapitiya Teaching Hospital Galle who agreed to help us by providing his expertise. We provided Dr. Nishantha with all details regarding our research the implementations, highlighting the different approaches taken with relation to human psychology along with the intention of doing so as well as our current findings and got his feedback on the following points.

Adopted approaches and techniques in password generation

a) The use of autobiographical episodic memories to generate memorable passphrases
b) The approach taken when applying autobiographical episodic memories to address the research problem
c) The use of mnemonics based on memorable phrases to generate passwords

Adopted approaches and techniques in password rehearsal

a) Use of elaborative rehearsal technique to rehearse generated passwords to improve the possibility of long-term retention
b) The approach taken to apply elaborative rehearsal in the password rehearsal process
c) The use of chunking to rehearse the password in an incremental manner to aid memorization
d) The use of spaced rehearsal approach to improve long-term retention of rehearsed password
e) Use of a limited user sample from a specific segment to conduct user studies to obtain a feedback

Upon evaluation of our work and the different approaches and techniques adopted to try and address the research problem by Dr. Nishantha we received the following comments.

"I have gone through the different techniques used for generation and rehearsal of passwords.
I feel in this limited endeavour, these techniques will suffice.
The ***memorizability*** *of anything depends on many other neurobiological factors which I think you need not go into at this point of your research."* (Appendix P)

It should be noted that these comments don't act as a substitute for a full user study, as they don't provide any external validity to the approach taken in our research. Rather, these comments are an expert's opinion on the sensibility of the different approaches and techniques related to human psychology used in addressing our research problem.

Chapter 05 – Evaluation & Discussion

Out of all the three iterations, we have carried out, passwords generated in iteration 01, have the highest strength in comparison to the passwords generated in iteration 02 and 03, even if the participants failed to successfully recall these passwords during the user study in iteration 1. In contrary, passwords generated in iterations 02 and 03 shows an acceptable level of resistance against password guessing attacks and were correctly recalled by the participants making these passwords comply with the current password policy standards. Additionally, results from iteration 03 show that passwords memorized in this interaction can be used in real-world applications. However, although overall result of iteration 03 has shown a greater improvement in acceptability than iteration 02, it should be noted that the last login in iteration 03 was only 4 days after the initial login. We were unable to evaluate the results after a more prolonged period given the time constraints; as a result, it is uncertain on what impact this method may have over time on recalling the password and accompanying phrase.

Through the course of our research, we identified key problems with regard to password-based authentication. The major issue identified was that users had a difficulty creating secure passwords that were memorable and password based authentication was becoming more and more vulnerable as a result [21,23,24].

We have identified that many schemes [8,16] have been presented as alternatives for password-based authentication. However, their limitations when it comes to ease and cost of implementation among other reasons, have resulted in the limited implementation of these schemes [19].

The model presented for password generation was built by using well-established theories and models in human psychology and computer security. When addressing memorability in generating passwords we used first letter mnemonics created using autobiographical episodic memories to support the retention and recall of information [89]. Autobiographical episodic memories which are in the long-term memory and can be recalled easily [89], and studies [56] have shown people find it easy to remember mnemonic phrases as opposed to random letters. Furthermore, to help in the long-term retention of the created passwords we set up an elaborative rehearsal and spaced repetition for users.

Prior research [91] have defined password strength as the how many attempts that attackers would use to guess a password. Therefore, checking the passwords in different dictionaries in order to provide the security measurement is a more important factor than calculating its entropy alone. Even if higher entropy means higher resistance to brute-force attacks, it is the attackers' last level technique. Because smart attackers' first-line approach is to guess the passwords based on dictionaries [83][84][91]Taking such matters into consideration in our approach to estimating password strength we have given priority to estimating guess ability in giving feedback on password strength.

The implemented system has been able to generate secure passwords which meet currently established guidelines as well as show resistance to popular attacks such as dictionary and brute force attacks. The used security model was recommended by prior research to be used with or without extensions as it was improved and released in 2016 reaching a higher maturity in comparison to other methods [91][93]. Although the limited user study was not sufficient to reasonably establish that the generated passwords memorable the result obtained were very promising**.**

Contribution

Despite a number of studies being available on trying to improve password memorability, this research project has explored some new approaches towards addressing the problem. Firstly, an approach using autobiographical episodic memories to create memorable passwords has not yet been explored by other researchers in the field making the approach of this research project a novelty.

The integration of images to aid text-based password creation has yet been studied only in one other study [86] to the best of our knowledge, however, this study does not use images of personal significance. Image-based techniques are primarily being used only for graphical password creation. By using this technique it allows our system to take advantage of the picture superiority effect [23] to improve memorability.

Furthermore, we have used a mix of both user generated mnemonic creation and system generated mnemonics, where other studies [1, 15] have only used one of the methods. In our implementation, the users create the initial mnemonic that they are comfortable with and the system mangles it to create the final mnemonic. Studies have shown that user generated mnemonics are more memorable whereas system generated mnemonics are strong [1][56], we have integrated both approaches in such a manner that advantages of both approaches are preserved to a reasonable extent.

Limitations

The memorability of the passwords generated in each iteration was tested using a user study comprising of a limited number of users chosen at random from fourth-year undergraduates from University of Colombo School of Computing. The results and findings which have been derived from this research are based on the limited user study. Hence, in the evaluation process, we have not paid much attention towards the external validity of the results presented in the research.

The performance evaluation of the entire package of our password generating system was calculated on how much the usage of a "single password" was comfortable for a user and its strength. Our research methodology and the results do not account to the effect of simultaneous usage of multiple passwords by a user which in fact lies beyond the scope of our research.

Enforcing security can be considered as a secondary concern for a user in the day to day work [69]. As the participants knew the study's true purpose, there is a risk that they may not have behaved normally as they would when creating and memorizing passwords in their day-to-day life which could consequently affect the overall observations and evaluation of the research. However, we have not evaluated how different moods, feelings and behavior of the user could affect the process of password generation in the user study as the comprehensive evaluation of the psychological and human behavior in password selection is beyond the scope of our research.

Open source tools John the Ripper and "zxcvbn" and their default capabilities have been used for the implementation of the password generating systems in iterations 02 and 03 based on the compliments made by prior research [90,91,92]. The password generators in these two iterations use the default mangling rule set in John the Ripper to create candidate passwords and the security of the passwords generated in Iterations 02 and 03 against dictionary attacks were evaluated using default dictionaries that are available in zxcvbn. Therefore, the password generation and strength evaluation process of the system is limited to the capabilities of the tools that we have integrated.

In addition to these considerations, when developing the graphical user interfaces of the system we have not paid much attention towards the human-computer interaction considerations such as visual processing and perception aspects. Furthermore, we have not taken into account the impact this may have on the usability and its effect on the memorability of passwords for users.

Chapter 06 – Conclusion

Text-based password authentication will remain an important means of authentication for some more time to come. Although authentication schemes such as graphical passwords and biometric authentication have been presented as alternatives to text-based passwords concerns relating to implementation and cost have restricted widespread implementation of such schemes [16]. On the contrary text-based password authentication can be implemented with relative ease with minimal associated costs [10, 11].

The results obtained from our limited user study shows that the password generating approach presented was accepted by users as well as shows promise of being able to balance password security and memorability. If results of a full user study show similar results this would be a very promising and novel approach towards solving an important issue in information security. The approach presented in this research can be used by both organizations as well as individuals for password generation to secure important logins.

Furthermore, although users have their own methods and approaches to creating passwords, studies show these methods are predictable and vulnerable especially due to misconceptions about the security of users with less awareness about password security [34]. The approach we have presented has shown to be user-friendly and takes into account best practices in password creation, so users if proven to be viable our approach could help many users in creating secure and memorable passwords.

Chapter 07 – Future Work

This kind of security usability studies related research require an explicitly defined user study approach as human memory is dependent on various demographics such as age, education as described in Chapter 02.

In our research, the user study was limited to 5 participants due to the 1-year time constraint. Password memorability related usability studies of related research projects [69, 86] have conducted explicitly defined user studies to study human memory. Human memory is dependent on various demographics such as age, education as described in Chapter 02. Considering these factors our research requires a properly designed user study in order to achieve a higher accuracy and generalizability of the results.

Developed entire package of password generating system takes a considerable amount of time to generate and rehearse a password along with the spaced repetition task. In the initial use of this process by a user faces some slight distractions since he/she is not familiar with the process. We could observe that from our limited user study. Therefore, it can affect to password selection, rehearsal and the overall results indirectly. However, if he/she uses this process again and again for a long time, adaptability on the process may make smooth usage and better results. Therefore, it needs to be evaluated with a properly designed user study.

Furthermore, it needs to be evaluated the ability of managing multiple passwords simultaneously with this model. To accomplish above consideration, it takes a considerable amount of time with a proper user test that evaluates the abilities step by steps.

Application improvements

The current version of the password generating system stores the selected phrase, first letter mnemonic and the respective candidate passwords in text files as plain texts. Above text files will be overwritten with new data once a new password generation process was carried out. This process in consequence could give rise to few security concerns such as unauthorized acquisition of the password related data. To avert this problem, the system can be improved to store such data in the volatile memory of the computer in order to prevent security breaches.

Users give different priorities to different systems and applications. Therefore, users tend to create passwords that include different strength levels based on the priority as defined by them [69]. As a result, users may not be pleased to use the system of our research to create passwords for low priority applications. As a solution to this concern, our system can be improved such a way that it caters to different priority levels as defined by the users to the systems and applications.

An example for possible categorization of applications is stated in the following Table 7.1

Priority Level of the application	Security model	Memorability Model
High priority	Current system can be used	
Low priority	Minimum length of 8 characters to be used in the passwords	Elaborative rehearsal without chunking and distractor activities

Table 7.1: *Categorization of applications and respective system*

However, it should be noted that a separate user study will have to be conducted to check the feasibility of the solution offered for low priority password generation system.

In the development process of our system, we have not considered the human-computer interactions to improve the usability of the system which could interrupt smooth execution of the steps in the password generating process. Thus, in the future development process, this consideration has to be dealt with. Along with these improvements, the entire package of password generation system can be developed as a browser plugin and improve compatibility of the system among different browsers. Consequently, the security model and the memory model of the password generating system has to be reevaluated covering multiple context (eg: Sri Lankan) as the state of the art advances.

References

[1] C_K. A. Juang, S. Ranganayakulu, and J. S. Greenstein, “Using System-Generated Mnemonics to Improve the Usability and Security of Password Authentication,” pp. 506–510, 2016

[2] S. Bosworth, Computer security handbook. Hoboken, NJ: Wiley, 2014.

[3] Komanduri, S., Shay, R., Kelley, P., Mazurek, M. L., Bauer, L., Christin, N., Egelman, S.)2011(. “Of Passwords and People: Measuring the Effect of Password-Composition Policies”.

[4] J. Yan, A. Blackwell, R. Anderson, and A. Grant, “Password memorability and security: empirical results,” IEEE Security & Privacy Magazine, vol. 2, no. 5, pp. 25–31, 2004.

[5] "mnemonic | Definition of mnemonic in English by Oxford Dictionaries", Oxford Dictionaries | English, 2017. [Online]. Available: https://en.oxforddictionaries.com/definition/mnemonic. [Accessed: 18- May-2017].

[6] P. Kelley, S. Komanduri, M. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. Cranor and J. Lopez, "Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms", 2012 IEEE Symposium on Security and Privacy, 2012.

[7] Deborah Nelson, Kim-Phuong L. Vu, “Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords“, in Computers in Human Behavior,705-715, pp

[8] D. Kim and M. G. Solomon, Fundamentals of information systems security. Burlington, MA: Jones & Bartlett Learning, 2012.

[9] D. Florencio and C. Herley, “A large-scale study of web password habits,” Proceedings of the 16th international conference on World Wide Web - WWW 07, 2007.

[10] P. Elftmann, “Secure Alternatives to Authentication Mechanisms submitted by,” Aachen Univ. Aachen, Ger. Thesis, no. October, pp. 1–92, 2006.

[11] Charathsandran, Gayathiri, “Text Password Survey: Transition from First Generation to Second Generation“, unpublished.

[12] P. G. Inglesant and M. A. Sasse, “The true cost of unusable password policies,”
Proceedings of the 28th international conference on Human factors in computing systems -
CHI 10, 2010.

[13] J. Andress, The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Amsterdam: Elsevier, 2011.

[14] C. E. Shannon, “Prediction and Entropy of Printed English”, Bell System Technical Journal, v.30, n. 1,1951, pp. 50-64.

]15[C. Kuo, S. Romanosky, and L. F. Cranor, “Human selection of mnemonic phrase-based passwords,” Proceedings of the second symposium on Usable privacy and security - SOUPS 06, 2006.
[16] Lawrence O’Gorman, et al, “Comparing Passwords, Tokens, and Biometrics for User Authentication“, IEEE , vol. 91, pp. 2020 - 2021, 12, Dec. 2003.

[17] Blake Ives Kenneth R. Walsh Helmut Schneider , “The Domino Effect of Password Reuse“, Communications of the ACM - Human-computer etiquette, vol. 47, pp. 75-78, April 2004.

[18] Kanaley, R. Login error trouble keeping track of all Your sign-ons? Here’s a place to keep your electronic keys, but you’d better remember the pass- word. San Jose Mercury News (Feb. 4, 2001)

[19] C. Herley, P. C. V. Oorschot, and A. S. Patrick, “Passwords: If We’re So Smart, Why Are We Still Using Them?,” Financial Cryptography and Data Security Lecture Notes in Computer Science, pp. 230–237, 2009.

[20] S. A. S. Acharya, “Two Factor Authentication Using Smartphone Generated One Time Password,” IOSR Journal of Computer Engineering, vol. 11, no. 2, pp. 85–90, 2013.

[21] E. D. Cristofaro, H. Du, J. Freudiger, and G. Norcie, “A Comparative Usability Study of Two-Factor Authentication,” Proceedings 2014 Workshop on Usable Security, 2014.

[22] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, “Usable security: User preferences for authentication methods in eBanking and the effects of experience,” Interacting with Computers, vol. 22, no. 3, pp. 153–164, 2010.

[23] H. Kumar, S. Arohi, and F. U. Khan, “Graphical Password Authentication Schemes: Current Status and Key Issues,” nt. J. Eng. Innov. Technol.(IJEIT), vol. 10, no. 2, pp. 437–443, 2013.

[24] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, “Authentication using graphical passwords,” Proceedings of the 2005 symposium on Usable privacy and security - SOUPS 05, 2005

[25] Real User Corporation, Passfaces TM http://www.realuser.com, Accessed on January 2017

[26] Dhamija and A. Perrig. “Déjà vu: A User Study Using Images for Authentication”, In Proceedings of the USENIX Security Symposium, 2000.

[27] G. Blonder, “Graphical Password”, In Lucent Technologies, Inc., Murray Hill, NJ,United States Patent 5559961, 1996

[28] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. The design and analysis of graphical passwords. Proceedings of the Eighth USENIX Security Symposium,, pages 1–14, 1999.

[29] H. Srivastava, “A Comparison Based Study on Biometrics for Human Recognition,” IOSR Journal of Computer Engineering, vol. 15, no. 1, pp. 22–29, 2013.

[30] G. S. Karimovich and K. Z. Turakulovich, “Biometric cryptosystems: Open issues and challenges,” 2016 International Conference on Information Science and Communications Technologies (ICISCT), 2016.

[31] Jain, Anil K. Nandakumar, Karthik, “Biometric authentication: System security and user privacy“, Computer, vol. 45, pp. 87-92, November 2012.

[32] H. P. Bahrick, “Semantic memory content in permastore: Fifty years of memory for Spanish learned in school.,” Journal of Experimental Psychology: General, vol. 113, no. 1, pp. 1–29, 1984.

[33] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, “The Tangled Web of Password Reuse,” Proceedings 2014 Network and Distributed System Security Symposium, 2014.

[34] B. Ur et al., “‘ I Added “!” at the End to Make It Secure ’: Observing Password Creation in the Lab,” Proc. Elev. Symp. Usable Priv. Secur., pp. 123–140, 2015.

[35] J. Bonneau, “The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords,” 2012 IEEE Symposium on Security and Privacy, 2012.

[36] Ji, Shouling Yang, Shukun Hu, Xin, et al, “Zero-sum password cracking game: A large-scale empirical study on the crackability, correlation, and security of passwords“, IEEE Transactions on Dependable and Secure Computing, vol. PP, pp. 1, September 2015

[37] Bruce Schneier. (2007, January 11). Choosing Secure Passwords (1st ed.) [Online]. Available: https://www.schneier.com/blog/archives/200

[38] Ashley.Creating a strong password [Online]. Available: https://support.google.com/accounts/answers/32040

[39] Joe Sanjour, Andrew Arensburger, Anne Brink. (03 October, 2002). Choosing a Good Password [Online]. Available: www.cs.umd.edu/faq/Passwords.shtml

[40] Manjesh Kumar Hanawal, Rajesh Sundaresan, “Randomised attacks on passwords“, in Programme on Advanced Research in Mathematical Engineering, Bangalore, India.

[41] SANS, “Password Construction Guidelines,” pp. 1–3, 2014.

[42] C. Castelluccia, M. Dürmuth, and D. Perito, “Adaptive Password-Strength Meters from Markov Models.,” in NDSS, 2012.

[43] J. Galbally, I. Coisel, and I. Sanchez, “A New Multimodal Approach for Password Strength Estimation - Part I: Theory and Algorithms.,” IEEE Trans. Information Forensics and Security, vol. 12, no. 12, pp. 2829–2844, 2017.

[44] S. Houshmand Yazdi, "Analyzing Password Strength and Efficient Password Cracking", 2017

[45] C. Matthew Weir, "Using Probabilistic Techniques to Aid in Password Cracking Attacks", Florida State University, 2010.

[46] National Institute of Standards and Technology, U.S Department of Commerce, "NIST Special Publication 800-63-2", U.S. Department of Commerce, 2013.

[47] A. Narayanan and V. Shmatikov, “Fast dictionary attacks on passwords using time-space tradeoff.,” in ACM Conference on Computer and Communications Security, 2005, pp. 364–372.

[48] B. Ur, S. M. Segreti, L. Bauer, N. Christin, L. F. Cranor, S. Komanduri, D. Kurilova, M. L. Mazurek, W. Melicher, and R. Shay, “Measuring Real-World Accuracies and Biases in Modeling Password Guessability.,” in USENIX Security Symposium, 2015, pp. 463–481

[49] The human memory [Online]. Available: www.human-memory.net/intro_what.html

[50] Paul Reber.What Is the Memory Capacity of the Human Brain? [Online]. Available: https://www.scientificamerican.com/article/what-is-the-memory-capacity/

[51] The Brain made simple [Online]. Available: brainmadesimple.com/memory/

[52] MEMORY: A Five-Day Unit Lesson Plan for High School Psychology Teachers, 1st ed., American Psychological Association, Washington DC, 1-58, pp.

[53] S. Das, E. Hayashi, J. I. Hong and I. Oakley, "Evaluating the Use of Autobiographical Memory for Authentication", Symposium On Usable Privacy and Security (SOUPS), 2012.

[54] Peter W. Foltz, “Models of Human memory and computer memory and computer information retrieval: Similar approaches to similar problems “,

[55] Douglas L. Hintzman, “MINERVA 2: A simulation model of human memory“, in Behavior Research Methods, Instruments, & Computers, 96-101, pp.

[56] Wijesekera, P., Cherapau, I., Samarakoon, A., & Beznosov, K., “Cued Mnemonics for Better Security and Memorability“, 2014

[57] A. G. Greenwald and M. M. S. Johnson, “The generation effect extended: Memory enhancement for generation cues,” Memory & Cognition, vol. 17, no. 6, pp. 673–681, 1989.

[58] Alan S. Brown1, Elisabeth Bracken, Sandy Zoccoli, King Douglas, “Generating and Remembering Passwords“, in Applied Cognitive Psychology, 641–651, pp. .

[59] A. S. Brown,T A. Rahhal, “Hiding valuables: A questionnaire study of mnemonically risky behavior”, Applied Cognitive Psychology, vol 8, issue 2, pp 141 -154, April 1994

[60] Pilar, D.R., Jaeger, A., Gomes, C.F.A., Stein, L.M.: Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background. PLoS One 7(12), e51067 (2012)

[61] Lyastani, S., Acar, Y., Fahl, S. and Backes, M. (2016). Improving Password Memorability and Strength Using Mangling Rules.
[62] Gehringer, E.F. (2002), “Choosing passwords: Security and human factors”, Technology and Society, pp369-373.
[63] R. Butler and M. J. Butler, “An Assessment of the Human Factors Affecting the Password Performance of South African Online Consumers,” no. Haisa, pp. 150–161, 2014.

[64] A. Psychology, R. A. M. Humrro, and R. A. Mccloy, “A Confirmatory Test of a Model of Performance Determinants,” no. August 1994, 2015.

[65] Australian Computer Emergency Response Team (AusCERT). Choosing good passwords. AusCERT Reference # GoodPasswords, February 1, 2001. http://www.auscert.org.au/render.html?it=2260 (accessed March 2006).

[66] G. B. Duggan, H. Johnson, and B. Grawemeyer, “Rational security: Modelling everyday password use.,” Int. J. Hum.-Comput. Stud., vol. 70, no. 6, pp. 415–431, 2012.

[67] Michelle L. Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur, “Measuring password guessability for an entire university“, in Computer & communications security, Berlin, Berlin, 173-186 , pp. .

[68] R. Wash, E. Rader, and R. Berman, “Understanding Password Choices : How Frequently Entered Passwords are Re-used Across Websites,” 2016.

[69] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley, “Does My Password Go up to Eleven ? The Impact of Password Meters on Password Selection,” pp. 2379–2388, 2013.

[70] E. Stobert and R. Biddle, “The Password Life Cycle : User Behaviour in Managing Passwords,” pp. 243–255.

[71] J. Campbell, “USER BEHAVIOURS ASSOCIATED WITH PASSWORD SECURITY AND,” vol. 14, no. 1, pp. 81–100, 2006.

[72] Alain Forget, Sonia Chiasson, et.al, “Improving text passwords through persuasion“, in Proceedings of the 4th Symposium on Usable Privacy and Security, SOUPS 2008, Pittsburgh, Pennsylvania, 1-12, pp. .

[73] “2017 Cost of Data Breach Study,” Ponemon Institute LLC, Traverse City, Michigan, rep.,2017

]74[“2017 Data Breach Investigations Report,” Verizon LLC, rep., 2017.

]75[V. Goel, “Verizon Will Pay $350 Million Less for Yahoo,” The New York Times, 21- Feb-2017.]Online[. Available:https://www.nytimes.com/2017/02/21/technology/verizonwill-pay-350-million-less-for- yahoo.html.]Accessed: 30-Oct-2017[.

]76[T. Hornyak, “Hack to cost Sony $35 million in IT repairs,” CSO Online, 04-Feb-2015.]Online[. Available: https://www.csoonline.com/article/2879444/data-breach/hack-to-costsony-35-million-in-it-repairs.html.]Accessed: 30-Oct-2017[.

]77[K. Palmer, “TalkTalk slashes bonuses as cyber attack weighs on profits,” The Telegraph,20-Jun-2016.]Online[. Available: http://www.telegraph.co.uk/business/2016/06/20/talktalkslashes-bonuses-as-cyber-attack-weighs-on-profits/.]Accessed: 30-Oct-2017[.

]78[Gist.)2017(. 8x Nvidia GTX 1080 Hashcat Benchmarks.]online[Available at: https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40]Accessed 31 Jul. 2017[.

]79[reddit.)2017(. John The Ripper vs oclHashcat-lite • r/crypto.]online[Available at: https://www.reddit.com/r/crypto/comments/yuqyi/john_the_ripper_vs_oclhashcatlite/]Accessed 31 Jul. 2017[.

]80[Hashcat.net.)2017(. statsprocessor v0.07.]online[Available at: https://hashcat.net/forum/thread-1291.html]Accessed 31 Jul. 2017[.

]81["hashcat/hashcat", GitHub, 2017.]Online[. Available: https://github.com/hashcat/hashcat/releases.]Accessed: 31- Jul- 2017[(

]82["hashcat v3.6.0", Hashcat.net, 2017.]Online[. Available: https://hashcat.net/forum/thread- 6630.html.]Accessed: 31- Jul- 2017[(

]83[Dropbox, “dropbox/zxcvbn,” GitHub, 12-Oct-2017.]Online[. Available: https://github.com/dropbox/zxcvbn.]Accessed: 30-Oct-2017[.

]84[“zxcvbn: realistic password strength estimation,” Dropbox Tech Blog, 10-Apr-2012.]Online[. Available: https://blogs.dropbox.com/tech/2012/04/zxcvbn-realistic- passwordstrength-estimation/.]Accessed: 30-Oct-2017[.

]85[Ormrod, Jeanne Ellis, Essentials of Educational Psychology, page 27,)Pearson Education Inc., 2009(

]86[J. Blocki, S. Komanduri, L. Cranor, and A. Datta, “Spaced Repetition and Mnemonics Enable Recall of Multiple Strong Passwords,” Proceedings 2015 Network and Distributed System Security Symposium, 2015.

]87[D. P. Ausubel and M. Youssef, “The Effect of Spaced Repetition on Meaningful Retention,” The Journal of General Psychology, vol. 73, no. 1, pp. 147–150, 1965.

]88[E. Chukharev-Hudilainen and T. A. Klepikova, “The effectiveness of computer-based spaced repetition in foreign language vocabulary instruction: a double-blind study,” CALICO Journal, 2014.

]89[M. S. Shum, “The role of temporal landmarks in autobiographical memory processes.,” Psychol. Bull., vol. 124, no. 3, pp. 423–442, 1998.

]90[S10(W.Melicher, B. Ur, S. M. Segreti, S. Komanduri, L. B., N. Christin, L. F. Cranor, "Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks", 25th usenix Security Symposium, pp. 463 - 481, 2016.

]91[D. L. Wheeler, “zxcvbn: Low-Budget Password Strength Estimation.,” in USENIX Security Symposium, 2016, pp. 157–173.

]92[M. Dell' Amico, P. Michiardi and Y. Roudier, "Password Strength: An Empirical Analysis", 2010 Proceedings IEEE INFOCOM, 2010.

]93[X. de Carné de Carnavalet and M. Mannan, “From Very Weak to Very Strong: Analyzing Password-Strength Meters.,” in NDSS, 2014.

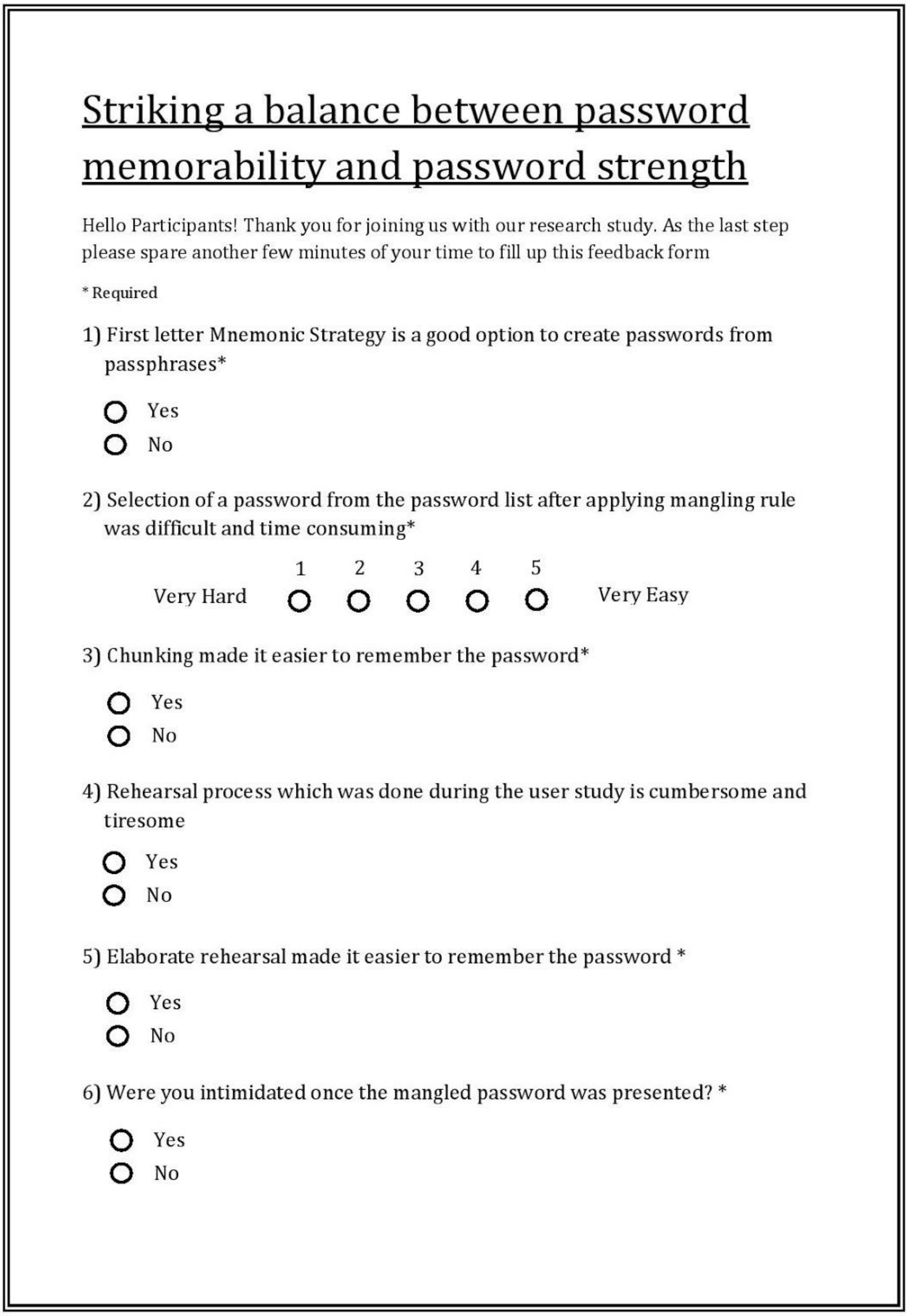
]94[P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez, “Guess Again)and Again and Again(: Measuring Password Strength by Simulating Password-Cracking Algorithms,” 2011.

]95[M. Dellamico and M. Filippone, “Monte Carlo Strength Evaluation,” Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS 15, 2015.

Appendices

Appendix A

Online feedback form which was given to participants of the user study



Striking a balance between password memorability and password strength

Hello Participants! Thank you for joining us with our research study. As the last step please spare another few minutes of your time to fill up this feedback form

* Required

1) First letter Mnemonic Strategy is a good option to create passwords from passphrases*

○ Yes
○ No

2) Selection of a password from the password list after applying mangling rule was difficult and time consuming*

	1	2	3	4	5	
Very Hard	○	○	○	○	○	Very Easy

3) Chunking made it easier to remember the password*

○ Yes
○ No

4) Rehearsal process which was done during the user study is cumbersome and tiresome

○ Yes
○ No

5) Elaborate rehearsal made it easier to remember the password *

○ Yes
○ No

6) Were you intimidated once the mangled password was presented? *

○ Yes
○ No

7) How comfortable are you with the password after the rehearsal process? *

Extremely uncomfortable	1	2	3	4	5	Extremely comfortable
	○	○	○	○	○	

8) GUI of the system made the password creation process easy *

○ Yes

○ No

○ Maybe

9) Feedback or Suggestions on the overall process

Iteration 02

10) How difficult was it to select a phrase?

	1	2	3	4	5	
Very Hard	○	○	○	○	○	Very Easy

11) How easy was it to remember the system generated phrase which used Facebook Data?

	1	2	3	4	5	
Very Hard	○	○	○	○	○	Very Easy

12) How comfortable was the wording of the generated phrase

Extremely uncomfortable	1	2	3	4	5	Extremely comfortable
	○	○	○	○	○	

Iteration 03

13) How comfortable was the password created from the photo?

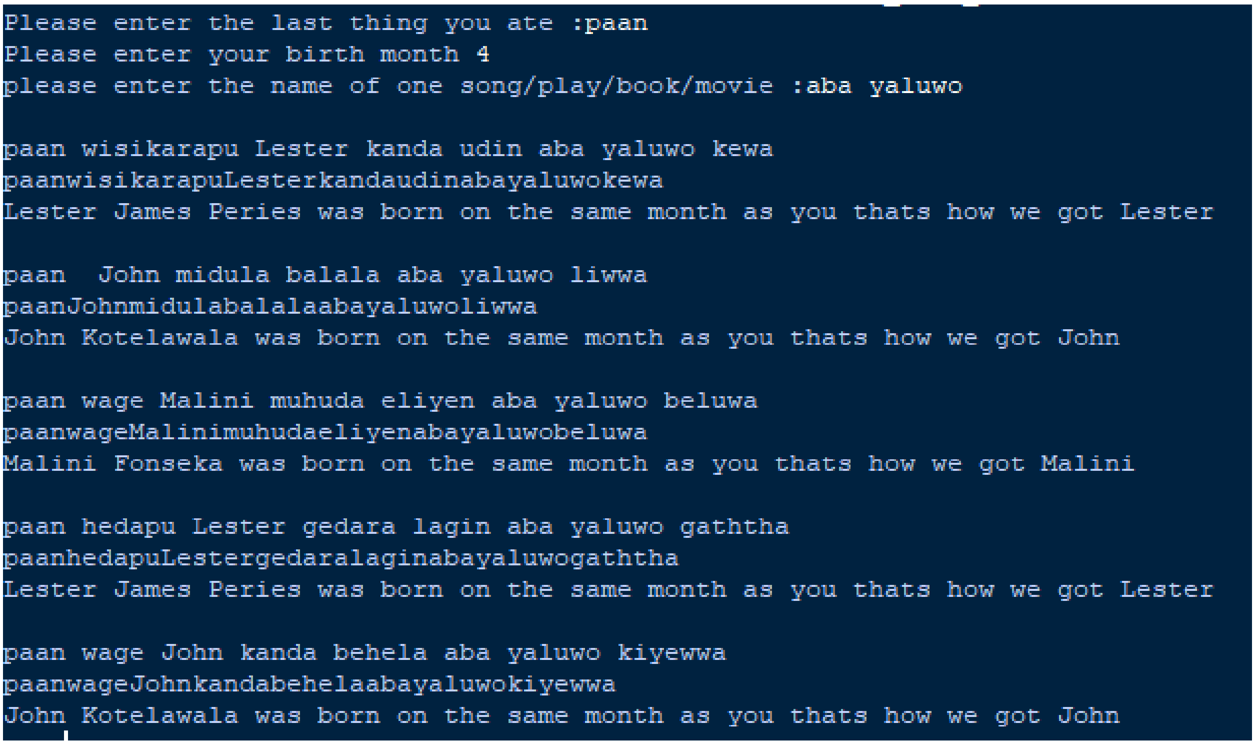
Extremely	1	2	3	4	5	Extremely
uncomfortable	○	○	○	○	○	comfortable

14) How easy was it to create your own phrase using the photo?

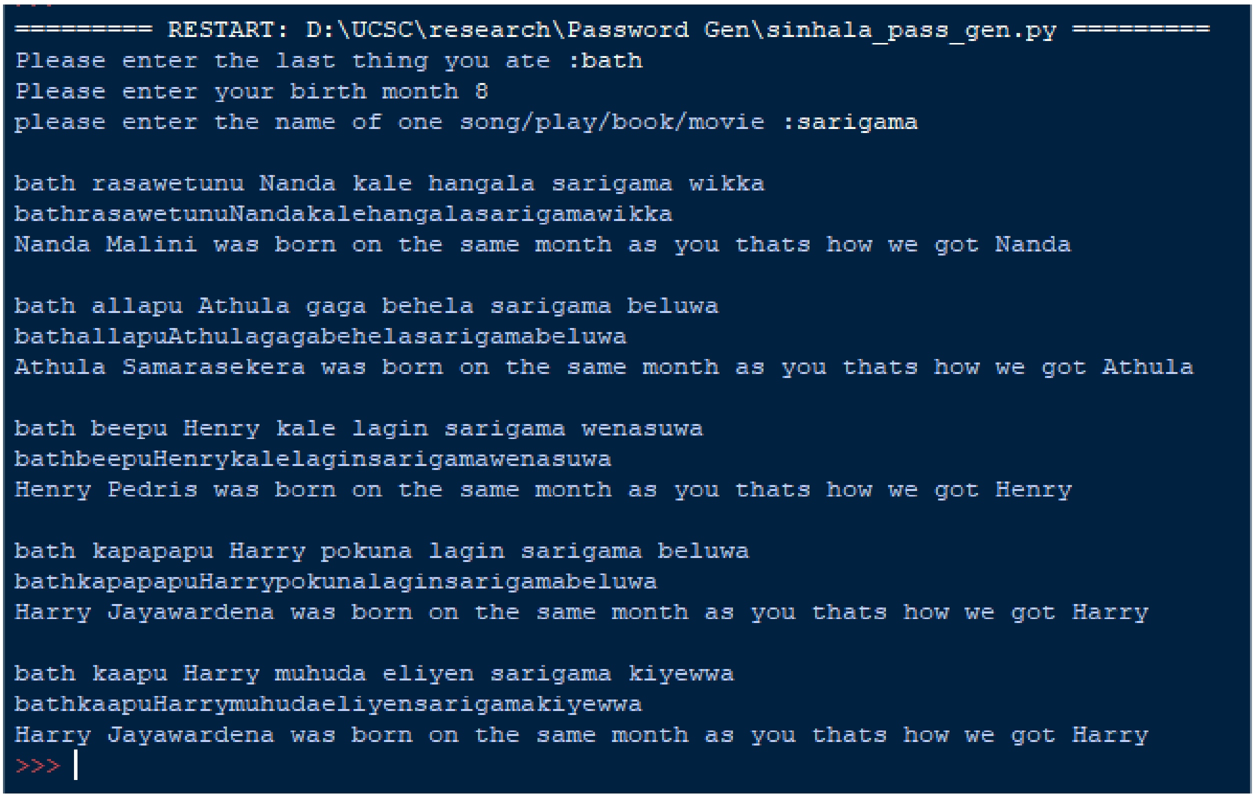
	1	2	3	4	5	
Very Hard	○	○	○	○	○	Very Easy

Appendix B:

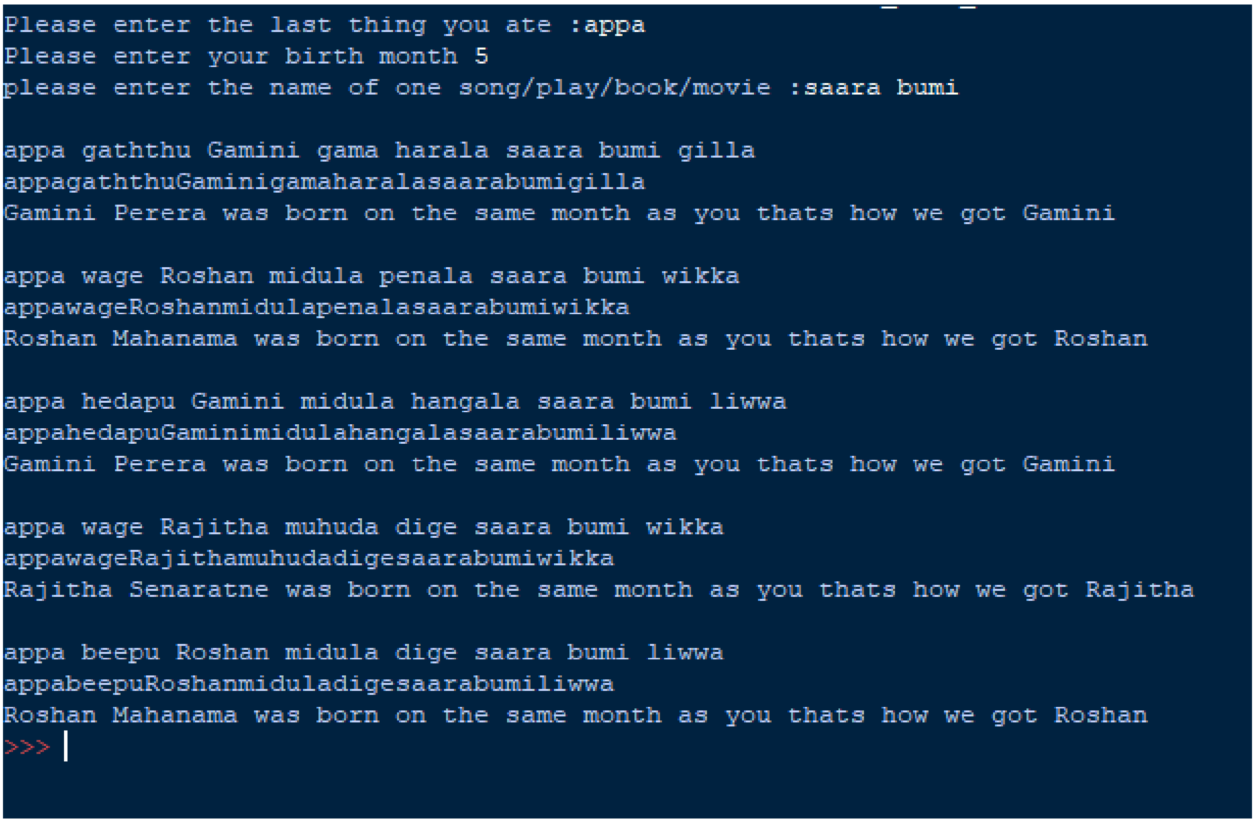
Detailed output created from the system for each participant in IT1-PG



```
Please enter the last thing you ate :paan
Please enter your birth month 4
please enter the name of one song/play/book/movie :aba yaluwo

paan wisikarapu Lester kanda udin aba yaluwo kewa
paanwisikarapuLesterkandaudinabayaluwokewa
Lester James Peries was born on the same month as you thats how we got Lester

paan  John midula balala aba yaluwo liwwa
paanJohnmidulabalalaabayaluwoliwwa
John Kotelawala was born on the same month as you thats how we got John

paan wage Malini muhuda eliyen aba yaluwo beluwa
paanwageMalinimuhudaeliyenabayaluwobeluwa
Malini Fonseka was born on the same month as you thats how we got Malini

paan hedapu Lester gedara lagin aba yaluwo gaththa
paanhedapuLestergedaralaginabayaluwogaththa
Lester James Peries was born on the same month as you thats how we got Lester

paan wage John kanda behela aba yaluwo kiyewwa
paanwageJohnkandabehelaabayaluwokiyewwa
John Kotelawala was born on the same month as you thats how we got John
```



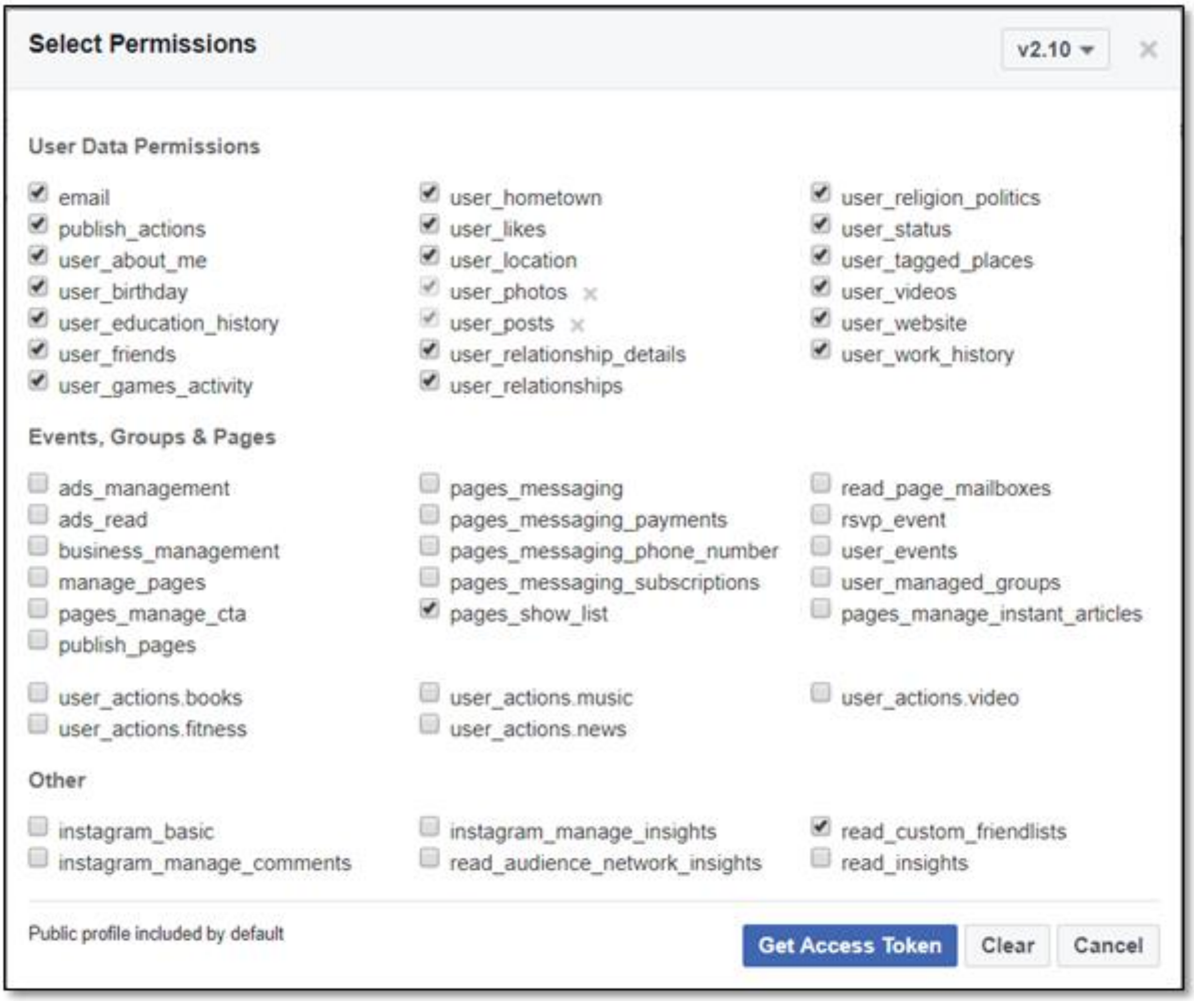
```
========= RESTART: D:\UCSC\research\Password Gen\sinhala_pass_gen.py =========
Please enter the last thing you ate :bath
Please enter your birth month 8
please enter the name of one song/play/book/movie :sarigama

bath rasawetunu Nanda kale hangala sarigama wikka
bathrasawetunuNandakalehangalasarigamawikka
Nanda Malini was born on the same month as you thats how we got Nanda

bath allapu Athula gaga behela sarigama beluwa
bathallapuAthulagagabehelasarigamabeluwa
Athula Samarasekera was born on the same month as you thats how we got Athula

bath beepu Henry kale lagin sarigama wenasuwa
bathbeepuHenrykalelaginsarigamawenasuwa
Henry Pedris was born on the same month as you thats how we got Henry

bath kapapapu Harry pokuna lagin sarigama beluwa
bathkapapapuHarrypokunalaginsarigamabeluwa
Harry Jayawardena was born on the same month as you thats how we got Harry

bath kaapu Harry muhuda eliyen sarigama kiyewwa
bathkaapuHarrymuhudaeliyensarigamakiyewwa
Harry Jayawardena was born on the same month as you thats how we got Harry
>>>
```



```
Please enter the last thing you ate :appa
Please enter your birth month 5
please enter the name of one song/play/book/movie :saara bumi

appa gaththu Gamini gama harala saara bumi gilla
appagaththuGaminigamaharalasaarabumigilla
Gamini Perera was born on the same month as you thats how we got Gamini

appa wage Roshan midula penala saara bumi wikka
appawageRoshanmidulapenalasaarabumiwikka
Roshan Mahanama was born on the same month as you thats how we got Roshan

appa hedapu Gamini midula hangala saara bumi liwwa
appahedapuGaminimidulahangalasaarabumiliwwa
Gamini Perera was born on the same month as you thats how we got Gamini

appa wage Rajitha muhuda dige saara bumi wikka
appawageRajithamuhudadigesaarabumiwikka
Rajitha Senaratne was born on the same month as you thats how we got Rajitha

appa beepu Roshan midula dige saara bumi liwwa
appabeepuRoshanmiduladigesaarabumiliwwa
Roshan Mahanama was born on the same month as you thats how we got Roshan
>>> 
```

Appendix C:

Permissions to generate the access token



User Data Permissions

☑ email
☑ publish_actions
☑ user_about_me
☑ user_birthday
☑ user_education_history
☑ user_friends
☑ user_games_activity
☑ user_hometown
☑ user_likes
☑ user_location
☑ user_photos ×
☑ user_posts ×
☑ user_relationship_details
☑ user_relationships
☑ user_religion_politics
☑ user_status
☑ user_tagged_places
☑ user_videos
☑ user_website
☑ user_work_history

Events, Groups & Pages

□ ads_management
□ ads_read
□ business_management
□ manage_pages
□ pages_manage_cta
□ publish_pages
□ pages_messaging
□ pages_messaging_payments
□ pages_messaging_phone_number
□ pages_messaging_subscriptions
☑ pages_show_list
□ read_page_mailboxes
□ rsvp_event
□ user_events
□ user_managed_groups
□ pages_manage_instant_articles

□ user_actions.books
□ user_actions.fitness
□ user_actions.music
□ user_actions.news
□ user_actions.video

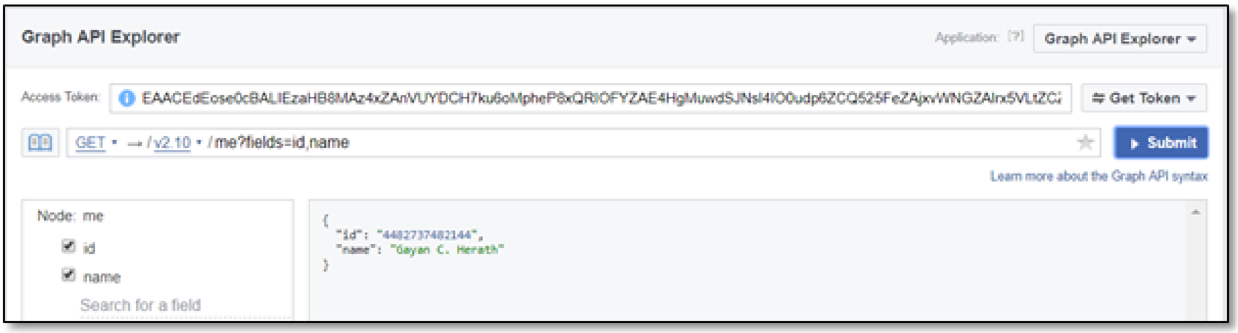
Other

□ instagram_basic
□ instagram_manage_comments
□ instagram_manage_insights
□ read_audience_network_insights
☑ read_custom_friendlists
□ read_insights

Public profile included by default

Appendix D:

Generated Access Token, Facebook Name and its ID



Access Token: EAACEdEose0cBALIEzaHB8MAz4xZAnVUYDCH7ku6oMpheP8xQRIOFYZAE4HgMuwdSJNsl4IO0udp6ZCQ525FeZAjxvWNGZAlrx5VLtZC

GET → /v2.10 /me?fields=id,name

Node: me

☑ id

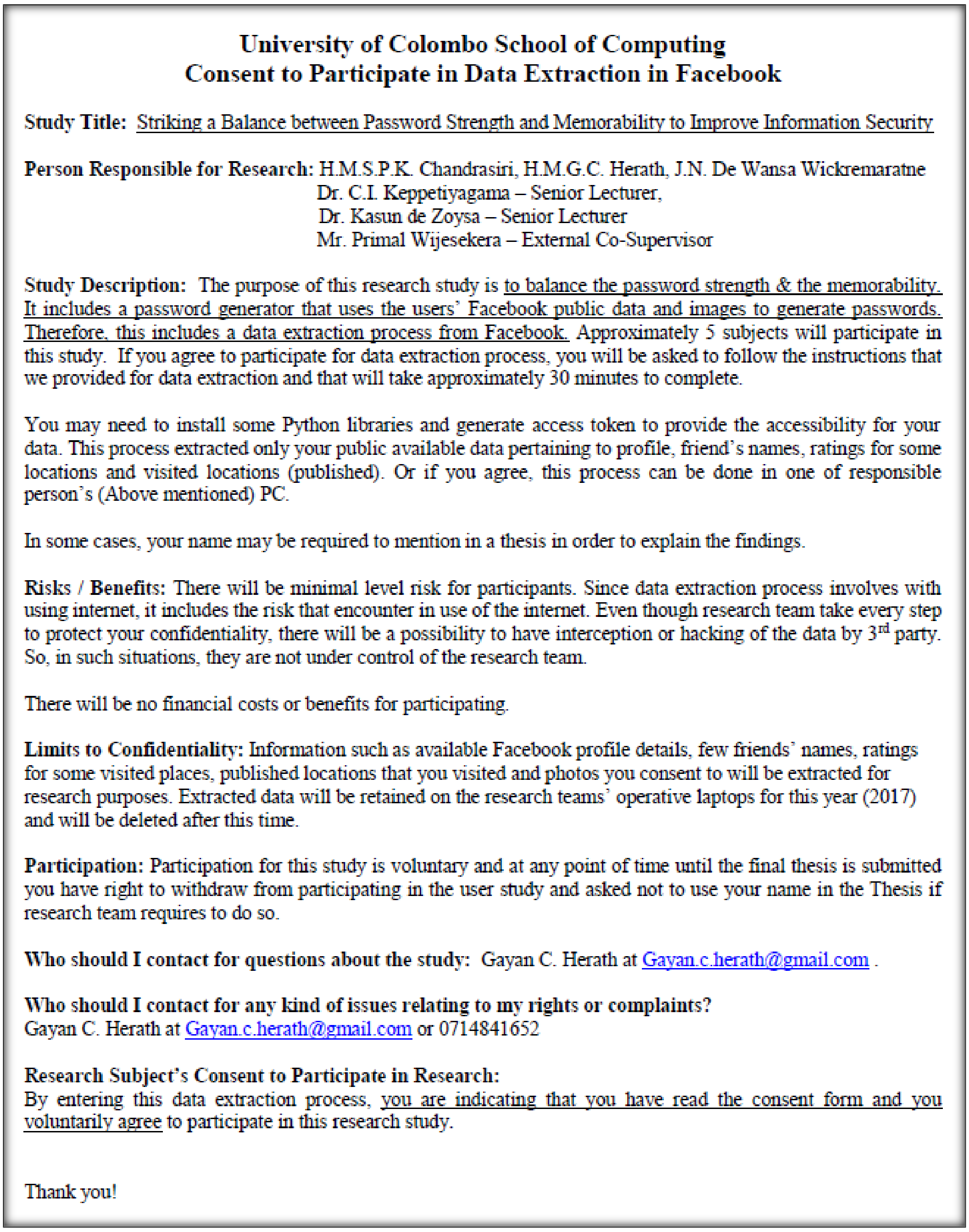
☑ name

Search for a field

```
{
  "id": "4482737482144",
  "name": "Gayan C. Herath"
}
```

Appendix E:

Consent form which is sent to participant



University of Colombo School of Computing
Consent to Participate in Data Extraction in Facebook

Study Title: Striking a Balance between Password Strength and Memorability to Improve Information Security

Person Responsible for Research: H.M.S.P.K. Chandrasiri, H.M.G.C. Herath, J.N. De Wansa Wickremaratne
Dr. C.I. Keppetiyagama – Senior Lecturer,
Dr. Kasun de Zoysa – Senior Lecturer
Mr. Primal Wijesekera – External Co-Supervisor

Study Description: The purpose of this research study is to balance the password strength & the memorability. It includes a password generator that uses the users' Facebook public data and images to generate passwords. Therefore, this includes a data extraction process from Facebook. Approximately 5 subjects will participate in this study. If you agree to participate for data extraction process, you will be asked to follow the instructions that we provided for data extraction and that will take approximately 30 minutes to complete.

You may need to install some Python libraries and generate access token to provide the accessibility for your data. This process extracted only your public available data pertaining to profile, friend's names, ratings for some locations and visited locations (published). Or if you agree, this process can be done in one of responsible person's (Above mentioned) PC.

In some cases, your name may be required to mention in a thesis in order to explain the findings.

Risks / Benefits: There will be minimal level risk for participants. Since data extraction process involves with using internet, it includes the risk that encounter in use of the internet. Even though research team take every step to protect your confidentiality, there will be a possibility to have interception or hacking of the data by 3rd party. So, in such situations, they are not under control of the research team.

There will be no financial costs or benefits for participating.

Limits to Confidentiality: Information such as available Facebook profile details, few friends' names, ratings for some visited places, published locations that you visited and photos you consent to will be extracted for research purposes. Extracted data will be retained on the research teams' operative laptops for this year (2017) and will be deleted after this time.

Participation: Participation for this study is voluntary and at any point of time until the final thesis is submitted you have right to withdraw from participating in the user study and asked not to use your name in the Thesis if research team requires to do so.

Who should I contact for questions about the study: Gayan C. Herath at Gayan.c.herath@gmail.com .

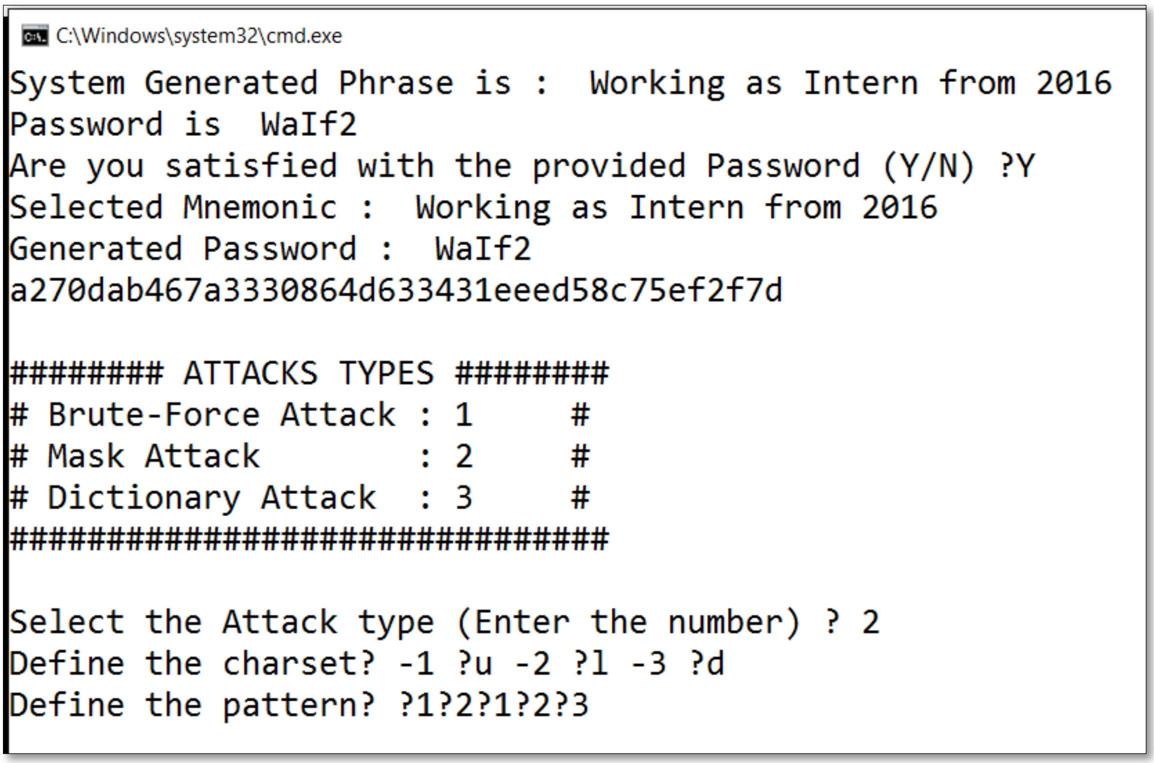
Who should I contact for any kind of issues relating to my rights or complaints?
Gayan C. Herath at Gayan.c.herath@gmail.com or 0714841652

Research Subject's Consent to Participate in Research:
By entering this data extraction process, you are indicating that you have read the consent form and you voluntarily agree to participate in this research study.

Thank you!

Appendix F:

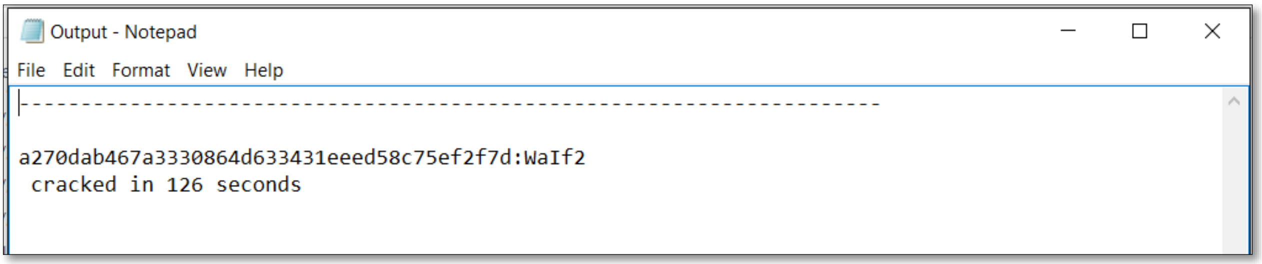
Selecting Masks Attacks for “WaIf2” Password. In here 1 is referred for uppercase, 2 is referred for lowercase characters and 3 is referred for digits. Based on these references, pattern is defined.



```
System Generated Phrase is :  Working as Intern from 2016
Password is  WaIf2
Are you satisfied with the provided Password (Y/N) ?Y
Selected Mnemonic :  Working as Intern from 2016
Generated Password :  WaIf2
a270dab467a3330864d633431eeed58c75ef2f7d

######## ATTACKS TYPES ########
# Brute-Force Attack : 1     #
# Mask Attack        : 2     #
# Dictionary Attack  : 3     #
###############################

Select the Attack type (Enter the number) ? 2
Define the charset? -1 ?u -2 ?l -3 ?d
Define the pattern? ?1?2?1?2?3
```

Appendix G:

Text File that saved the status of cracked password



```
|----------------------------------------------------------------------

a270dab467a3330864d633431eeed58c75ef2f7d:WaIf2
 cracked in 126 seconds
```

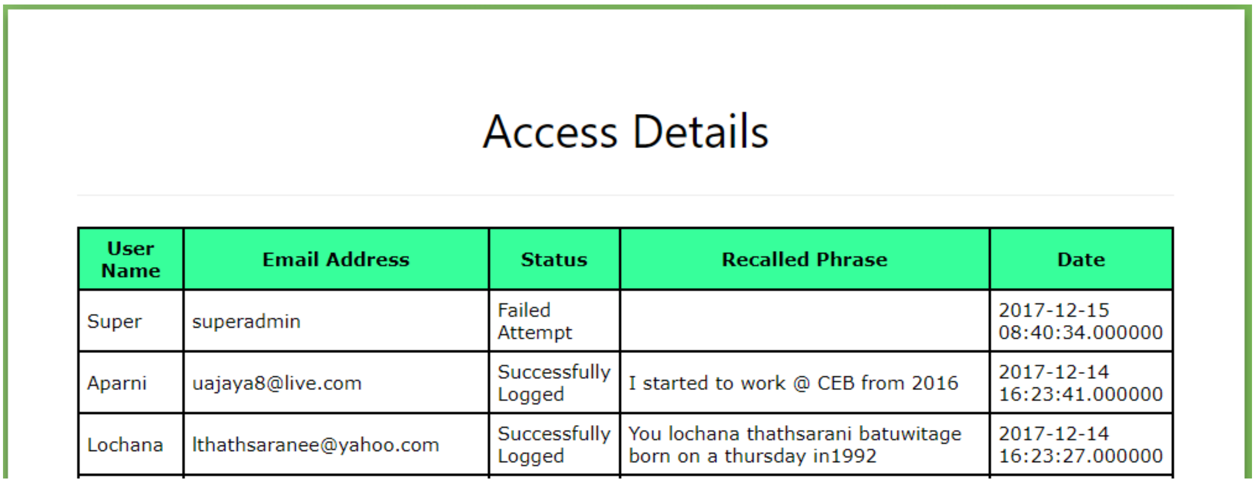
Appendix H:

Cutoff values which represents the strength of the passwords.

Bits	**Strength**
0-64	Very Weak
64-80	Weak
80-112	Moderate
112-128	Strong
>= 128	Very Strong

Appendix I:

Access Log for each users' login that represents the successful sign in and failed attempts

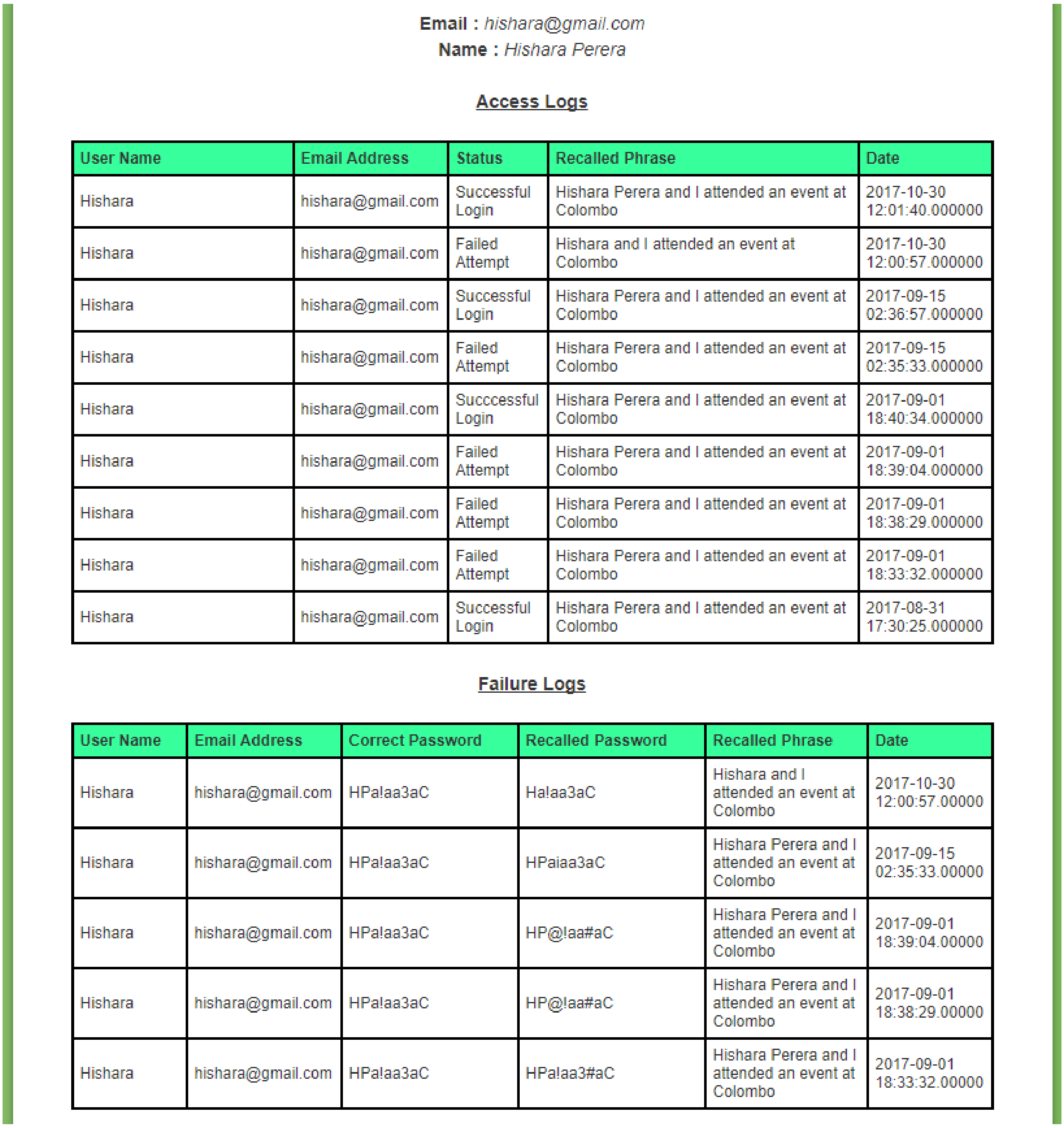


Access Details

User Name	Email Address	Status	Recalled Phrase	Date
Super	superadmin	Failed Attempt		2017-12-15 08:40:34.000000
Aparni	uajaya8@live.com	Successfully Logged	I started to work @ CEB from 2016	2017-12-14 16:23:41.000000
Lochana	lthathsaranee@yahoo.com	Successfully Logged	You lochana thathsarani batuwitage born on a thursday in1992	2017-12-14 16:23:27.000000

Appendix J

Summary of individual users' sign in details that shows access logs and failed logs for one participant. These details can be queried by searching user from their email address



Email : *hishara@gmail.com*
Name : *Hishara Perera*

Access Logs

User Name	Email Address	Status	Recalled Phrase	Date
Hishara	hishara@gmail.com	Successful Login	Hishara Perera and I attended an event at Colombo	2017-10-30 12:01:40.000000
Hishara	hishara@gmail.com	Failed Attempt	Hishara and I attended an event at Colombo	2017-10-30 12:00:57.000000
Hishara	hishara@gmail.com	Successful Login	Hishara Perera and I attended an event at Colombo	2017-09-15 02:36:57.000000
Hishara	hishara@gmail.com	Failed Attempt	Hishara Perera and I attended an event at Colombo	2017-09-15 02:35:33.000000
Hishara	hishara@gmail.com	Succcessful Login	Hishara Perera and I attended an event at Colombo	2017-09-01 18:40:34.000000
Hishara	hishara@gmail.com	Failed Attempt	Hishara Perera and I attended an event at Colombo	2017-09-01 18:39:04.000000
Hishara	hishara@gmail.com	Failed Attempt	Hishara Perera and I attended an event at Colombo	2017-09-01 18:38:29.000000
Hishara	hishara@gmail.com	Failed Attempt	Hishara Perera and I attended an event at Colombo	2017-09-01 18:33:32.000000
Hishara	hishara@gmail.com	Successful Login	Hishara Perera and I attended an event at Colombo	2017-08-31 17:30:25.000000

Failure Logs

User Name	Email Address	Correct Password	Recalled Password	Recalled Phrase	Date
Hishara	hishara@gmail.com	HPa!aa3aC	Ha!aa3aC	Hishara and I attended an event at Colombo	2017-10-30 12:00:57.00000
Hishara	hishara@gmail.com	HPa!aa3aC	HPaiaa3aC	Hishara Perera and I attended an event at Colombo	2017-09-15 02:35:33.00000
Hishara	hishara@gmail.com	HPa!aa3aC	HP@!aa#aC	Hishara Perera and I attended an event at Colombo	2017-09-01 18:39:04.00000
Hishara	hishara@gmail.com	HPa!aa3aC	HP@!aa#aC	Hishara Perera and I attended an event at Colombo	2017-09-01 18:38:29.00000
Hishara	hishara@gmail.com	HPa!aa3aC	HPa!aa3#aC	Hishara Perera and I attended an event at Colombo	2017-09-01 18:33:32.00000

Appendix K

Results from the password Generator for Iteration 02

<table>
<tr><th colspan="2">Participant 01</th></tr>
<tr><td>Templates created</td><td>You Nathaliya Jayawardena born in 1993.
You Nathaliya Jayawardena born on a Monday in 1993.
AIESEC in University of Colombo - Srilanka is one of my working place
I started to work @ AIESEC in University of Colombo - Srilanka from 2015
I started 2 work at AIESEC in University of Colombo - Srilanka as Vice President Finance
Working as Intern from 2015
I went to University of Colombo School of Computing and it is my High School
I have 1193 friends and Hiran Eranda Weerasinghe is one of them
I have Hiran Eranda Weerasinghe and Sachini Chathurika as friends on FB
I have visited New Arts Theatre - University of Colombo and University of Colombo recently
I rated New Arts Theatre - University of Colombo as a best place to visit
Pasan Ranathunga and I attended an event at Kithul Kanda - The Mountain Resort
Kasun Jay has liked 1 Picture of mine @ Kithul Kanda - The Mountain Resort
Information phrase selected by the candidate: “You Nathaliya Jayawardena born on a Monday in 1993”</td></tr>
<tr><td>Phrase Chosen</td><td>You Nathaliya Jayawardena born on a Monday in 1993</td></tr>
<tr><td>First letter mnemonic</td><td>YNJboaMi1</td></tr>
<tr><td>Candidate passwords generated with mangling rules</td><td>'YNJbo@Mi1', 'YNJboaM!1', 'Ynjbo@mi1', 'Ynjboam!1', 'YNJ8o@Mi1', 'YNJbo@M11', 'YNJbo@M!1', 'YNJbo4M!1', 'YNJbo@M|1', 'YNJb0@Mi1', 'YNJbo4Mi!', 'Ynj8o@mi1', 'Ynjbo@m11', 'Ynjbo@m!1', 'Ynjbo4m!1', 'Ynjbo@m|1', 'Ynjb0@mi1', 'Ynjbo4mi!', 'YNJ8o@Mi1', 'YNJ8oaM!1', 'YNJ8oaMi!', 'Ynj8o@mi1', 'Ynj8oam!1', 'Ynj8oami!', 'YNJbo@M11', 'YNJbo@M!1', 'YNJbo@M|1', 'YNJbo4M!1', 'YNJ8oaM!1', 'YNJb0aM!1', 'Ynjbo@m11', 'Ynjbo@m!1', 'Ynjbo@m|1', 'Ynjbo4m!1', 'Ynj8oam!1', 'Ynjb0am!1', 'YNJb0@Mi1', 'YNJb0aM!1', 'YNJb0aMi!', 'Ynjb0@mi1', 'Ynjb0am!1', 'Ynjb0ami!', 'YNJbo4Mi!', 'YNJ8oaMi!', 'YNJboaM1!', 'YNJb0aMi!', 'Ynjbo4mi!', 'Ynj8oami!', 'Ynjboam1!', 'Ynjb0ami!'</td></tr>
<tr><td>Password Chosen</td><td>Ynjbo@m!1</td></tr>
</table>

Participant 02	
Templates created	You Hishara Perera born in 1992 You Hishara Perera born on a Wednesday in 1992 Facebook is one of my working place I started to work @ Facebook from 0000 Working as Intern from 0000 I went to St. Peter's College Colombo and it is my College I have 1184 friends and Ashan Maduranga is one of them I have Ashan Maduranga and Thushara Dahanayake as friends on FB I have visited University of Colombo School of Computing and New Arts Theatre - University of Colombo recently I rated University of Colombo School of Computing as best a place to visit Hishara Perera and I attended an event at Colombo Lahiru Nirmal has liked 1 Picture of mine @ Colombo Information phrase selected by the candidate: “Hishara Perera and I attended an event at Colombo”
Phrase Chosen	Hishara Perera and I attended an event at Colombo
First letter mnemonic	HPaIaaeaC
Candidate passwords generated with mangling rules	'HP@1@@e@C', 'HP4!44e4C', 'Hp@i@@3@c', 'Hp@1@@e@c', 'Hp4!44e4c', 'HPa!aa3aC', 'Hp@i@@3@c', 'Hpa!aa3ac', 'HP@1@@e@C', 'HP4!44e4C', 'HPa!aa3aC', 'Hp@1@@e@c', 'Hp4!44e4c', 'Hpa!aa3ac'
Password Chosen	HPa!aa3aC

<table>
<tr><th colspan="2">Participant 03</th></tr>
<tr><td>Templates created</td><td>You Himashi Sandamini born in 1993
You Himashi Sandamini born on a Monday in 1993
UCSC Mozilla Club is one of my working place
I started to work @ UCSC Mozilla Club from 0000
I started 2 work at UCSC Mozilla Club as Core Team Member
Working as Intern from 0000
I went to Sujatha Vidyalaya and it is my High School
I have 615 friends and Sulakshi Chandrasiri is one of them
I have Sulakshi Chandrasiri and Hiran Eranda Weerasinghe as friends on FB
I have visited University of Colombo School of Computing and New Arts Theatre - University of Colombo recently
I rated University of Colombo School of Computing as worst a place to visit
Nipuni Jayalath and I attended an event at Bandaranaike Memorial International Conference Hall
Anjana Silva has liked 1 Picture of mine @ Bandaranaike Memorial International Conference Hall</td></tr>
<tr><td>Phrase Chosen</td><td>I started to work @ UCSC Mozilla Club from 0000</td></tr>
<tr><td>First letter mnemonic</td><td>Istw@UMCf0</td></tr>
<tr><td>Candidate passwords generated with mangling rules</td><td>'1stw@UMCf0', '!stw@UMCf0', '|stw@UMCf0', 'I$tw@UMCf0', 'I5tw@UMCf0', 'Is+w@UMCf0', 'I$tw@umcf0', 'I5tw@umcf0', 'Is+w@umcf0', '1$tw@UMCf0', '!$tw@UMCf0', '|$tw@UMCf0', '15tw@UMCf0', '!5tw@UMCf0', '|5tw@UMCf0', '1s+w@UMCf0', '!s+w@UMCf0', '|s+w@UMCf0', '1stw@UMCfo', '1stw@UMCfO', '1$tw@UMCf0', '15tw@UMCf0', '!$tw@UMCf0', '!5tw@UMCf0', '|$tw@UMCf0', '|5tw@UMCf0', 'I$+w@UMCf0', 'I5+w@UMCf0', 'I5tw@UMCfo', 'I5tw@UMCfO', 'I$+w@umcf0', 'I5+w@umcf0', 'I5tw@umcfo', 'I5tw@umcfo', '1s+w@UMCf0', '!s+w@UMCf0', '|s+w@UMCf0', 'I$+w@UMCf0', 'I5+w@UMCf0', 'I$+w@umcf0', 'I5+w@umcf0', '1stw@UMCfo', '1stw@UMCfO', 'I5tw@UMCfo', 'I5tw@UMCfO', 'I5tw@umcfo'</td></tr>
<tr><td>Password Chosen</td><td>I$tw@UMCf0</td></tr>
</table>

Participant 04	
Templates created	You Lochana Thathsarani Batuwitage born in 1992 You Lochana Thathsarani Batuwitage born on a Thursday in 1992 I went to Prajapathi Balika Vidyalaya and it is my High School I have 655 friends and Dilini Madhubhashini is one of them I have Dilini Madhubhashini and Chathura Ranaweera as friends on FB I have visited University of Colombo and Faculty of Agriculture - Rajarata University of Sri Lanka recently I rated University of Colombo as best a place to visit NC Dikwella and I attended an event at Faculty of Agriculture - Rajarata University of Sri Lanka Lochana Thathsarani Batuwitage has liked 1 Picture of mine @ Faculty of Agriculture - Rajarata University of Sri Lanka
Phrase Chosen	You Lochana Thathsarani Batuwitage born on a Thursday in 1992
First letter mnemonic	YLTBboaTi1
Candidate passwords generated with mangling rules	'YLTBbo@Ti1', 'YLTBboaT!1', 'Yltbbo@ti1', 'Yltbboat!1', 'Y!TBboaTi1', 'Y!tbboati1', 'YLTB8o@Ti1', 'YLT8bo@Ti1', 'YLTBbo@T11', 'YLTBbo@T!1', 'YLTBbo4T!1', 'YLTBbo@T|1', 'Y1TBbo@Ti1', 'Y7TBbo@Ti1', 'Y|TBbo@Ti1', 'Y!TBbo@Ti1', 'Y!TBbo4Ti1', 'YLTBb0@Ti1', 'YL+Bbo@+i1', 'YLTBbo4Ti!', 'Yltb8o@ti1', 'Ylt8bo@ti1', 'Yltbbo@t11', 'Yltbbo@t!1', 'Yltbbo4t!1', 'Yltbbo@t|1', 'Y1tbbo@ti1', 'Y7tbbo@ti1', 'Y|tbbo@ti1', 'Y!tbbo@ti1', 'Y!tbbo4ti1', 'Yltbb0@ti1', 'Yl+bbo@+i1', 'Yltbbo4ti!', 'YLTB8o@Ti1', 'YLTB8oaT!1', 'Y!TB8oaTi1', 'YLTB8oaTi!', 'Yltb8o@ti1', 'Yltb8oat!1', 'Y!tb8oati1', 'Yltb8oati!', 'YLT8bo@Ti1', 'YLT8boaT!1', 'Y!T8boaTi1', 'YLT8boaTi!', 'Ylt8bo@ti1', 'Ylt8boat!1', 'Y!t8boati1', 'Ylt8boati!', 'YLTBbo@T11', 'YLTBbo@T!1', 'YLTBbo@T|1', 'YLTBbo4T!1', 'YLTB8oaT!1', 'YLT8boaT!1', 'Y1TBboaT!1', 'Y7TBboaT!1', 'Y|TBboaT!1', 'Y!TBboaT11', 'Y!TBboaT!1', 'Y!TBboaT|1', 'YLTBb0aT!1', 'YL+Bboa+!1', 'Yltbbo@t11', 'Yltbbo@t!1', 'Yltbbo@t|1', 'Yltbbo4t!1', 'Yltb8oat!1', 'Ylt8boat!1', 'Y1tbboat!1', 'Y7tbboat!1', 'Y|tbboat!1', 'Y!tbboat11', 'Y!tbboat!1', 'Y!tbboat|1', 'Yltbb0at!1', 'Yl+bboa+!1', 'YLTBbo@Ti1', 'Yltbbo@ti1', 'YLTBb0@Ti1', 'YLTBb0aT!1', 'Y!TBb0aTi1', 'YLTBb0aTi!', 'Yltbb0@ti1', 'Yltbb0at!1', 'Y!tbb0ati1', 'Yltbb0ati!', 'YL+Bbo@+i1', 'YL+Bboa+!1', 'Y!+Bboa+i1', 'Yl+bbo@+i1', 'Yl+bboa+!1', 'Y!+bboa+i1', 'YLTBbo4Ti!', 'YLTB8oaTi!', 'YLT8boaTi!', 'YLTBboaT1!', 'Y1TBboaTi!', 'Y7TBboaTi!', 'YLTBb0aTi!', 'Yltbbo4ti!', 'Yltb8oati!', 'Ylt8boati!', 'Yltbboat1!', 'Y1tbboati!', 'Y7tbboati!', 'Yltbb0ati!'
Password Chosen	Yltbbo4ti!

<table>
<tr><th colspan="2">Participant 05</th></tr>
<tr><td>Templates created</td><td>You Aparni Jayawardena born in 1992
You Aparni Jayawardena born on a Tuesday in 1992
Ceylon Electricity Board is one of my working place
I started to work @ Ceylon Electricity Board from 2016
I started 2 work at Ceylon Electricity Board as Business Analyst Trainee - Internship
Working as Intern from 2016
I went to Yasodara Devi Balika Maha Vidyalaya and it is my High School
I have 520 friends and Gayan C. Herath is one of them
I have Gayan C. Herath and Himashi Sandamini as friends on FB
I have visited Anuradhapura and Seethawaka Botanical Garden - Wet Zone recently
I rated Anuradhapura as best a place to visit
Chamindi Anupa Wimaladharma and I attended an event at Ihalayagoda
Madhu Somarathne has liked 1 Picture of mine @ Ihalayagoda</td></tr>
<tr><td>Phrase Chosen</td><td>I started to work @ Ceylon Electricity Board from 2016</td></tr>
<tr><td>First letter mnemonic</td><td>Istw@CEBf2</td></tr>
<tr><td>Candidate passwords generated with mangling rules</td><td>'Istw@CE8f2', 'Istw@C3Bf2', '1stw@CEBf2', '!stw@CEBf2', '|stw@CEBf2', 'Istw@ce8f2', 'Istw@c3bf2', 'I$tw@CEBf2', 'I5tw@CEBf2', 'Is+w@CEBf2', 'I$tw@cebf2', 'I5tw@cebf2', 'Is+w@cebf2', 'Istw@C37f2', '1stw@CE8f2', '!stw@CE8f2', '|stw@CE8f2', 'I$tw@CE8f2', 'I5tw@CE8f2', 'Is+w@CE8f2', 'Istw@c37f2', 'I$tw@ce8f2', 'I5tw@ce8f2', 'Is+w@ce8f2', 'Istw@C37f2', '1stw@C3Bf2', '!stw@C3Bf2', '|stw@C3Bf2', 'I$tw@C3Bf2', 'I5tw@C3Bf2', 'Is+w@C3Bf2', 'Istw@c37f2', 'I$tw@c3bf2', 'I5tw@c3bf2', 'Is+w@c3bf2', '1stw@CE8f2', '!stw@CE8f2', '|stw@CE8f2', '1stw@C3Bf2', '!stw@C3Bf2', '|stw@C3Bf2', '1$tw@CEBf2', '!$tw@CEBf2', '|$tw@CEBf2', '15tw@CEBf2', '!5tw@CEBf2', '|5tw@CEBf2', '1s+w@CEBf2', '!s+w@CEBf2', '|s+w@CEBf2', 'I$tw@CE8f2', 'I5tw@CE8f2', 'I$tw@C3Bf2', 'I5tw@C3Bf2', '1$tw@CEBf2', '15tw@CEBf2', '!$tw@CEBf2', '!5tw@CEBf2', '|$tw@CEBf2', '|5tw@CEBf2', 'I$+w@CEBf2', 'I5+w@CEBf2', 'I$tw@ce8f2', 'I5tw@ce8f2', 'I$tw@c3bf2', 'I5tw@c3bf2', 'I$+w@cebf2', 'I5+w@cebf2', 'Is+w@CE8f2', 'Is+w@C3Bf2', '1s+w@CEBf2', '!s+w@CEBf2', '|s+w@CEBf2', 'I$+w@CEBf2', 'I5+w@CEBf2', 'Is+w@ce8f2', 'Is+w@c3bf2', 'I$+w@cebf2', 'I5+w@cebf'</td></tr>
<tr><td>Password Chosen</td><td>Istw@c37f2</td></tr>
</table>

Appendix L

Results for the Memorability module for Iteration 02

		Participant 01		
Original password		Ynjbo@m!1		
Original Passphrase		You Nathaliya Jayawardena born on a Monday in 1993		
0 hrs (Initial Login)	Attempts	Attempt 01		
	Pasword inserted	Ynjbo@m!1		
	Phrase Used	You Nathaliya Jayawardena born on a Monday in 1993		
	Status	Successful Login		
24 hrs	Attempts	Attempt 01		
	Pasword inserted	Ynjbo@m!1		
	Phrase Used	You Nathaliya Jayawardena born on a Monday in 1993		
	Status	Successful Login		
15 days	Attempts	Attempt 01	Attempt 02	Attempt 03
	Pasword inserted	Ynjbm@!1	Ynjbo2!1	Ynjbo@m!1
	Phrase Used	You Nathaliya Jayawardena born on a Monday in 1993	You Nathaliya Jayawardena born on a Monday in 1993	You Nathaliya Jayawardena born on a Monday in 1993
	Status	Failed Attempt	Failed Attempt	Successful Login
45 days	Attempts	Attempt 01		
	Pasword inserted	Ynjbo@m!1		
	Phrase Used	You Nathaliya Jayawardena born on a Monday in 1993		

	Status	Successful Login

		Participant 02			
Original password		HPa!aa3aC			
Original Passphrase		Hishara Perera and I attended an event at Colombo			
0 hrs	Attempts	Attempt 01			
	Pasword inserted	HPa!aa3aC			
	Phrase Used	Hishara Perera and I attended an event at Colombo			
	Status	Successful Login			
24 hrs	Attempts	Attempt 01	Attempt 02	Attempt 03	Attempt 04
	Pasword inserted	HPa!aa3#aC	HP@!aa#aC	HP@!aa#aC	HPa!aa3aC
	Phrase Used	Hishara Perera and I attended an event at Colombo	Hishara Perera and I attended an event at Colombo	Hishara Perera and I attended an event at Colombo	Hishara Perera and I attended an event at Colombo
	Status	Failed Attempt	Failed Attempt	Failed Attempt	Successful Login
15 days	Attempts	Attempt 01		Attempt 02	
	Pasword inserted	HPaiaa3aC		HPa!aa3aC	
	Phrase Used	Hishara Perera and I attended an event at Colombo		Hishara Perera and I attended an event at Colombo	
	Status	Failed Attempt		Successful Login	
45 days	Attempts	Attempt 01		Attempt 02	
	Pasword inserted	Ha!aa3aC		HPa!aa3aC	
	Phrase Used	Hishara and I attended an event at Colombo		Hishara Perera and I attended an event at Colombo	

	Status	Failed Attempt	Successful Login

		Participant 03			
Original password		I$tw@UMCf0			
Original Passphrase		I started to work @ UCSC Mozilla Club from 0000			
0 hrs (Initial Login)	Attempts	Attempt 01			
	Pasword inserted	I$tw@UMCf0			
	Phrase Used	I started to work @ UCSC Mozilla Club from 0000			
	Status	Successful Login			
24 hrs	Attempts	Attempt 01	Attempt 02	Attempt 03	Attempt 04
	Pasword inserted	I$w@UMCf0	I$w@UMCf0	I$w@UMCf0	I$tw@UMCf0
	Phrase Used	I started working @ UCSC Mozilla Club from 0000	I started working @ UCSC Mozilla Club from 0000	I started working @ UCSC Mozilla Club from 0000	I started to work @ UCSC Mozilla Club from 0000
	Status	Failed Attempt	Failed Attempt	Failed Attempt	Successful Login
15 days	Attempts	Attempt 01		Attempt 02	
	Pasword inserted	Istw@UMCf0		I$tw@UMCf0	
	Phrase Used	I started to work @UCSC Mozilla Club from 0000		I started to work @ UCSC Mozilla Club from 0000	
	Status	Failed Attempt		Successful Login	
45 days	Attempts	Attempt 01			
	Pasword inserted	I$tw@UMCf0			
	Phrase Used	I started to work @ UCSC Mozilla Club from 0000			

	Status	Successful Login

		Participant 04			
Original Password		Yltbbo4ti!			
Original Passphrase		You Lochana Thathsarani Batuwitage born on a Thursday in 1992			
0 hrs (Initial Login)	Attempts	Attempt 01			
	Pasword inserted	Yltbbo4ti!			
	Phrase Used	You Lochana Thathsarani Batuwitage born on a Thursday in 1992			
	Status	Successful Login			
24 hrs	Attempts	Attempt 01	Attempt 02	Attempt 03	Attempt 04
	Pasword inserted	Yltbboti!	Yltbboti!	Yltbbo@ti1	Yltbbo4ti!
	Phrase Used	You Lochana Thathsarani Batuwitage born on Thursday in 1992	You Lochana Thathsarani Batuwitage born on Thursday in 1992	You Lochana Thathsarani Batuwitage born on a Thursday in 1992	You Lochana Thathsarani Batuwitage born on a Thursday in 1992
	Status	Failed Attempt	Failed Attempt	Failed Attempt	Successful Login
15 days	Attempts	Attempt 01	Attempt 02	Attempt 03	Attempt 04
	Pasword inserted	Yltbbo@ti!	Yltbbo4ti1	Yltbboti!	Yltbbo4ti!
	Phrase Used	You Lochana Thathsarani Batuwitage born on a Thursday in 1992	You Lochana Thathsarani Batuwitage born on a Thursday in 1992	You Lochana Thathsarani Batuwitage born on Thursday in 1992	You Lochana Thathsarani Batuwitage born on a Thursday in 1992
	Status	Failed Attempt	Failed Attempt	Failed Attempt	Successful Login
45 days	Attempts	Attempt 01		Attempt 02	

	Pasword inserted	Yltbbo4tia!	Yltbbo4ti!
	Phrase Used	You Lochana Thathsarani Batuwitage born on a Thursday in a 1992	You Lochana Thathsarani Batuwitage born on a Thursday in 1992
	Status	Failed Attempt	Successful Login

		Participant 05	
Original password		Istw@CEBf2	
Original Passphrase		I started to work @ Ceylon Electricity Board from 2016	
0 hrs (Initial Login)	Attempts	Attempt 01	
	Pasword inserted	Istw@c37f2	
	Phrase Used	I started to work @ Ceylone Electricity board from 2016	
	Status	Successful Login	
24 hrs	Attempts	Attempt 01	Attempt 02
	Pasword inserted	Iwtw@tc37f2	Istw@c37f2
	Phrase Used	I went to work @ the Ceylone Electricity board from 2016	I started to work @ Ceylone Electricity board from 2016
	Status	Failed Attempt	Successful Login
15 days	Attempts	Attempt 01	Attempt 02
	Password inserted	Istw@ce8f2	Istw@c37f2
	Phrase Used	I started to work @ Ceylone Electricity board from 2016	I started to work @ Ceylone Electricity board from 2016
	Status	Successful Login	Successful Login
45 days	Attempts	Attempt 01	

	Password inserted	Istw@c37f2
	Phrase Used	I started to work @ Ceylone Electricity board from 2016
	Status	Successful Login

Appendix M:

Results for the Password Generator for Iteration 03

<table>
<tr><th>Participant</th><th>First letter mnemonic</th><th>Candidate passwords generated with mangling rules</th></tr>
<tr><td>Participant 01</td><td>IwtSpwM1lF</td><td>!wtSpwM1lF', '|wtSpwM1lF', 'IwtSpwM1|F', 'IwtSpwM1!F', 'Iwtspwm1|f', 'Iwtspwm1!f', 'Iwt$pwM1lF', 'Iwt$pwm1lf', '!wtSpwM11F', '|wtSpwM11F', '!wtSpwM17F', '|wtSpwM17F', '1wtSpwM1|F', '!wtSpwM1|F', '|wtSpwM1|F', '1wtSpwM1!F', '!wtSpwM1!F', '|wtSpwM1!F', '1wt$pwM1lF', '!wt$pwM1lF', '|wt$pwM1lF', '!wt5pwM1lF', '|wt5pwM1lF', '!w+SpwM1lF', '|w+SpwM1lF', '7wtSpwM1|F', '7wtSpwM1!F', '|wtSpwM11F', '|wtSpwM17F', '|wtSpwM1|F', '|wtSpwM1!F', '!wtSpwM11F', '!wtSpwM17F', '!wtSpwM1|F', '!wtSpwM1!F', 'Iwt$pwM11F', 'Iwt$pwM17F', 'Iwt$pwM1|F', 'Iwt$pwM1!F', 'Iwt5pwM1|F', 'Iwt5pwM1!F', 'Iw+SpwM1|F', 'Iw+SpwM1!F', 'IwtSpwM!7F', 'IwtSpwM|7F', 'Iwt$pwm11f', 'Iwt$pwm17f', 'Iwt$pwm1|f', 'Iwt$pwm1!f', 'Iwt5pwm1|f', 'Iwt5pwm1!f', 'Iw+spwm1|f', 'Iw+spwm1!f', 'Iwtspwm!7f', 'Iwtspwm|7f', '1wt$pwM1lF', '!wt$pwM1lF', '!wt5pwM1lF', '|wt$pwM1lF', '|wt5pwM1lF', 'Iwt$pwM11F', 'Iwt$pwM17F', 'Iwt$pwM1|F', 'Iwt5pwM1|F', 'Iwt$pwM1!F', 'Iwt5pwM1!F', 'Iw+$pwM1lF', 'Iwt5pwM!lF', 'Iwt5pwM|lF', 'Iwt$pwm11f', 'Iwt$pwm17f', 'Iwt$pwm1|f', 'Iwt5pwm1|f', 'Iwt$pwm1!f', 'Iwt5pwm1!f', 'Iw+$pwm1lf', 'Iwt5pwm!lf', 'Iwt5pwm|lf', '!w+SpwM1lF', '|w+SpwM1lF', 'Iw+SpwM1|F', 'Iw+SpwM1!F', 'Iw+$pwM1lF', 'Iw+spwm1|f', 'Iw+spwm1!f', 'Iw+$pwm1lf', '1wtSpwM!lF', '1wtSpwM|lF', 'IwtSpwM!1F', 'IwtSpwM|1F', 'IwtSpwM!7F', 'IwtSpwM|7F', 'Iwt5pwM!lF', 'Iwt5pwM|lF', 'Iwtspwm!1f', 'Iwtspwm|1f', 'Iwtspwm!7f', 'Iwtspwm|7f', 'Iwt5pwm!lf', 'Iwt5pwm|lf'</td></tr>
<tr><td>Participant 02</td><td>Msbdargjwmb</td><td>'Ms8d@rgjwm8', 'M$bd4rgjwmb', 'M5bd@rgjwmb', 'Ms8d@rgjwm8', 'M$8dargjwm8', 'M5bd@rgjwmb', 'M$bd4rgjwmb', 'M$8dargjwm8'</td></tr>
<tr><td>Participant 03</td><td>SaDwawmiml</td><td>'S@Dw@wm1ml', 'S4Dw4wm!ml', 'S4Dw4wm|ml', 'S@Dw@wmim1', 'S@Dw@wmim7', 'S4Dw4wmim|', 'S4Dw4wmim!', '$4Dw4wmiml', '5@Dw@wmiml', 'S@dw@wm1ml', 'S4dw4wm!ml', 'S4dw4wm|ml', 'S@dw@wmim1', 'S@dw@wmim7', 'S4dw4wmim|', 'S4dw4wmim!', 'S@Dw@wm1ml', 'S4Dw4wm!ml', 'S4Dw4wm|ml', 'SaDwawm!m1', 'SaDwawm|m1', 'SaDwawm!m7', 'SaDwawm|m7', 'SaDwawm1m|', 'SaDwawm1m!', '$aDwawm1ml',</td></tr>
</table>

<table>
<tr><td></td><td></td><td>'5aDwawm!ml', '5aDwawm|ml', 'S@dw@wm1ml', 'S4dw4wm!ml', 'S4dw4wm|ml', 'Sadwawm!m1', 'Sadwawm|m1', 'Sadwawm!m7', 'Sadwawm|m7', 'Sadwawm1m|', 'Sadwawm1m!', 'S@Dw@wmim1', 'S@Dw@wmim7', 'S4Dw4wmim|', 'S4Dw4wmim!', 'SaDwawm1m|', 'SaDwawm1m!', 'SaDwawm|m1', 'SaDwawm|m7', 'SaDwawm1m|', 'SaDwawm1m!', '$aDwawmim1', '$aDwawmim7', '5aDwawmim|', '5aDwawmim!', 'S@dw@wmim1', 'S@dw@wmim7', 'S4dw4wmim|', 'S4dw4wmim!', 'Sadwawm1m|', 'Sadwawm1m!', 'Sadwawm|m1', 'Sadwawm|m7', 'Sadwawm1m|', 'Sadwawm1m!', '5@Dw@wmiml', '$4Dw4wmiml', '$aDwawm1ml', '5aDwawm!ml', '5aDwawm|ml', '$aDwawmim1', '$aDwawmim7', '5aDwawmim|', '5aDwawmim!'</td></tr>
<tr><td>Participant 04</td><td>Trbsfethicl</td><td>'Tr8sfeth!cl', 'Tr8sfeth|cl', 'Tr8sfethic|', 'Tr8sfethic!', 'Tr8$fethicl', 'Trbsf3th!cl', 'Trbsf3th|cl', 'Trbsf3thic|', 'Trbsf3thic!', 'Trb$f3thicl', 'Tr8sfeth!cl', 'Tr8sfeth|cl', 'Trbsf3th!cl', 'Trbsf3th|cl', 'Trbsfeth!c1', 'Trbsfeth|c1', 'Trbsfeth!c7', 'Trbsfeth|c7', 'Trbsfeth1c|', 'Trbsfeth1c!', 'Trb$feth1cl', 'Trb5feth!cl', 'Trb5feth|cl', 'Tr8sfethic|', 'Tr8sfethic!', 'Trbsf3thic|', 'Trbsf3thic!', 'Trbsfeth1c|', 'Trbsfeth1c!', 'Trbsfeth|c1', 'Trbsfeth|c7', 'Trbsfeth1c|', 'Trbsfeth1c!', 'Trb$fethic1', 'Trb$fethic7', 'Trb5fethic|', 'Trb5fethic!', 'Tr8$fethicl', 'Trb$f3thicl', 'Trb$feth1cl', 'Trb5feth!cl', 'Trb5feth|cl', 'Trb$fethic1', 'Trb$fethic7', 'Trb5fethic|', 'Trb5fethic!', 'Trb$f3thic'</td></tr>
<tr><td>Participant 05</td><td>sdatbdilIltt</td><td>'sd@t8dilIltt', 'sd@tbd1lIltt', 'sd4tbd!lIltt', 'sd4tbd|lIltt', 'sd@tbdi1I1tt', 'sd@tbdi7I7tt', 'sd4tbdi|I|tt', 'sd4tbdi!I!tt', '$d4tbdilIltt', '5d@tbdilIltt', 'Sd@t8dililtt', 'Sd@tbd1liltt', 'Sd4tbd!liltt', 'Sd4tbd|liltt', 'Sd@tbdil1ltt', 'Sd4tbdil!ltt', 'Sd4tbdil|ltt', 'Sd@tbdi1i1tt', 'Sd@tbdi7i7tt', 'Sd4tbdi|i|tt', 'Sd4tbdi!i!tt', 'sd@t8dilIltt', 'sdat8d!lIltt', 'sdat8d|lIltt', 'sdat8di|I|tt', 'sdat8di!I!tt', '$dat8dilIltt', 'Sd@t8dililtt', 'Sdat8d!liltt', 'Sdat8d|liltt', 'Sdat8dil!ltt', 'Sdat8dil|ltt', 'Sdat8di|i|tt', 'Sdat8di!i!tt', 'sd@tbd1lIltt', 'sd4tbd!lIltt', 'sd4tbd|lIltt', 'sdat8d!lIltt', 'sdat8d|lIltt', 'sdatbd!1I1tt', 'sdatbd|1I1tt', 'sdatbd!7I7tt', 'sdatbd|7I7tt', 'sdatbd1|I|tt', 'sdatbd1!I!tt', '$datbd1lIltt', '5datbd!lIltt', '5datbd|lIltt', 'Sd@tbd1liltt', 'Sd4tbd!liltt', 'Sd4tbd|liltt', 'Sdat8d!liltt', 'Sdat8d|liltt', 'Sdatbd!l1ltt', 'Sdatbd|l1ltt', 'Sdatbd1l!ltt', 'Sdatbd1l|ltt', 'Sdatbd!1i1tt', 'Sdatbd|1i1tt', 'Sdatbd!7i7tt', 'Sdatbd|7i7tt', 'Sdatbd1|i|tt', 'Sdatbd1!i!tt', 'Sd@tbdil1ltt', 'Sd4tbdil!ltt', 'Sd4tbdil|ltt', 'Sdat8dil!ltt', 'Sdat8dil|ltt', 'Sdatbd1l!ltt', 'Sdatbd1l|ltt', 'Sdatbd!l1ltt', 'Sdatbd|l1ltt', 'Sdatbdi1!1tt', 'Sdatbdi1|1tt', 'Sdatbdi7!7tt', 'Sdatbdi7|7tt', 'Sdatbdi|1|tt', 'Sdatbdi!1!tt', 'sd@tbdi1I1tt', 'sd@tbdi7I7tt', 'sd4tbdi|I|tt', 'sd4tbdi!I!tt', 'sdat8di|I|tt', 'sdat8di!I!tt', 'sdatbd1|I|tt', 'sdatbd1!I!tt', 'sdatbd|1I1tt', 'sdatbd|7I7tt', 'sdatbd1|I|tt', 'sdatbd1!I!tt', '$datbdi1I1tt', '$datbdi7I7tt', '5datbdi|I|tt', '5datbdi!I!tt', 'Sd@tbdi1i1tt', 'Sd@tbdi7i7tt', 'Sd4tbdi|i|tt', 'Sd4tbdi!i!tt', 'Sdat8di|i|tt', 'Sdat8di!i!tt', 'Sdatbd1|i|tt', 'Sdatbd1!i!tt', 'Sdatbd|1i1tt', 'Sdatbd|7i7tt', 'Sdatbd1|i|tt', 'Sdatbd1!i!tt', 'Sdatbdi|7|tt', 'Sdatbdi!7!tt', 'Sdatbdi1|1tt', 'Sdatbdi7|7tt', 'Sdatbdi1!1tt', 'Sdatbdi7!7tt', '5d@tbdilIltt', '$d4tbdilIltt', '$dat8dilIltt', '$datbd1lIltt', '5datbd!lIltt', '5datbd|lIltt', '$datbdi1I1tt', '$datbdi7I7tt', '5datbdi|I|tt', '5datbdi!I!tt', '$d4tbdi1I1tt'</td></tr>
</table>

Appendix N:

Results for the Memorability Module for Iteration 03

		Participant 01	
Original password		Iwt$pwm11f	
Original Passphrase		I went to Siri pada with MTG 18 last February	
0 hrs (Initial Login)	Attempts	Attempt 01	Attempt 02
	Pasword inserted	Iwt$wm11f	Iwt$pwm11f
	Phrase Used	I went to Siri pada with MTG 18 last February	I went to Siri pada with MTG 18 last February
	Status	Failed Attempt	Successful Login
12 hrs	Attempts	Attempt 01	
	Pasword inserted	Iwt$pwm11f	
	Phrase Used	I went to Siri pada with MTG 18 last February	
	Status	Successful Login	
18 hrs	Attempts	Attempt 01	
	Pasword inserted	Iwt$pwm11f	
	Phrase Used	I went to Siri pada with MTG 18 last February	
	Status	Successful Login	
27 Hrs	Attempts	Attempt 01	
	Pasword inserted	Iwt$pwm11f	
	Phrase Used	I went to Siri pada with MTG 18 last February	

	Status	Successful Login
40.5 hrs	Attempts	Attempt 01
	Pasword inserted	Iwt$pwm11f
	Phrase Used	I went to Siri pada with MTG 18 last February
	Status	Successful Login

		Participant 02
Original password		M5bd@rgjwmb
Original Passphrase		My sister's big day at royal grand ja-ela with massina's brother
0 hrs (Initial Login)	Attempts	Attempt 01
	Pasword inserted	M5bd@rgjwmb
	Phrase Used	My sister's big day at royal grand ja-ela with massina's brother
	Status	Successful Login
12 hrs	Attempts	Attempt 01
	Pasword inserted	M5bd@rgjwmb
	Phrase Used	My sister's big day at royal grand ja-ela with massina's brother
	Status	Successful Login
18 hrs	Attempts	Attempt 01
	Pasword inserted	M5bd@rgjwmb
	Phrase Used	My sister's big day at royal grand ja-ela with massina's brother

	Status	Successful Login
27 Hrs	Attempts	Attempt 01
	Pasword inserted	M5bd@rgjwmb
	Phrase Used	My sister's big day at royal grand ja-ela with massina's brother
	Status	Successful Login
40.5 hrs	Attempts	Attempt 01
	Pasword inserted	M5bd@rgjwmb
	Phrase Used	My sister's big day at royal grand ja-ela with massina's brother
	Status	Successful Login

		Participant 03
Original password		Sadwawm!m7
Original Passphrase		Sightseeing at Deniyaya was a wonderful memory in my life
0 hrs (Initial Login)	Attempts	Attempt 1
	Pasword inserted	Sadwawm!m7
	Phrase Used	Sightseeing at Deniyaya was a wonderful memory in my life
	Status	Successful Login
12 hrs	Attempts	Attempt 1
	Pasword inserted	Sadwawm!m7
	Phrase Used	Sightseeing at Deniyaya was a wonderful memory in my life
	Status	Successful Login

18 hrs	Attempts	Attempt 1
	Pasword inserted	Sadwawm!m7
	Phrase Used	Sightseeing at Deniyaya was a wonderful memory in my life
	Status	Successful Login
27 Hrs	Attempts	Attempt 1
	Pasword inserted	Sadwawm!m7
	Phrase Used	Sightseeing at Deniyaya was a wonderful memory in my life
	Status	Successful Login
40.5 hrs	Attempts	Attempt 1
	Pasword inserted	Sadwawm!m7
	Phrase Used	Sightseeing at Deniyaya was a wonderful memory in my life
	Status	Successful Login

		Participant 04
Original password		Trb5feth!cl
Original Passphrase		The reason behind smiling faces even the heart is crying loud
0 hrs (Initial Login)	Attempts	Attempt 1
	Pasword inserted	Trb5feth!cl
	Phrase Used	The reason behind smiling faces even the heart is crying loud
	Status	Successful Login
	Attempts	Attempt 1

12 hrs	Pasword inserted	Trb5feth!cl
	Phrase Used	The reason behind smiling faces even the heart is crying loud
	Status	Successful Login
18 hrs	Attempts	Attempt 1
	Pasword inserted	Trb5feth!cl
	Phrase Used	The reason behind smiling faces even the heart is crying loud
	Status	Successful Login
27 Hrs	Attempts	Attempt 1
	Pasword inserted	Trb5feth!cl
	Phrase Used	The reason behind smiling faces even the heart is crying loud
	Status	Successful Login
40.5 hrs	Attempts	Attempt 1
	Pasword inserted	Trb5feth!cl
	Phrase Used	The reason behind smiling faces even the heart is crying loud
	Status	Successful Login

		Participant 05
Original password		$dat8dilIltt
Original Passphrase		school days are the best days in life, I love that time.
	Attempts	Attempt 1

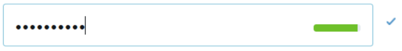
0 hrs (Initial Login)	Pasword inserted	$dat8dilIltt			
	Phrase Used	school days are the best days in life, I love that time.			
	Status	Successful Login			
12 hrs	Attempts	Attempt 01	Attempt 02	Attempt 03	Attempt 04
	Pasword inserted	$lit8tilIltt	$lit8tilIltt	$lit8dolIltt	$dat8dilIltt
	Phrase Used	school life is the best thing in life, I love that time.	school life is the best thing in life, I love that time	school life is the best days of life, I love that time.	school days are the best days in life, I love that time.
	Status	Failed Attempt	Failed Attempt	Failed Attempt	Successful Login
18 hrs	Attempts	Attempt 01	Attempt 02	Attempt 03	Attempt 04
	Pasword inserted	$dat8tilIltt	$dat8tilIltt	$lit8tilIltt	$dat8dilIltt
	Phrase Used	school days are the best time in life, I love that time	school days are the best time in life, I love that time	<No input>	school days are the best days in life, I love that time.
	Status	Failed Attempt	Failed Attempt	Failed Attempt	Successful Login
27 Hrs	Attempts	Attempt 1			
	Pasword inserted	$dat8dilIltt			
	Phrase Used	school days are the best days in life, I love that time.			
	Status	Successful Login			
40.5 hrs	Attempts	Attempt 1			
	Pasword inserted	$dat8dilIltt			
	Phrase Used	school days are the best days in life, I love that time.			
	Status	Successful Login			

Appendix O:

Acceptability of the passwords generated from Iteration 03 in popular websites.

E commerce			
Site	**Password**	**Acceptability**	**Feedback or Suggestions**
amazon	Iwt$pwm11f	Accepted	
	M5bd@rgjwmb	Accepted	
	Sadwawm!m7	Accepted	
	Trb5feth!cl	Accepted	
	$dat8dilIltt	Accepted	
eBay	Iwt$pwm11f	Accepted	
	M5bd@rgjwmb	Accepted	
	Sadwawm!m7	Accepted	
	Trb5feth!cl	Accepted	
	$dat8dilIltt	Accepted	
Alibaba.com	Iwt$pwm11f	Accepted	“Medium Strength”
	M5bd@rgjwmb	Accepted	“Medium Strength”
	Sadwawm!m7	Accepted	“Medium Strength”
	Trb5feth!cl	Accepted	“Medium Strength”
	$dat8dilIltt	Accepted	“Medium Strength”

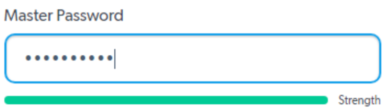
takas.lk	Iwt$pwm11f	Accepted	
	M5bd@rgjwmb	Accepted	
	Sadwawm!m7	Accepted	
	Trb5feth!cl	Accepted	
	$dat8dilIltt	Accepted	

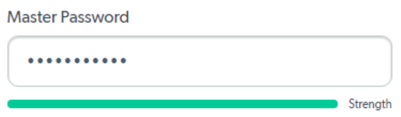
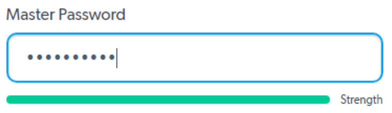
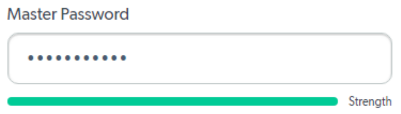
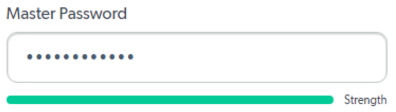
Social Media			
Site	**Password**	**Acceptability**	**Feedback or Suggestions**
Facebook	Iwt$pwm11f	Accepted	
	M5bd@rgjwmb	Accepted	
	Sadwawm!m7	Accepted	
	Trb5feth!cl	Accepted	
	$dat8dilIltt	Accepted	
Twitter	Iwt$pwm11f	Accepted	
	M5bd@rgjwmb	Accepted	
	Sadwawm!m7	Accepted	
	Trb5feth!cl	Accepted	
	$dat8dilIltt	Accepted	
LinkedIn	Iwt$pwm11f	Accepted	
	M5bd@rgjwmb	Accepted	

	Sadwawm!m7	Accepted	
	Trb5feth!cl	Accepted	
	$dat8dilIltt	Accepted	
Instagram	Iwt$pwm11f	Accepted	
	M5bd@rgjwmb	Accepted	
	Sadwawm!m7	Accepted	
	Trb5feth!cl	Accepted	
	$dat8dilIltt	Accepted	

Social Media			
Site	**Password**	**Acceptability**	**Feedback or Suggestions**
gmail	Iwt$pwm11f	Accepted	Strong
	M5bd@rgjwmb	Accepted	Strong
	Sadwawm!m7	Accepted	Strong
	Trb5feth!cl	Accepted	Strong
	$dat8dilIltt	Accepted	Strong
Yahoo	Iwt$pwm11f	Accepted	

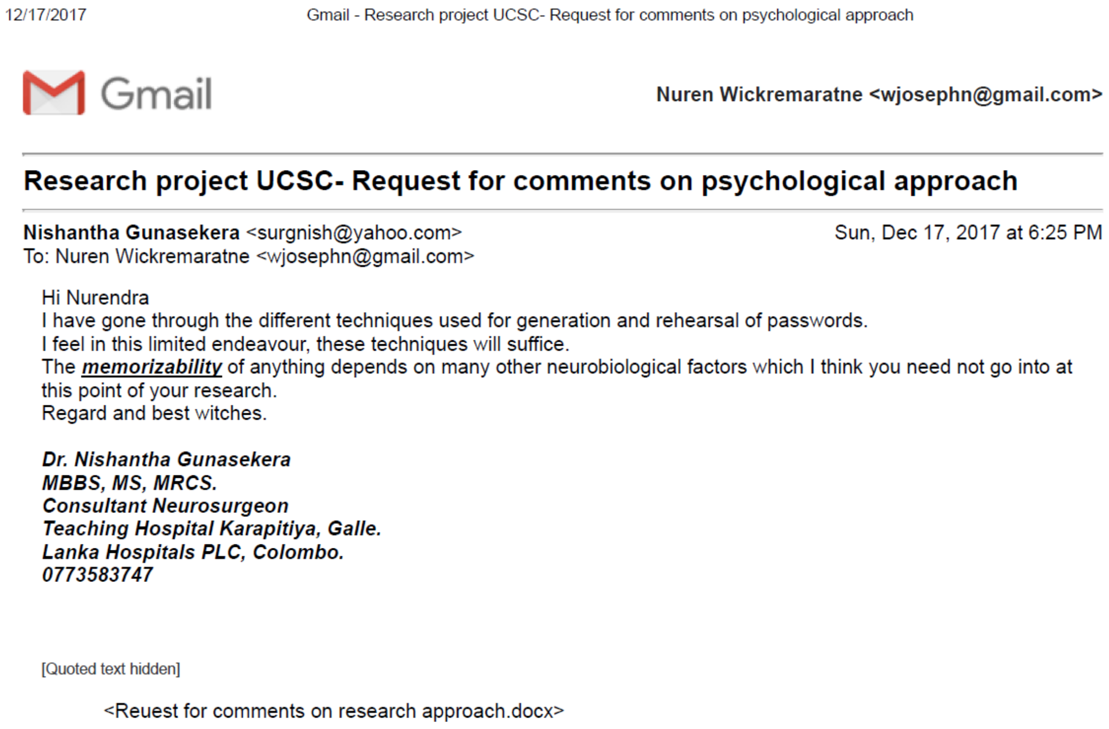
	M5bd@rgjwmb	Accepted	
	Sadwawm!m7	Accepted	
	Trb5feth!cl	Accepted	
	$dat8dilIltt	Accepted	
Hot mail	Iwt$pwm11f	Accepted	
	M5bd@rgjwmb	Accepted	
	Sadwawm!m7	Accepted	
	Trb5feth!cl	Accepted	
	$dat8dilIltt	Accepted	

Other			
Site	**Password**	**Acceptability**	**Feedback or Suggestions**
Paypal	Iwt$pwm11f	Accepted	
	M5bd@rgjwmb	Accepted	
	Sadwawm!m7	Accepted	
	Trb5feth!cl	Accepted	
	$dat8dilIltt	Accepted	
LastPass	Iwt$pwm11f	Accepted	 Master Password •••••••••• Strength

	M5bd@rgjwmb	Accepted	
	Sadwawm!m7	Accepted	
	Trb5feth!cl	Accepted	
	$dat8dilIltt	Accepted	

Appendix P:

Expert Comments



12/17/2017 Gmail - Research project UCSC- Request for comments on psychological approach

Gmail Nuren Wickremaratne <wjosephn@gmail.com>

Research project UCSC- Request for comments on psychological approach

Nishantha Gunasekera <surgnish@yahoo.com> Sun, Dec 17, 2017 at 6:25 PM
To: Nuren Wickremaratne <wjosephn@gmail.com>

Hi Nurendra
I have gone through the different techniques used for generation and rehearsal of passwords.
I feel in this limited endeavour, these techniques will suffice.
The ***memorizability*** of anything depends on many other neurobiological factors which I think you need not go into at this point of your research.
Regard and best witches.

Dr. Nishantha Gunasekera
MBBS, MS, MRCS.
Consultant Neurosurgeon
Teaching Hospital Karapitiya, Galle.
Lanka Hospitals PLC, Colombo.
0773583747

[Quoted text hidden]

<Reuest for comments on research approach.docx>